]HackingTeam[

# RCS 9.6

*The hacking suite for governmental interception*

## Manuale del tecnico

# Proprietà delle informazioni



richieste di ulteriori copie di questo manuale o di informazioni tecniche sul prodotto, devono essere indirizzate a:

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

**Tel.**: + 39 02 29 060 603

**Fax**: + 39 02 63 118 946

**e-mail**: info@hackingteam.com

# Sommario


Introduzione a questa Guida ..... 1
Informazioni utili sulla Guida ..... 1
Obiettivi del manuale ..... 1
Novità della guida ..... 1
Documentazione fornita ..... 3
Convenzioni tipografiche per le segnalazioni ..... 4
Convenzioni tipografiche per la formattazione ..... 4
Destinatari del prodotto e di questa guida ..... 5
Dati di identificazione dell'autore del software ..... 6
RCS Console per il Tecnico ..... 7
Avvio di RCS Console ..... 8
Introduzione ..... 8
Come si presenta la pagina di login ..... 8
Accedere a RCS Console ..... 8
Descrizione della homepage ..... 9
Introduzione ..... 9
Come si presenta ..... 9
Descrizione dei wizard da homepage ..... 10
Introduzione ..... 10
Come si presenta ..... 10
Investigazione Rapida ..... 11
Elementi e azioni comuni dell'interfaccia ..... 11
Introduzione ..... 11
Come si presenta RCS Console ..... 11
Cambiare la lingua dell'interfaccia o la propria password ..... 13
Convertire le date-ora di RCS Console al proprio fuso orario ..... 13
Azioni sulle tabelle ..... 14
Procedure del Tecnico ..... 16
Introduzione ..... 16
Effettuare l'infezione su connessioni HTTP ..... 16
Infettare un computer non connesso a internet ..... 16
Infettare un computer connesso a Internet ..... 17

Mantenere aggiornato il software degli agent ..... 17
Operation e target ..... 18
Cose da sapere sulle operation ..... 19
Cos'è un'operation ..... 19
Cose da sapere sui target ..... 19
Cos'è un target ..... 19
Gestione delle operation ..... 19
Scopo ..... 19
Come si presenta la funzione ..... 19
Per saperne di più ..... 20
Visualizzare i target di un'operation ..... 20
Dati delle operation ..... 21
Pagina dell'operation ..... 21
Scopo ..... 21
Come si presenta la funzione ..... 21
Per saperne di più ..... 22
Creare una factory ..... 23
Dati della pagina di un'operation ..... 23
I target ..... 24
Pagina del target ..... 25
Scopo ..... 25
Come si presenta la funzione ..... 25
Per saperne di più ..... 26
Creare una factory ..... 27
Chiudere una factory o un agent ..... 27
Eliminare una factory o un agent ..... 27
Importare le evidence del target ..... 27
Dati della pagina target ..... 28
Cose da sapere sulle Factory e sugli Agent ..... 29
Modalità di infezione ..... 29
Componenti della strategia di infezione ..... 29
Le factory ..... 30
Modalità di creazione delle factory ..... 30
I vettori di installazione ..... 30

Gli agent ..... 31
I moduli per l'acquisizione dei dati ..... 31
Compilazione di una factory ..... 31
Scopo ..... 31
Passi successivi ..... 31
Come si presenta la funzione ..... 31
Per saperne di più ..... 32
Creare un agent ..... 32
Creare un agent da collaudare in modalità demo ..... 33
Gli agent ..... 34
Cose da sapere sugli agent ..... 35
Introduzione ..... 35
Processo di installazione di un agent ..... 35
Icone degli agent ..... 35
Agent scout ..... 36
Agent soldier ..... 36
Agent elite ..... 36
Sincronizzazione di un agent ..... 36
Agent offline e online ..... 36
Disabilitazione temporanea di un agent ..... 37
Collaudo di un agent ..... 37
Configurazione dell'agent ..... 37
Pagina dell'agent ..... 38
Scopo ..... 38
Come si presenta la funzione ..... 38
Per saperne di più ..... 40
Dati dello storico configurazioni di un agent ..... 40
Dati dello storico eventi di un agent ..... 40
Dati dello storico sincronizzazioni dell'agent ..... 40
Pagina dei comandi ..... 41
Scopo ..... 41
Come si presenta la funzione ..... 41
Per saperne di più ..... 42
Trasferimento file da/a il target ..... 42

Scopo ... 42
Come si presenta la funzione ... 42
Per saperne di più ... 44
Factory e agent: configurazione base ... 45
Cose da sapere sulla configurazione base ... 46
Configurazione base ... 46
Esportazione e importazione di configurazioni ... 46
Salvataggio della configurazione come template ... 46
Configurazione base di una factory o di un agent ... 46
Scopo ... 47
Passi successivi ... 47
Come si presenta la funzione ... 47
Per saperne di più ... 48
Configurare una factory o un agent ... 48
Dati della configurazione base ... 49
Factory e agent: configurazione avanzata ... 51
Cose da sapere sulla configurazione avanzata ... 52
Configurazione avanzata ... 52
Componenti della configurazione avanzata ... 52
Lettura delle sequenze ... 53
Eventi ... 53
Azioni ... 54
Relazioni tra azioni e moduli ... 54
Relazioni tra azioni e eventi ... 54
Moduli ... 55
Esportazione e importazione di configurazioni ... 55
Salvataggio della configurazione come template ... 55
Configurazione avanzata di una factory o di un agent ... 55
Scopo ... 55
Passi successivi ... 56
Come si presenta la funzione ... 56
Per saperne di più ... 57
Creare una sequenza di attivazione semplice ... 57
Creare una sequenza di attivazione complessa ... 58

Dati globali dell'agent ..... 59
I Network Injector ..... 60
Cose da sapere su Network Injector e le sue regole ..... 61
Introduzione ..... 61
Tipi di Network Injector ..... 61
Tipi di risorse infettabili ..... 61
Come creare una regola ..... 61
Regole di identificazione automatica e da operatore ..... 61
Cosa succede quando si abilita/disabilita una regola ..... 62
Avvio dell'infezione ..... 62
Gestione dei Network Injector ..... 62
Scopo ..... 62
Cosa è possibile fare ..... 62
Per saperne di più ..... 63
Aggiungere una nuova regola di infezione ..... 64
Inviare le regole al Network Injector ..... 64
Dati delle regole di infezione ..... 64
Verifica dello stato dei Network Injector ..... 69
Introduzione ..... 69
Individuare quando il Network Injector è sincronizzato ..... 69
Cose da sapere su Appliance Control Center ..... 70
Introduzione ..... 70
Funzionamento di Appliance Control Center ..... 70
Sincronizzazione con il server RCS ..... 70
Chiave di autenticazione ..... 70
Aggiornamento delle regole di infezione ..... 70
Utilizzo delle interfacce di rete ..... 71
Indirizzo IP dell'interfaccia di infezione ..... 71
Processo di infezione tramite identificazione automatica ..... 71
Infezione tramite identificazione automatica ..... 71
Cose da sapere su Tactical Control Center ..... 72
Introduzione ..... 72
Funzionamento del Tactical Control Center ..... 72
Sincronizzazione con il server RCS ..... 72

Chiave di autenticazione ..... 73
Aggiornamento delle regole di infezione ..... 73
Utilizzo delle interfacce di rete ..... 73
Processo di infezione tramite identificazione automatica ..... 73
Processo di infezione tramite identificazione manuale ..... 74
Acquisizione password di rete WiFi protetta ..... 74
Forzatura dell'autenticazione dei dispositivi sconosciuti ..... 75
Infezione tramite identificazione automatica ..... 75
Infezione tramite identificazione da operatore ..... 75
Impostazione di filtri sul traffico intercettato ..... 75
Individuazione del target tramite l'analisi della cronologia ..... 76
Emulazione di un Access Point conosciuto dal target ..... 76
Cose da sapere per individuare la password di rete WiFi ..... 77
Introduzione ..... 77
WPA/WPA2 dictionary attack ..... 77
WEP bruteforce attack ..... 77
WPS PIN bruteforce attack ..... 77
Stato di avanzamento dell'attacco ..... 77
Cose da sapere per lo sblocco della password del sistema operativo ..... 78
Introduzione ..... 78
Requisiti del Tactical Network Injector ..... 78
Requisiti del computer target ..... 78
Processo standard ..... 79
Cose da sapere per l'accesso remoto al Control Center ..... 79
Introduzione ..... 79
Password del disco (solo Tactical Control Center) ..... 80
Modem 3G per la connessione ..... 80
Indirizzo IP del dispositivo ..... 81
Modalità di invio dell'e-mail con l'indirizzo IP ..... 81
Protocollo di rete ..... 81
Altre funzioni utili ..... 81
Comandi Tactical Control Center e Appliance Control Center ..... 81
Introduzione ..... 81
Comandi ..... 81

Appliance Control Center ..... 82
Scopo ..... 82
Richiesta della password ..... 82
Come si presenta la funzione ..... 83
Per saperne di più ..... 83
Abilitare la sincronizzazione con il server RCS per ricevere nuove regole ..... 83
Avviare un test della rete ..... 84
Infettare i target tramite identificazione automatica ..... 85
Configurare l'accesso remoto all'applicativo ..... 87
Visualizzare i dettagli dell'infezione ..... 88
Dati Appliance Control Center ..... 89
Dati della scheda Network Injector ..... 89
Dati scheda System Management ..... 89
Tactical Control Center ..... 90
Scopo ..... 90
Richiesta della password ..... 90
Come si presenta la funzione ..... 90
Per saperne di più ..... 91
Abilitare la sincronizzazione con il server RCS per ricevere nuove regole ..... 91
Avviare un test della rete ..... 92
Acquisire la password di una rete WiFi protetta ..... 93
Infettare i target tramite identificazione automatica ..... 95
Forzare l'autenticazione dei dispositivi sconosciuti ..... 97
Infettare i target tramite identificazione manuale ..... 98
Impostare i filtri sul traffico intercettato ..... 100
Individuare un target analizzando la cronologia web ..... 101
Pulire i dispositivi erroneamente infettati ..... 102
Emulare un Access Point conosciuto dal target ..... 102
Sbloccare la password di un sistema operativo ..... 103
Configurare l'accesso remoto all'applicativo ..... 104
Spegnere il Tactical Network Injector ..... 107
Visualizzare i dettagli dell'infezione ..... 107
Dati del Tactical Control Center ..... 107
Dati scheda Network Injector ..... 107

Dati dei dispositivi rilevati ..... 107
Dati scheda Wireless Intruder ..... 108
Dati scheda Fake Access Point ..... 109
Dati scheda System Management ..... 109
Altri applicativi installati sui Network Injector ..... 109
Introduzione ..... 109
Applicativi ..... 109
Monitoraggio del sistema ..... 111
Monitoraggio del sistema (Monitor) ..... 112
Scopo ..... 112
Come si presenta la funzione ..... 112
Per saperne di più ..... 113
Dati del monitoraggio del sistema (Monitor) ..... 113
Appendice: azioni ..... 115
Elenco delle sotto-azioni ..... 116
Descrizione dati sotto-azioni ..... 116
Descrizione tipi di sotto-azioni ..... 116
Azione Destroy ..... 116
Scopo ..... 116
Parametri ..... 116
Azione Execute ..... 117
Scopo ..... 117
Riferimento a cartella dell'agent ..... 117
Dati significativi ..... 117
Azione Log ..... 117
Scopo ..... 117
Parametri ..... 118
Azione SMS ..... 118
Scopo ..... 118
Parametri ..... 118
Azione Synchronyze ..... 118
Scopo ..... 118
Parametri desktop ..... 119
Parametri mobile ..... 119

Criteri di selezione del tipo di connessione (Windows Phone) ..... 119
Azione Uninstall ..... 120
Scopo ..... 120
Appendice: eventi ..... 121
Elenco degli eventi ..... 122
Descrizione dati eventi ..... 122
Descrizione tipi eventi ..... 122
Evento AC ..... 123
Scopo ..... 123
Evento Battery ..... 123
Scopo ..... 123
Parametri ..... 123
Evento Call ..... 123
Scopo ..... 123
Parametri ..... 124
Evento Connection ..... 124
Scopo ..... 124
Parametri desktop ..... 124
Evento Idle ..... 124
Scopo ..... 124
Parametri ..... 125
Evento Position ..... 125
Scopo ..... 125
Parametri ..... 125
Evento Process ..... 125
Scopo ..... 125
Parametri ..... 125
Evento Quota ..... 126
Scopo ..... 126
Parametri ..... 126
Evento Screensaver ..... 126
Scopo ..... 126
Evento SimChange ..... 126
Scopo ..... 126

Evento SMS 126
Scopo 126
Parametri 127
Evento Standby 127
Evento Timer 127
Scopo 127
Parametri 128
Evento Window 128
Scopo 128
Evento WinEvent 128
Scopo 128
Parametri 128
Appendice: moduli 129
Elenco dei moduli 130
Descrizione tipi moduli 130
Modulo Addressbook 132
Scopo 132
Modulo Application 132
Scopo 132
Modulo Calendar 132
Scopo 132
Modulo Call 132
Scopo 132
Dati significativi 132
Modulo Camera 133
Scopo 133
Dati significativi 133
Modulo Chat 133
Scopo 133
Modulo Clipboard 133
Scopo 133
Modulo Conference 133
Scopo 133
Dati significativi 134

Modulo Crisis 134
Comportamento su dispositivi desktop 134
Comportamento su dispositivi mobile 134
Dati significativi desktop 134
Dati significativi mobile 135
Modulo Device 135
Scopo 135
Dati significativi mobile 135
Modulo File 136
Scopo 136
Dati significativi 136
Modulo Keylog 137
Scopo 137
Modulo Livemic 137
Scopo 137
Dati significativi 137
Modulo Messages 137
Scopo 137
Dati significativi 138
Modulo Mic 138
Scopo 138
Dati significativi desktop 138
Modulo Money 139
Scopo 139
Modulo Mouse 139
Scopo 139
Dati significativi 139
Modulo Password 140
Scopo 140
Modulo Photo 140
Scopo 140
Modulo Position 140
Scopo 140
Dati significativi mobile 140

Modulo Screenshot ..... 141
Scopo ..... 141
Dati significativi ..... 141
Modulo Url ..... 141
Scopo ..... 141
Appendice: vettori di installazione ..... 142
Elenco dei vettori di installazione ..... 143
Descrizione tipi vettori di installazione ..... 143
Cose da sapere su Android ..... 144
Privilegi di root ..... 144
Ottenere i privilegi di root ..... 144
Verificare di avere i privilegi di root ..... 144
Ottenere un certificato per il Code Signing ..... 145
Introduzione ..... 145
Installazione del certificato Code Signing ..... 145
Vettore Exploit ..... 145
Scopo ..... 145
Installazione per dispositivi desktop ..... 145
Installazione per dispositivi mobile ..... 145
Esempio di comandi per copiare un installer nel dispositivo iOS ..... 145
Eliminazione di file non più utilizzati ..... 146
Parametri ..... 146
Vettore Installation Package ..... 146
Scopo ..... 146
Note per sistemi operativi Android (preparazione del vettore) ..... 146
Note per sistemi operativi Android (installazione) ..... 146
Note per sistemi operativi Windows Phone (preparazione del vettore) ..... 147
Note per sistemi operativi Windows Phone (installazione) ..... 147
Note per sistemi operativi Windows Mobile ..... 148
Note per sistemi operativi BlackBerry ..... 149
Note per sistemi operativi Symbian ..... 149
Parametri Android, WinMobile, Windows Phone ..... 149
Parametri BlackBerry ..... 149
Parametri Symbian ..... 150

Preparazione Installation Package per Windows Phone ..... 150
Introduzione ..... 150
Sequenza consigliata ..... 150
Come leggere queste istruzioni ..... 150
Ottenere un codice identificativo Symantec ..... 151
Ottenere il certificato Symantec ..... 152
Installare il certificato Symantec ..... 152
Generare il file .pfx e il file .aetx ..... 153
Caricare il file .pfx e il file .aetx sul server database RCS ..... 154
Vettore Local Installation ..... 154
Scopo ..... 154
Vettore Melted Application ..... 155
Scopo ..... 155
Parametri ..... 155
Vettore Network Injection ..... 156
Scopo ..... 156
Vettore Offline Installation ..... 156
Scopo ..... 156
Parametri ..... 156
Installare o disinstallare l'agent ..... 156
Esportare le evidence ..... 157
Vettore Persistent Installation (desktop) ..... 157
Scopo ..... 157
Preparazione del vettore ..... 157
Installare l'agent ..... 158
Condizioni per l'attivazione dell'infezione ..... 158
Verificare l'installazione ..... 158
Vettore Persistent Installation (mobile) ..... 159
Scopo ..... 159
Preparazione del vettore ..... 159
Installare l'agent ..... 159
Parametri ..... 160
Vettore QR Code/Web link ..... 160
Scopo ..... 160

Funzionamento ..... 160
Eliminazione file non più utilizzati ..... 160
Parametri ..... 160
Vettore Silent Installer ..... 161
Scopo ..... 161
Vettore U3 Installation ..... 161
Scopo ..... 161
Vettore WAP Push Message ..... 162
Scopo ..... 162
Funzionamento ..... 162
Installazione ..... 162
Eliminazione dei file non più utilizzati ..... 162
Parametri ..... 162
Glossario dei termini ..... 164

# 1

# Introduzione a questa Guida

## Informazioni utili sulla Guida

### Obiettivi del manuale

Questo manuale guida il *Tecnico* a utilizzare RCS Console per:

- creare gli agent e installarli su un target definito dall'Amministratore
- creare le regole per l'infezione di connessioni HTTP per i Network Injector

### Novità della guida

Elenco note di rilascio e aggiornamenti di questa guida in linea.

| *Data rilascio* | *Codice* | *Versione software* | *Descrizione* |
|---|---|---|---|
| 15 Marzo 2015 | Manuale del tecnico 2.0 MAR-2015 | 9.6 | Aggiunto modulo **Photo**, *vedi "**Modulo Photo**" a pagina 140*<br>Aggiornato modulo **Chat**, *vedi "**Modulo Chat**" a pagina 133*<br>Aggiornato modulo **Position**, *vedi "**Modulo Position**" a pagina 140*.<br>Aggiunta disabilitazione automatica per inserimento password errata e procedure di riabilitazione, *vedi "**Avvio di RCS Console**" a pagina 8*. |
| 24 Novembre 2014 | Manuale del tecnico 2.0 MAR-2015 | 9.5 | Aggiunto vettore di installazione Persistent Installation per mobile, *vedi "**Vettore Persistent Installation (mobile)**" a pagina 159*.<br>Modificata la procedura di installazione dell'agent per il vettore di installazione Persistent Installation per desktop, *vedi "**Vettore Persistent Installation (desktop)**" a pagina 157*.<br>Aggiunta sezione nella scheda **System Management** in Control Center per configurare l'Anonymizer, definire chiave di autenticazione per il Network Injector e avviare manualmente la sincronizzazione con il server RCS, *vedi "**Tactical Control Center** " a pagina 90* e *"**Appliance Control Center** " a pagina 82*. |

| *Data rilascio* | *Codice* | *Versione software* | *Descrizione* |
|---|---|---|---|
| 20 Settembre 2014 | Manuale del tecnico 1.8 SET-2014 | 9.4 | Aggiunte procedure per installare/disintallare l'agent ed esportare evidence sul computer del target per il vettore Offline Installation, *vedi "**Vettore Offline Installation**" a pagina 156*. |
| 23 Giugno 2014 | Manuale del tecnico 1.7 GIU-2014 | 9.3 | Aggiunta funzione di sblocco password di un sistema operativo su Tactical Control Center, *vedi "**Cose da sapere per lo sblocco della password del sistema operativo**" a pagina 78*, "*Cose da sapere su Tactical Control Center" a pagina 72*.<br>Aggiunta gestione abilitazione regole di identificazione e di infezione tramite Control Center.<br>Aggiunto elenco applicativi di terze parti installati su Network Injector, *vedi "**Altri applicativi installati sui Network Injector**" a pagina 109*.<br>Aggiunto vettore di installazione Persistent Installation, *vedi "**Vettore Persistent Installation (desktop)**" a pagina 157*<br>Aggiornata sezione storico sincronizzazioni dell'agent, *vedi "**Dati dello storico sincronizzazioni dell'agent**" a pagina 40* |

| *Data rilascio* | *Codice* | *Versione software* | *Descrizione* |
|---|---|---|---|
| 19 Febbraio 2014 | Manuale del tecnico 1.6 FEB-2014 | 9.2 | Rimosse informazioni relative ai sistemi operativi che supportano ogni azione, modulo e evento della configurazione avanzata. Se necessario, contattare l'assistenza tecnica.<br>Aggiunto modulo **Money**, *vedi " **Modulo Money** " a pagina 139*.<br>Aggiornata documentazione dei vettori di installazione, *vedi "**Appendice: vettori di installazione**" a pagina 142*.<br>Aggiunto agent di livello soldier, *vedi "**Cose da sapere sugli agent**" a pagina 35*.<br>Aggiunta configurazione accesso remoto agli applicativi sul Tactical Control Center e sull'Applicance Control Center, *vedi " **Tactical Control Center** " a pagina 90*, *"**Cose da sapere per l'accesso remoto al Control Center**" a pagina 79*<br>Aggiunto test di rete su Appliance Control Center, *vedi "**Appliance Control Center** " a pagina 82*.<br>Rimossa la regola INJECT-UPGRADE, *vedi "**Dati delle regole di infezione**" a pagina 64*.<br>Aggiunte cose da sapere per funzione **Wireless Intruder**, *vedi "**Cose da sapere per individuare la password di rete WiFi**" a pagina 77*.<br>Aggiunta descrizione comandi da terminale per applicativi Tactical Control center e Appliance Control Center, *vedi " **Comandi Tactical Control Center e Appliance Control Center**" a pagina 81* |
| 30 Settembre 2013 | Manuale del tecnico 1.5 SET - 2013 | 9 | Aggiunta la piattaforma Windows Phone, *vedi "**Vettore Installation Package**" a pagina 146*<br>Aggiornamento documentazione per gestione privilegi di root per dispositivi Android, *vedi "**Cose da sapere su Android**" a pagina 144*.<br>Aggiornata documentazione gestione Network Injectors, *vedi "**I Network Injector**" a pagina 60*.<br>Aggiornata documentazione per migliorie apportate all'interfaccia utente.<br>Migliorato sommario. |

## Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

| *Manuale* | *Destinatari* | *Codice* | *Formato di distribuzione* |
|---|---|---|---|
| **Manuale dell'amministratore di sistema** | Amministratore di sistema | Manuale dell'amministratore di sistema 1.9 MAR-2015 | PDF |
| **Manuale dell'amministratore** | Amministratori | Manuale dell'amministratore 1.7 MAR-2015 | PDF |
| **Manuale del tecnico (questo manuale)** | Tecnici | Manuale del tecnico 2.0 MAR-2015 | PDF |
| **Manuale dell'analista** | Analisti | Manuale dell'analista 1.9 MAR-2015 | PDF |

## Convenzioni tipografiche per le segnalazioni

Di seguito le segnalazioni previste in questo documento (Microsoft Manual of Style):

**AVVERTENZA: indica una situazione rischiosa che se non evitata, può causare danni fisici all'utente o alle attrezzature.**

***PRUDENZA: indica una situazione rischiosa che se non evitata, può causare la perdita di dati.***

**IMPORTANTE: offre indicazioni essenziali al completamento del compito. Mentre le note possono essere trascurate e non inficiano il completamento del compito, le indicazioni importanti non devono essere trascurate.**

NOTA: informazioni neutre e positive che enfatizzano o aggiungono informazioni a dei punti nel testo principale. Fornisce informazioni che possono essere applicate solo in casi speciali.

Suggerimento: consiglia l'utente nell'applicare le tecniche e le procedure descritte nel testo ai loro bisogni specifici. Può suggerire un metodo alternativo e non è fondamentale alla comprensione del testo.

*Richiede assistenza: l'operazione può essere portata a termine solo su indicazioni dell'assistenza tecnica.*

## Convenzioni tipografiche per la formattazione

Di seguito la legenda di alcune convenzioni tipografiche:

| *Esempio* | *Stile* | *Descrizione* |
|---|---|---|
| *Vedi " **Dati degli utenti**"* | *corsivo* | indica il titolo di un capitolo, una sezione, una sottosezione, un paragrafo, una tabella o una figura di questo manuale, o di un'altra pubblicazione di riferimento. |
| <ggmmaaaa> | <aaa> | indica un testo che dovrà essere specificato dall'utente secondo una certa sintassi. Nell'esempio <ggmmaaaa> è una data e può diventare "14072011". |
| Selezionare uno dei server elencati **[2]**. | **[x]** | indica l'oggetto citato nel testo e che compare nell'immagine adiacente. |
| Fare clic su **Add**.<br>Selezionare il menu **File, Save data.** | **grassetto** | indica una scritta sull'interfaccia operatore, sia di un elemento grafico (es.: tabella, scheda) sia di un pulsante a video. |
| Premere Enter | prima lettera maiuscola | indica il nome di un tasto della tastiera. |
| Cfr.: Network Injector Appliance | - | suggerisce di confrontare la definizione di un termine in glossario o contenuto con altro termine o contenuto. |

## Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS:

| *Destinatario* | *Attività* | *Competenze* |
|---|---|---|
| **Amministratore di sistema** | Segue le indicazioni dell'assistenza HackingTeam fornite in fase contrattuale. Installa e aggiorna i server RCS, i Network Injector e le RCS Console. Programma e gestisce i backup. Ripristina i backup in caso di sostituzione dei server.<br>  **AVVERTENZA: l'amministratore di sistema deve avere tutte le competenze necessarie richieste. HackingTeam non si assume alcuna responsabilità di malfunzionamenti o danni alle attrezzature arrecati da una installazione non professionale.** | Tecnico di reti esperto |

| *Destinatario* | *Attività* | *Competenze* |
|---|---|---|
| **Amministratore** | Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze. | Responsabile dell'indagine |
| **Tecnico** | Crea gli agent e li configura. Configura le regole di un Network Injector. | Tecnico specializzato in intercettazioni |
| **Analista** | Analizza le evidence e le esporta. | Operativo |

## Dati di identificazione dell'autore del software

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
**Tel.**: + 39 02 29 060 603
**Fax**: + 39 02 63 118 946
**e-mail**: info@hackingteam.com

# 2

# RCS Console per il Tecnico

## Presentazione

### Introduzione

RCS (Remote Control System) è una soluzione a supporto delle investigazioni che intercetta attivamente e passivamente dati e informazioni dai dispositivi dei bersagli di tali investigazioni. RCS infatti crea, configura e installa nell'assoluto anonimato degli agenti software che raccolgono dati e informazioni e inviano i risultati al database centrale per la decodifica e il salvataggio.

### Ruolo del Tecnico

Il ruolo del Tecnico è:

- creare delle regole di infezione per ogni Network Injector installato
- creare agent di infezione per i vari dispositivi del target
- mantenere aggiornato il software degli agent

### Funzioni abilitate per il Tecnico

Per completare le attività che gli competono, il Tecnico ha accesso alle seguenti funzioni:

- **Operations**
- **System**

### Contenuti

Questa sezione include i seguenti argomenti:


**Avvio di RCS Console** ..... **8**
**Descrizione della homepage** ..... **9**
**Descrizione dei wizard da homepage** ..... **10**
**Elementi e azioni comuni dell'interfaccia** ..... **11**
**Procedure del Tecnico** ..... **16**

# Avvio di RCS Console

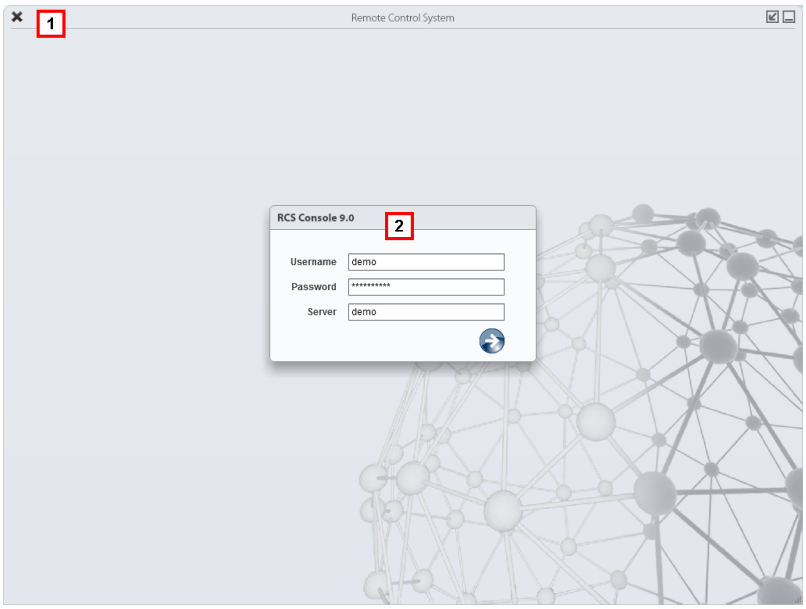
## Introduzione

All'avvio, RCS Console chiede di inserire le proprie credenziali (nome utente e password) precedentemente impostate dall'Amministratore.

**IMPORTANTE: se viene inserita per cinque volte consecutive la password sbagliata, l'utente viene disabilitato automaticamente dal sistema e non può più accedere a RCS Console. Rivolgersi all'Amministratore.**

## Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:




| *Area* | *Descrizione* |
|---|---|
| **1** | Barra del titolo con pulsanti di comando:<br>Chiusura di RCS Console.<br>Pulsante di ingrandimento della finestra.<br>Pulsante di riduzione a icona della finestra. |
| **2** | Finestra di dialogo per inserimento delle proprie credenziali. |

## Accedere a RCS Console

Per accedere alle funzioni di RCS Console:

| *Passo* | *Azione* |
|---|---|
| **1** | In **Username** e **Password** inserire le credenziali come assegnate dall'Amministratore. |
| **2** | In **Server** inserire il nome della macchina o l'indirizzo del server cui ci si vuole collegare. |
| **3** | Fare clic su  : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. *Vedi "**Descrizione della homepage**" nel seguito.* |

# Descrizione della homepage

*Per visualizzare l'homepage:*

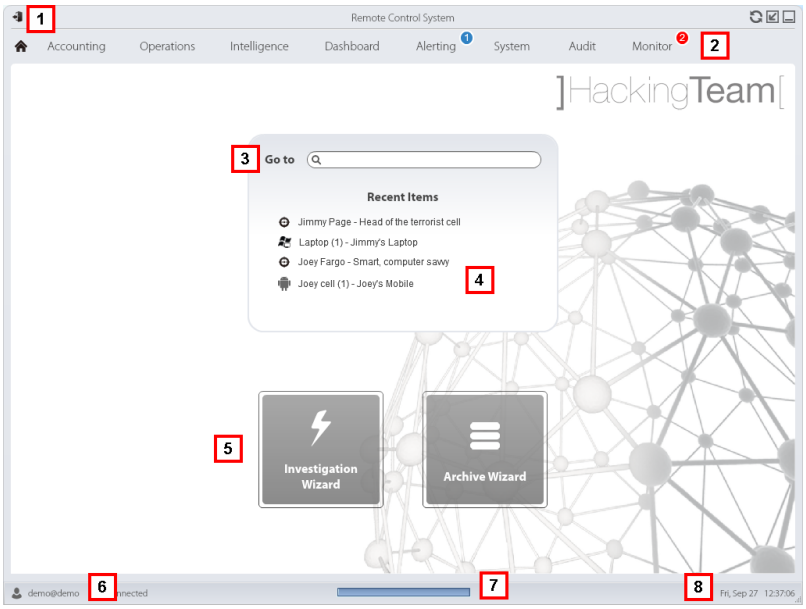
- fare clic su 

## Introduzione

RCS Console presenta all'avvio questa homepage, unica per tutti gli utenti. I menu abilitati dipendono dai ruoli assegnati al proprio account.

## Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia degli argomenti recenti. Per il dettaglio degli elementi e le azioni comuni:




| *Area* | *Descrizione* |
|---|---|
| **1** | Barra del titolo con pulsanti di comando. |

| *Area* | *Descrizione* |
|---|---|
| **2** | Menu di RCS con le funzioni abilitate per l'utente. |
| **3** | Casella di ricerca per cercare tra i nomi di operation, target, agent ed entità, per nome o descrizione. |
| **4** | Collegamenti agli ultimi cinque elementi aperti (operation della sezione **Operations**, operation della sezione **Intelligence**, target, agent ed entità). |
| **5** | Pulsanti per avvio dei wizard. |
| **6** | Utente connesso con la possibilità di cambiare la lingua e la password. |
| **7** | Area download con possibilità durante una esportazione o una compilazione di vedere lo stato di avanzamento. |
| **8** | Data e ora attuale con la possibilità di cambiare il fuso orario. |

# Descrizione dei wizard da homepage

***Per visualizzare l'homepage:***

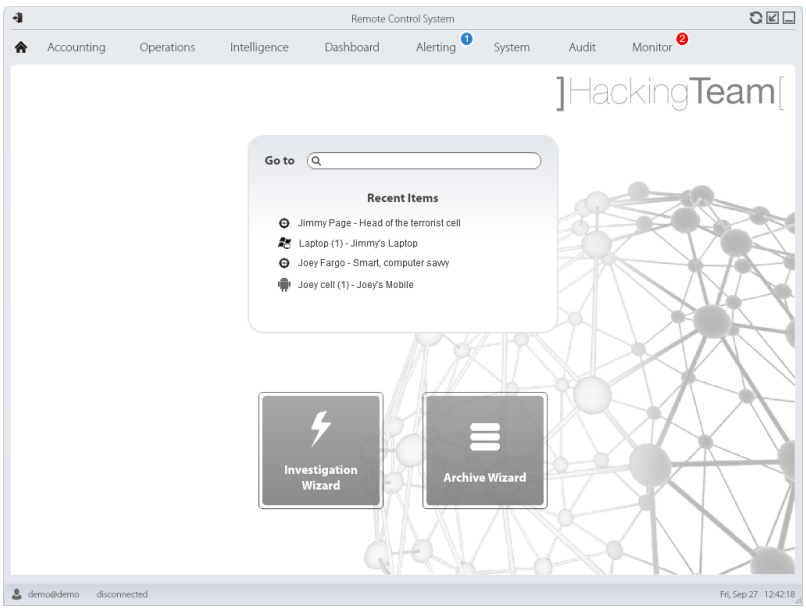
- fare clic su 

## Introduzione

Per utenti con certi privilegi RCS Console presenta dei pulsanti che attivano dei wizard.

## Come si presenta

Ecco come viene visualizzata l'homepage con i wizard abilitati:



| *Pulsante* | *Funzione* |
|---|---|
|   | Apre il wizard per la creazione rapida di un agent.<br>NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico. |
|   | Apre il wizard per l'archiviazione rapida dei dati di operation e target.<br>NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Amministratore di sistema. |

### Investigazione Rapida

Questo wizard crea un agent rapidamente. Il wizard chiede il nome (es.: "SmartSpy") e il tipo di agent che si vuole creare (desktop o mobile) e in sequenza crea:

1. una operation "SmartSpy"
2. un target "SmartSpy"
3. una factory "SmartSpy"
4. un gruppo di utenti "SmartSpy" di cui l'utente attuale è il solo appartenente

e porta direttamente alla pagina della configurazione della factory. *Vedi "**Configurazione base di una factory o di un agent**" a pagina 46*

A questa operation, target o gruppo di utenti è possibile aggiungere altri elementi semplicemente agendo nelle pagine di dettaglio.

# Elementi e azioni comuni dell'interfaccia

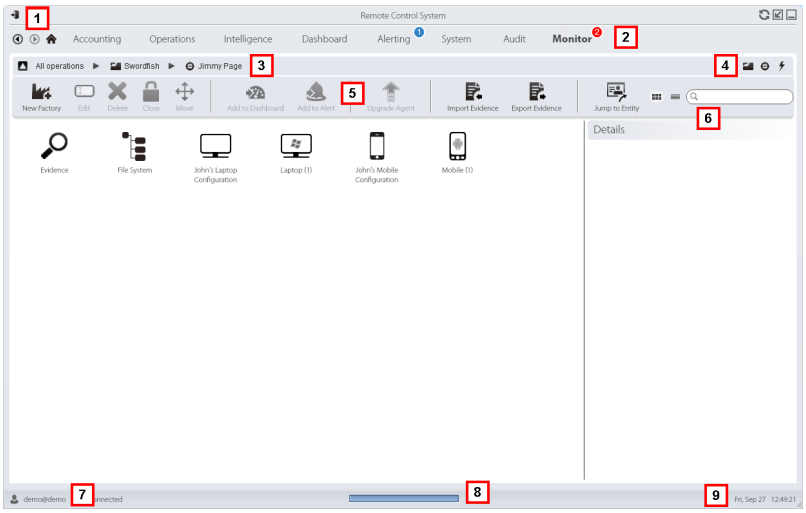
### Introduzione

Ogni pagina del programma utilizza elementi comuni e permette azioni simili tra loro.

Per facilitare la consultazione di questo manuale, sono stati descritti in questo capitolo elementi e azioni comuni ad alcune funzioni.

### Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console. In questo esempio mostriamo la pagina di un target:




| *Area* | *Descrizione* |
|---|---|
| **1** | Barra del titolo con pulsanti di comando:<br>Logout da RCS.<br>Pulsante di aggiornamento della pagina.<br>Pulsante di ingrandimento della finestra.<br>Pulsante di riduzione a icona della finestra. |
| **2** | Pulsante per tornare indietro nella cronologia di navigazione<br>Pulsante per andare avanti nella cronologia di navigazione<br>Pulsante per tornare alla homepage<br>Menu di RCS con le funzioni abilitate per l'utente |
| **3** | Barra di navigazione per l'operation. Di seguito la descrizione:<br>Torna al livello superiore.<br>Mostra la pagina dell'operation (sezione **Operations**).<br>Mostra la pagina del target.<br>Mostra la pagina della factory.<br>Mostra la pagina dell'agent.<br>Mostra la pagina dell'operation (sezione **Intelligence**).<br>Mostra la pagina dell'entità. |

| *Area* | *Descrizione* |
|---|---|
| **4** | Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:<br>  Mostra tutte le operation.<br>  Mostra tutti i target.<br>  Mostra tutti gli agent.<br>  Mostra tutte le entità. |
| **5** | Barre con i pulsanti della finestra. |
| **6** | Pulsanti e casella di ricerca:<br>  Casella di ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite.<br>  Visualizza gli elementi in una tabella.<br>  Visualizza gli elementi come icone. |
| **7** | Utente connesso con possibilità di cambiare la lingua e la password. |
| **8** | Area download con possibilità durante una esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download.<br>• Barra superiore: percentuale di generazione sul server.<br>• Barra inferiore: percentuale di download dal server su RCS Console. |
| **9** | Data e ora attuale con la possibilità di cambiare il fuso orario. |

## Cambiare la lingua dell'interfaccia o la propria password

Per cambiare la lingua dell'interfaccia o la propria password:

| *Passo* | *Azione* |
|---|---|
| **1** | Fare clic su **[7]**: compare una finestra di dialogo con i dati dell'utente. |
| **2** | Cambiare lingua o password e fare clic su **Salva** per confermare e uscire. |

## Convertire le date-ora di RCS Console al proprio fuso orario

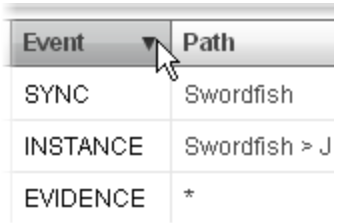
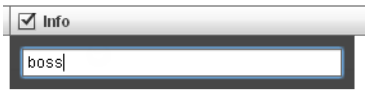
Per convertire tutte le date-ora al proprio fuso orario:

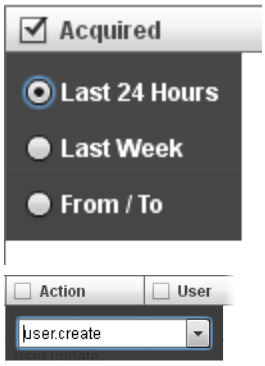
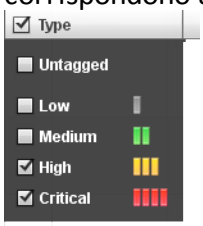
| *Passo* | *Azione* |
|---|---|
| **1** | Fare clic su **[9]**: compare una finestra di dialogo con la data-ora attuale.<br>**Ora UTC**: data-ora di Greenwitch (GMT)<br>**Ora Locale**: data-ora dove è installato il server RCS<br>**Ora Console**: data-ora della console da cui si sta lavorando e che può essere convertita |
| **2** | Cambiare il fuso orario e fare clic su **Salva** per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto. |

## Azioni sulle tabelle

RCS Console mostra diversi dati in forma di tabella. Le tabelle permettono di:

- ordinare i dati per colonna in ordine crescente/decrescente
- filtrare i dati per ogni colonna

| *Azione* | *Descrizione* |
|---|---|
| **Ordinare per colonna** | Fare clic sull'intestazione per ottenere l'ordine per quella colonna, crescente o decrescente.<br>  |
| **Filtrare un testo** | Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.<br>  <br>L'esempio mostra elementi con descrizioni tipo:<br>• "my**boss**"<br>• "**boss**anova" |

| *Azione* | *Descrizione* |
|---|---|
| **Filtrare in base a una opzione** | Selezionare una opzione: compaiono gli elementi che corrispondono all'opzione scelta.<br>  |
| **Filtrare in base a più opzioni** | Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte.<br>  |
| **Cambiare la dimensione delle colonne** | Selezionare il bordo della colonna e trascinarlo. |

# Procedure del Tecnico

## Introduzione

Il Tecnico deve occuparsi delle regole di infezione per il recupero di informazioni importanti. Di seguito la descrizione di alcune procedure tipiche con il rimando ai capitoli importanti. Si tratta solo di semplici indicazioni. È fondamentale la competenza e la capacità di sfruttare la flessibilità di RCS per adattarlo alle esigenze dell'indagine.

## Effettuare l'infezione su connessioni HTTP

Per effettuare l'infezione su connessioni HTTP è necessario utilizzare Network Injector:

| *Passo* | *Azione* |
|---|---|
| **1** | Nella sezione **System**, **Network Injectors** creare le regole di identificazione e infezione per Network Injector Appliance e Tactical Network Injector.<br>*Vedi "**Gestione dei Network Injector**" a pagina 62*<br>  NOTA: non è richiesta l'installazione di alcun agent. |
| **2** | Nel caso di utilizzo del Network Injector Appliance, il sistema applica le regole di identificazione sul traffico dati. Una volta trovati i dispositivi target li infetta con le regole di infezione.<br>Oppure nel caso di utilizzo del Tactical Network Injector si potrà operare sia con identificazione e infezione automatica sia tramite operatore.<br>*Vedi "**Tactical Control Center** " a pagina 90.* |

## Infettare un computer non connesso a internet

Per infettare un computer non connesso a Internet.

| *Passo* | *Azione* |
|---|---|
| **1** | Creare una factory disabilitando la sincronizzazione a livello di operation, *vedi "**Pagina dell'operation**" a pagina 21*.<br>Oppure creare una factory a livello di target, sempre senza sincronizzazione, *vedi "**Pagina del target**" a pagina 25* |
| **2** | Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e al metodo di installazione, quindi creare l'agent.<br>*Vedi "**Compilazione di una factory**" a pagina 31.* |
| **3** | Installare l'agent presso il dispositivo del target nelle modalità scelte.<br>*Vedi "**Elenco dei vettori di installazione**" a pagina 143.* |

| Passo | Azione |
|---|---|
| 4 | Dopo il tempo necessario recuperare le evidence prodotte sul dispositivo del target. |
| 5 | Importare le evidence dell'agent e analizzarle.<br>*Vedi "**Pagina dell'agent**" a pagina 38.* |

## Infettare un computer connesso a Internet

Per infettare un computer connesso a Internet.

Suggerimento: questi passaggi sono fondamentali quando non si conoscono sin dall'inizio le attività del target da registrare, oppure si vuole evitare di registrare una quantità eccessiva di dati.

| Passo | Azione |
|---|---|
| 1 | Creare una factory: il sistema abilita automaticamente la sincronizzazione.<br>*Vedi "**Pagina dell'operation**" a pagina 21* |
| 2 | Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e al metodo di installazione, quindi creare l'agent.<br>*Vedi "**Compilazione di una factory**" a pagina 31.* |
| 3 | Installare l'agent presso il dispositivo del target nelle modalità scelte.<br>*Vedi "**Elenco dei vettori di installazione**" a pagina 143.* |
| 4 | Alla prima sincronizzazione l'agent compare nella pagina del target.<br>*Vedi "**Pagina del target**" a pagina 25* |
| 5 | Riconfigurare l'agent utilizzando la configurazione base o avanzata. Alla successiva sincronizzazione l'agent applica la nuova configurazione.<br>*Vedi "**Configurazione base di una factory o di un agent**" a pagina 46*<br>*Vedi "**Configurazione avanzata di una factory o di un agent**" a pagina 55.* |

## Mantenere aggiornato il software degli agent

Ciclicamente HackigTeam aggiorna il suo software. Per aggiornare agent già installati:

| Passo | Azione |
|---|---|
| 1 | • Nella sezione **Operations**, **Target** aggiornare gli agent. *Vedi "**Pagina del target**" a pagina 25*<br><br>oppure<br>• Nella sezione **Operations**, **Target** entrare in un agent e aggiornarlo. *Vedi "**Pagina dell'agent**" a pagina 38.* |

# 3

# Operation e target

## Presentazione

### Introduzione

La gestione delle operation stabilisce i target da sottoporre a intercettazione.

### Contenuti

Questa sezione include i seguenti argomenti:


**Cose da sapere sulle operation** ..... **19**
**Cose da sapere sui target** ..... **19**
**Gestione delle operation** ..... **19**
**Pagina dell'operation** ..... **21**

# Cose da sapere sulle operation

## Cos'è un'operation

L'operation rappresenta l'indagine da eseguire. Un'operation contiene uno o più target, ovvero le persone fisiche da intercettare. Il Tecnico assegna al target uno o più agent di tipo *desktop* o *mobile*. Così l'agent può essere installato su un computer o su un dispositivo mobile.

# Cose da sapere sui target

## Cos'è un target

Il target rappresenta la persona fisica da investigare. Il Tecnico assegna al target uno o più agent di tipo desktop o mobile. Così l'agent può essere installato su un computer o su un dispositivo mobile.

# Gestione delle operation

| | |
|---|---|
| ***Per gestire le operation:*** | • sezione **Operations** |

## Scopo

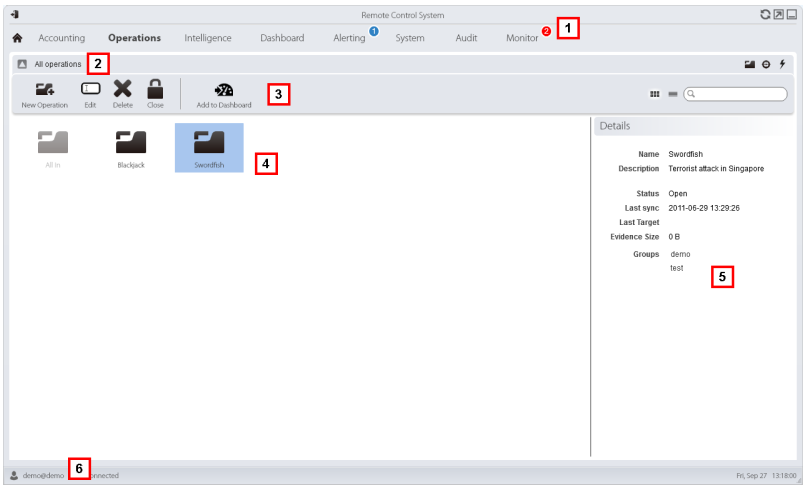
Questa funzione permette di:

- visualizzare e gestire i target associati a una operation

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione operation**.

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |
| **3** | Barre con i pulsanti della finestra. |
| **4** | Elenco delle operation create:<br>  Operation aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, si ricevono le evidence raccolte.<br>  Operation chiusa. Tutti i target sono chiusi e gli agent disinstallati. È comunque possibile vedere tutti i suoi target e tutte le sue evidence. |
| **5** | Dati dell'operation selezionata. |
| **6** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati delle operation**" alla pagina successiva*.

Per saperne di più sulle operation *vedi "**Cose da sapere sulle operation**" alla pagina precedente*.

## Visualizzare i target di un'operation

Per visualizzare i target di un'operation:

| *Passo* | *Azione* |
|---|---|
| 1 | Fare doppio clic su un'operation: si apre la pagina per la gestione dei target. *Vedi "**Pagina dell'operation**" nel seguito* |

### Dati delle operation

Di seguito la descrizione dei dati dell'operation selezionata:

| *Dato* | *Descrizione* |
|---|---|
| **Nome** | Nome dell'operation. |
| **Descrizione** | Descrizione libera. |
| **Contatto** | Campo descrittivo per definire, ad esempio, il nome di un referente (Giudice, Magistrato, e così via). |
| **Stato** | Stato di un'operation e comando di chiusura:<br>**Open**: l'operation è aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, RCS riceve le evidence raccolte.<br>**Closed**: l'operation è chiusa, senza più possibilità di riaprirla. Gli agent non inviano più i dati, ma è possibile consultare le evidence già ricevute. |
| **Gruppi** | Gruppi abilitati a visualizzare l'operation. |

# Pagina dell'operation

*Per entrare in una operation:* • sezione **Operations**, doppio-clic su una operation

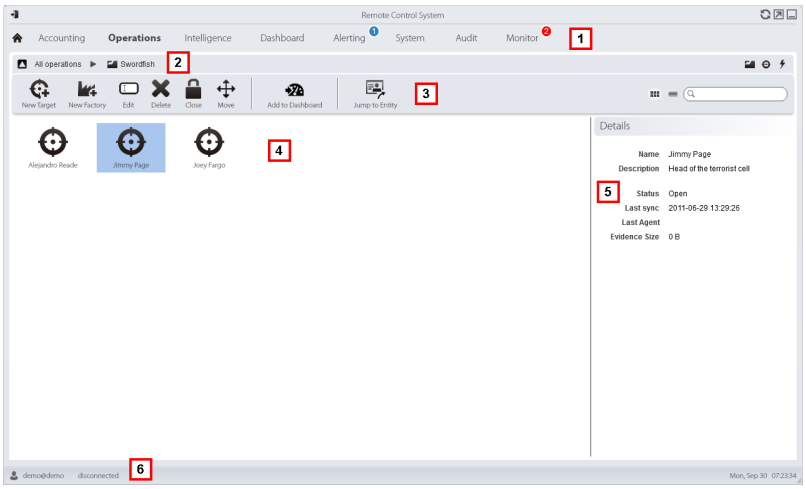
### Scopo

Questa funzione permette di:

- gestire le factory, che compilate, diventeranno agent da installare sui dispositivi*vedi "**Configurazione avanzata di una factory o di un agent**" a pagina 55*

### Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |
| **3** | Barre con i pulsanti della finestra. Di seguito la descrizione:<br>  Crea una factory.<br>  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Creazione factory.** È possibile creare una factory anche a livello di target, ***vedi "Pagina dell'operation" alla pagina precedente*.** |
| **4** | Elenco dei target:<br>  target aperto<br>  target chiuso |
| **5** | Dati del target selezionato. |
| **6** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *vedi "Elementi e azioni comuni dell'interfaccia" a pagina 11*.

Per saperne di più sulle operation *vedi "Cose da sapere sulle operation" a pagina 19*.

Per saperne di più sulle factory *vedi "Cose da sapere sulle Factory e sugli Agent" a pagina 29*.

Per la descrizione dei dati presenti sulla finestra *vedi "Dati della pagina di un'operation" alla pagina successiva*.

Per gestire rapidamente i dati di un'operation *vedi "Descrizione dei wizard da homepage" a pagina 10*.

## Creare una factory

Per creare una factory:

| *Passo* | *Azione* |
|---|---|
| **1** | • Fare clic su **Nuova Factory**: compaiono i dati da compilare.<br>• Inserire il nome e la descrizione e in **Tipo** selezionare il tipo di dispositivo. |
| **2** | Fare clic su **Salva**: nell'area di lavoro principale compare la nuova factory con il nome scelto. |

## Dati della pagina di un'operation

Di seguito la descrizione dei dati del target selezionato:

| *Dato* | *Descrizione* |
|---|---|
| **Nome** | Nome del target. |
| **Descriztione** | Descrizione libera. |
| **Stato** | Definisce lo stato di un target:<br>  Aperto. Se il Tecnico ha installato correttamente gli agent, RCS riceve le evidence raccolte.<br>  Chiuso. Chiuso senza più possibilità di riaprirlo. |

# 4

# I target

## Presentazione

### Introduzione

Un target è una persona fisica da sottoporre a monitoraggio. Possono essere utilizzati più agent, uno per ogni dispositivo posseduto dal target.

### Contenuti

Questa sezione include i seguenti argomenti:


**Pagina del target** ..... **25**
**Cose da sapere sulle Factory e sugli Agent** ..... **29**
**Compilazione di una factory** ..... **31**

# Pagina del target

| | |
|---|---|
| *Per entrare in un target* | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target |

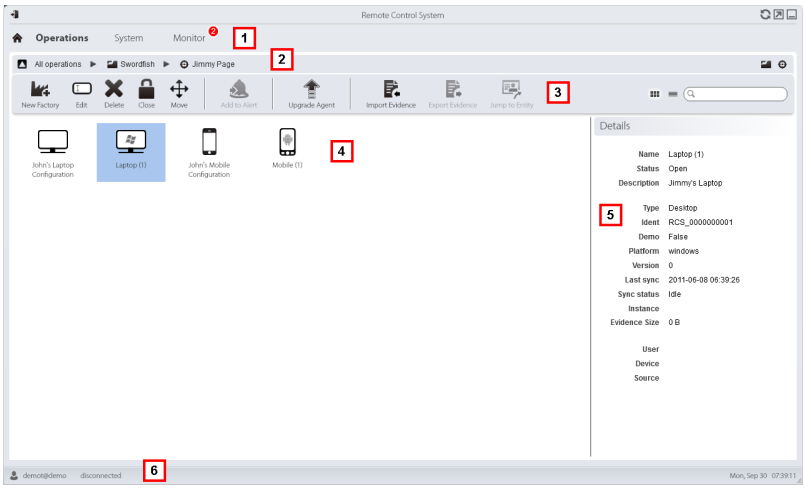
## Scopo

Questa funzione permette di:

- gestire le factory, che compilate, diventeranno agent da installare sul dispositivo del target.
- aprire una factory per la configurazione base (*vedi "Configurazione base di una factory o di un agent" a pagina 46*) o per la configurazione avanzata (*vedi "Configurazione avanzata di una factory o di un agent" a pagina 55*)
- importare le evidence del target
- entrare in un agent installato
- aggiornare il software dell'agent

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |

| *Area* | *Descrizione* |
|---|---|
| **3** | Barre con i pulsanti della finestra. Di seguito la descrizione:<br>  Crea una factory.<br>  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Creazione Factory**.<br>È possibile creare una factory anche a livello di operation, *vedi "Pagina dell'operation" a pagina 21*.<br>  Modifica una factory o un agent.<br>  Eliminare una factory o un agent.<br>  Chiude l'agent ola factory.<br>  Sposta la factory o l'agent in un altro target.<br>  Aggiorna il software di tutti gli agent con l'ultima versione ricevuta dall'assistenza HackingTeam.<br>  ***PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene trasmessa agli agent alla successiva sincronizzazione.***<br>  **IMPORTANTE: per Android, per aggiornare l'agent è necessario ottenere i privilegi di root. *Vedi "Cose da sapere su Android" a pagina 144*.**<br>  Importa le evidence del target raccolte fisicamente sul dispositivo.<br>NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Importa evidence**. |
| **4** | Icone/elenco delle factory create e degli agent installati.<br>  Agent in modalità demo.<br>  Agent scout in attesa di verifica.<br>  Agent soldier installato.<br>  Agent elite installato. |
| **5** | Dati della factory o dell'agent selezionato. |
| **6** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *vedi "Elementi e azioni comuni dell'interfaccia" a pagina 11*.

Per la descrizione dei dati presenti sulla finestra *vedi "Dati della pagina target" a pagina 28*.

Per saperne di più sui target *vedi "Cose da sapere sulle Factory e sugli Agent" a pagina 29*
Per gestire rapidamente i dati di un target *vedi "Descrizione dei wizard da homepage" a pagina 10*.

## Creare una factory

Per creare una factory:

| *Passo* | *Azione* |
|---|---|
| **1** | • Fare clic su **Nuova Factory**: compaiono i dati da compilare.<br>• Inserire il nome e la descrizione e in **Tipo** selezionare il tipo di dispositivo. |
| **2** | Fare clic su **Salva**: nell'area di lavoro principale compare la nuova factory con il nome scelto. |

## Chiudere una factory o un agent

Per chiudere una factory o un agent:

| *Passo* | *Azione* |
|---|---|
| **1** | Selezionare una factory o un agent e fare clic su **Chiudi.** |
| **2** | Confermare la chiusura.<br>***PRUDENZA: chiudere un agent è un'azione irreversibile che ne provoca la sua disinstallazione alla prima sincronizzazione. Chiudere una factory, invece, non la rende più accessibile. Gli agent attivi resteranno comunque accessibili mentre tutti gli agent che non hanno effettuato almeno una sincronizzazione prima della chiusura della factory saranno disinstallati.*** |

## Eliminare una factory o un agent

Per eliminare una factory o un agent:

| *Passo* | *Azione* |
|---|---|
| **1** | Selezionare una factory o un agent, quindi fare clic su **Cancella**.<br>Confermare l'azione: sono eliminati gli storici, le configurazioni, le evidence.<br>***PRUDENZA: l'operazione è irreversibile.*** |

## Importare le evidence del target

Per importare le evidence:

| *Passo* | *Azione* |
|---|---|
| **1** | Fare clic su **Importa Evidence**: si apre la finestra di importazione.<br>Fare clic su **Seleziona Cartella** e selezionare la cartella dove il file offline.ini è salvato |
| **2** | Fare clic su **Importa**: le evidence sono salvate nel database e disponibili per la visualizzazione da parte degli Analisti. |

## Dati della pagina target

### Introduzione

| | |
|---|---|
| *Per visualizzare i dati della pagina:* | • Sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **Vista a icone** o **Vista a tabella** |

Gli elementi della pagina possono essere visualizzati a icone o a tabella.

### Visualizzazione a icone

Di seguito la descrizione delle icone:

| *Dato* | *Descrizione* |
|---|---|
|  | Factory di tipo desktop in stato aperto. |
|  | Esempio di agent scout per dispositivo desktop Windows, in stato aperto. |
|  | Esempio di agent soldier per dispositivo desktop Windows, in stato aperto. |
|  | Esempio di agent elite per dispositivo desktop Windows, in stato aperto. |
|  | NOTA: factory e agent in stato chiuso hanno l'icona di colore grigio chiaro. Questa è l'icona di un agent mobile per Android in stato chiuso:  . |
|  | NOTA: agent in stato chiuso hanno l'icona di colore grigio chiaro. Questa è l'icona di un agent mobile per Android in stato chiuso:  . |

### Visualizzazione a tabella

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Nome** | Nome della factory o dell'agent. |

| *Dato* | *Descrizione* |
|---|---|
| **Descrizione** | Descrizione della factory o dell'agent. |
| **Stato** | **Open**: una factory aperta può essere compilata per creare più agent. Un agent aperto può essere installato, è funzionante e registra evidence.<br>**Closed**: una factory o un agent chiusi non possono essere più aperti. I dati presenti in RCS sono ancora consultabili. |
| **Tipo** | Tipologia desktop o mobile. |
| **Livello** | (solo agent) Livello dell'agent: scout, soldier, elite. |
| **Piattaforma** | (solo agent) Sistema operativo su cui l'agent si è installato. |
| **Versione** | (solo agent) Versione dell'agent. A ogni nuova configurazione viene creata una nuova versione. |
| **Ultima sync** | (solo agent) Data e ora dell'ultima sincronizzazione dell'agent. |
| **Ident** | (solo agent) Identificativo univoco di un agent. |
| **Istanza** | (solo agent) Identificativo univoco del dispositivo su cui l'agent è installato. |

# Cose da sapere sulle Factory e sugli Agent

## Modalità di infezione

È possibile infettare un dispositivo tramite:

- **infezione fisica**: il dispositivo viene infettato tramite l'esecuzione di un file trasferito da memorie USB, CD o documenti. Le evidence possono essere raccolte fisicamente o via Internet non appena il dispositivo si connette.
- **infezione da remoto**: il dispositivo viene infettato dall'esecuzione di un file trasferito via connessione Internet o reso disponibile in una risorsa Web. Le evidence possono essere raccolte fisicamente o via Internet non appena il dispositivo si connette. L'infezione da remoto può essere potenziata tramite l'utilizzo di un Network Injector.

## Componenti della strategia di infezione

I componenti richiesti per una corretta infezione sono:

- **Factory**: modello di un agent.
- **Vettori di installazione**: canali di infezione.
- **Agent**: il software da installare sul dispositivo del target.
- **Target e operation***:* definiti in fase di apertura dell'indagine da chi ha il ruolo di

Amministratore di sistema. Fare riferimento al Manuale dell'Amministratore di sistema.

- **Evidence**: le registrazioni da raccogliere

## Le factory

La *factory* è un modello da cui creare un agent da installare. L'icona che la rappresenta è diversa in base al tipo di dispositivo cui l'agent è destinato:

-  : factory per agent desktop
-  : factory per agent mobile

Nella factory devono essere configurati:

- i *dati* da acquisire (configurazione base) oppure i *moduli* da attivare dinamicamente (configurazione avanzata)
- i *vettori di installazione* (es.: CD, exploit, Network Injector)

Suggerimento: è possibile salvare una configurazione come template per caricarla alla successiva creazione di un agent simile.

Suggerimento: una factory può essere usata per creare più agent, per esempio da installare tramite vettori di installazione diversi (es.: due computer con sistemi operativi diversi).

## Modalità di creazione delle factory

Le factory sono dei modelli che possono essere creati a due livelli della gerarchia operation-target-agent:

- *a livello di operation*: la factory, dopo la sua installazione e la prima sincronizzazione, crea automaticamente per ogni dispositivo un agent e un target
- *a livello di target*: la factory, dopo la sua installazione e la prima sincronizzazione, crea automaticamente un agent per quel target

La modalità a *livello di operation* garantisce l'assegnazione separata delle evidence raccolte. Infatti crea tanti agent quanti sono i dispositivi. Successivamente, se due o più dispositivi appartengono allo stesso target, sarà possibile spostare l'agent nel target giusto.

La modalità a *livello di target*, se erroneamente usata, rischia di creare una factory utilizzata per la creazione di più agent.

## I vettori di installazione

I vettori di installazione sono scelti durante la compilazione e definiscono la modalità di installazione, fisica o remota, di un agent. Durante la compilazione i vettori di installazione disponibili possono variare in base al sistema operativo del dispositivo.

È possibile utilizzare più vettori di installazione per uno stesso agent.

NOTA: per effettuare l'infezione su connessioni HTTP vengono utilizzate le regole di infezione.*Vedi "**Gestione dei Network Injector**" a pagina 62*

### Gli agent

Un *agent* è il risultato della compilazione di una factory con uno o più vettori di installazione. Un agent è pronto per essere installato sul dispositivo.

La configurazione base definisce il tipo di dati da acquisire, mentre la configurazione avanzata consente di attivare o disattivare i moduli in maniera dinamica ed autonoma.

Per i tipi di moduli disponibili nella configurazione base e avanzata *vedi "**Elenco dei moduli**" a pagina 130*

Per saperne di più sugli agent *vedi "**Cose da sapere sugli agent**" a pagina 35*.

### I moduli per l'acquisizione dei dati

I moduli determinano alcune attività sul dispositivo del target, in massima parte acquisizione dati. Sono abilitati e configurati nella configurazione base (solo alcuni) o nella configurazione avanzata.

I tipi di moduli disponibili dipendono anche dal tipo di dispositivo.

Per l'elenco completo *vedi "**Elenco dei moduli**" a pagina 130*.

## Compilazione di una factory

| | |
|---|---|
| ***Per compilare una factory:*** | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory, fare clic su **Crea**<br>• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory, fare clic su **Config Avanzata** , **Crea** |

### Scopo

Questa funzione permette di creare uno o più agent (effettivi o da collaudare in modalità demo) in base ai vettori di installazione e alle piattaforme scelte.

NOTA: per la descrizione dettagliata di ogni vettore di installazione *vedi "**Elenco dei vettori di installazione**" a pagina 143*

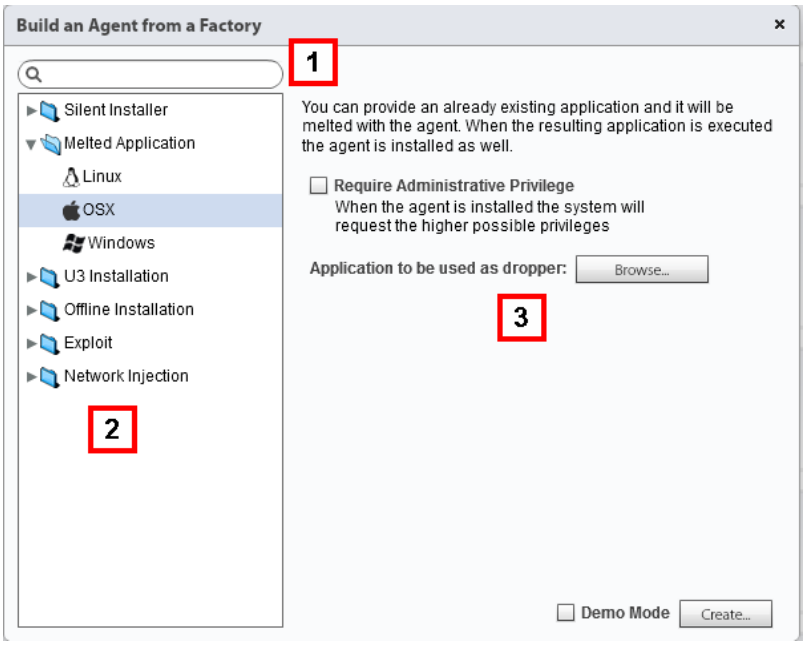
NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Creazione vettori di infezione**.

### Passi successivi

La creazione di un agent implica la successiva installazione sul dispositivo del target.

### Come si presenta la funzione

Ecco come viene visualizzata la pagina per un agent desktop:




| *Area* | *Descrizione* |
|---|---|
| **1** | Casella di ricerca dei vettori di installazione e piattaforme. |
| **2** | Visualizzazione ad albero dei vettori e delle piattaforme. |
| **3** | Area per l'inserimento dei parametri di compilazione dei vettori scelti. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per saperne di più sulle factory *vedi "**Cose da sapere sulle Factory e sugli Agent**" a pagina 29*.

Per la descrizione dettagliata di ogni vettore di installazione *vedi "**Elenco dei vettori di installazione**" a pagina 143*

## Creare un agent

Per creare un agent:

| *Passo* | *Azione* |
|---|---|
| **1** | Selezionare uno o più vettori di installazione e impostare le opzioni richieste. |
| **2** | Fare clic su **Crea**: viene creato un file ZIP o ISO e scaricato nella cartella RCS Download, pronto per essere installato sul dispositivo. |

## Creare un agent da collaudare in modalità demo

**IMPORTANTE: utilizzare questa opzione solo per collaudi effettuati su dispositivi interni. Gli agent in modalità demo non sono invisibili e la presenza di RCS non viene quindi nascosta.**

Per creare un agent a scopo di collaudo:

| *Passo* | *Azione* |
|---|---|
| **1** | Selezionare uno o più vettori di installazione e impostare le opzioni richieste. |
| **2** | Selezionare la casella di controllo **Modalità Demo**. |
| **3** | Fare clic su **Crea**: l'agent installato sul dispositivo mostrerà la sua presenza con messaggi sonori e video. |

# 5

# Gli agent

## Presentazione

### Introduzione

Gli agent acquisiscono dati dal dispositivo su cui sono installati e li inviano ai Collector di RCS. La loro configurazione e il loro software possono essere aggiornati e possono essere trasferiti file in modo assolutamente invisibile dal/al target.

### Contenuti

Questa sezione include i seguenti argomenti:


**Cose da sapere sugli agent** ..... **35**
**Pagina dell'agent** ..... **38**
**Pagina dei comandi** ..... **41**
**Trasferimento file da/a il target** ..... **42**

# Cose da sapere sugli agent

## Introduzione

L'agent può essere esposto e identificato se viene installato in ambienti con antivirus o in ambienti gestiti da personale tecnicamente esperto.

Per evitare che questo accada sono stati previsti tre livelli diversi di agent:

- scout
- soldier
- elite

L'*agent scout* è in realtà un sostituto dell'agent inviato all'inizio della fase di installazione con lo scopo di analizzare il livello di sicurezza del dispositivo del target.

L'*agent soldier* e l'*agent elite* sono agent veri e propri. L'*agent soldier* viene installato in ambienti non completamente sicuri e quindi permette di raccogliere solo alcune tipi di evidence. L'*agent elite* viene installato in ambienti sicuri e può raccogliere tutti i tipi di evidence disponibili.

## Processo di installazione di un agent

| *Fase* | *Descrizione* |
|---|---|
| **1** | Il Tecnico installa l'agent scout sul dispositivo del target. |
| **2** | L'agent scout raccoglie le evidence dal dispositivo per verificarne il livello di sicurezza. |
| **3** | Il Tecnico aggiorna l'agent: |

| *Se l'ambiente è...* | *Allora...* |
|---|---|
| sicuro | il sistema installa l'agent elite. |
| non completamente sicuro | il sistema installa l'agent soldier. |
| non sicuro | non è possibile aggiornare l'agent. |

## Icone degli agent

L'icona di un agent riporta le seguenti informazioni:

- livello (scout, soldier, elite)
- tipo di dispositivo (desktop o mobile)
- sistema operativo su cui è installato

Di seguito sono riportate le icone dei tre livelli di agent, a titolo di esempio per un dispositivo desktop Windows:

-  : scout
-  : soldier
-  : elite

## Agent scout

Una volta installato, alla prima sincronizzazione l'agent scout compare nella pagina del target.
Lo scout agent acquisisce evidence:

- di tipo **Screenshot** utili a identificare il dispositivo del target
- di tipo **Device** utili a capire se l'ambiente da infettare è tranquillo oppure se contiene applicazioni rischiose per l'integrità dell'agent.

**IMPORTANTE: Le evidence di tipo screenshot vengono raccolte solo se il modulo è attivo nella configurazione. Se necessario, ricordarsi di abilitarlo prima di inviare l'agent.**

## Agent soldier

L'agent soldier permette di raccogliere le evidence definite dai moduli della configurazione base tranne i moduli **Call** e **Accessed file**.

**IMPORTANTE: la configurazione avanzata non è abilitata per gli agent soldier.**

Suggerimento: una volta che l'agent soldier è installato, verificare la configurazione definita in fase iniziale per assicurarsi che risponda alle necessità dell'indagine e alle caratteristiche dell'agent.

## Agent elite

L'agent elite permette di raccogliere tutti i tipi di evidence, utilizzando sia la configurazione base che quella avanzata.

## Sincronizzazione di un agent

Un agent si sincronizza solo se:

- la sincronizzazione è abilitata nella configurazione base.
- nella configurazione avanzata è stata aggiunta un'azione di tipo **Synchronize**.

## Agent offline e online

L'agent si comporta diversamente in base alla disponibilità di una connessione a Internet:

| *Se la connessione a Internet è...* | *Allora...* |
|---|---|
| non disponibile | se l'agent ha già dei moduli abilitati inizia a registrare i dati internamente al dispositivo. |
| disponibile | se l'agent ha effettuato la prima sincronizzazione è possibile:<br>• cambiare configurazione, per esempio man mano che le richieste di registrazioni si fanno più specifiche per quel dispositivo. La riconfigurazione dell'agent non modifica la configurazione della factory<br>• aggiornare il suo software<br>• trasferire dei file da e verso il dispositivo<br>• analizzare le evidence che sono state già inviate<br><br>Suggerimento: iniziare creando un agent e abilitando solo la sincronizzazione e il modulo del dispositivo. Quindi, una volta che l'agent è installato e alla ricezione della prima sincronizzazione, abilitare gradualmente gli altri moduli in base alle capacità del dispositivo e al tipo di evidence che si vogliono raccogliere. |

## Disabilitazione temporanea di un agent

È possibile sospendere temporaneamente le attività di un agent senza disinstallarlo, semplicemente disabilitando tutti i moduli e lasciando attiva solo la sincronizzazione.

## Collaudo di un agent

Per testare una configurazione prima di usarla, creare un agent in modalità Demo (*vedi "**Compilazione di una factory**" a pagina 31*).

L'agent viene creato in versione *demo* comportandosi in base alla configurazione impostata, con la sola differenza che segnala in modo evidente (con segnalazioni audio, led e messaggi a video) la sua presenza sul dispositivo. Le segnalazioni permettono di identificare facilmente il dispositivo infettato usato per il test.

NOTA: eventuali non ricezioni di evidence da un agent in modalità demo possono essere dovute a una errata configurazione del server, oppure all'impossibilità di raggiungere l'indirizzo del Collector impostato (es.: per problemi nella configurazione di rete).

## Configurazione dell'agent

La configurazione di un agent (base o avanzata) può essere modificata più volte. A ogni salvataggio viene creata una copia della configurazione e viene salvata nello storico configurazioni.

Alla successiva sincronizzazione, l'agent riceverà la nuova configurazione (**Ora di invio**) e comunicherà l'avvenuta installazione (**Attivato**). Da quel momento eventuali modifiche saranno possibili solo salvando una nuova versione della configurazione.

NOTA: Se **Ora di invio** e **Attivato** non sono ancora valorizzati, è possibile ancora modificare la configurazione corrente.

Per la descrizione dello storico delle configurazioni degli agent *vedi "**Dati dello storico configurazioni di un agent**" a pagina 40.*

# Pagina dell'agent

| | |
|---|---|
| ***Per gestire gli agent:*** | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent |

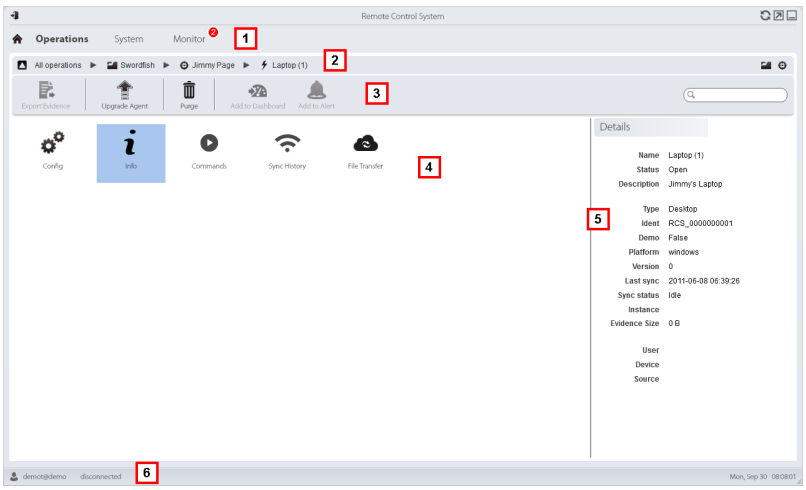
## Scopo

Questa funzione permette di:

- verificare lo storico delle configurazioni dell'agent ed entrare nel dettaglio di ogni configurazione.
- trasferire file dal/al dispositivo del target
- importare/esportare le evidence dell'agent
- sostituire l'agent scout con il vero agent (elite o soldier) e aggiornare il software dell'agent
- visualizzare i comandi eseguiti dall'agent
- visualizzare la cronologia delle sincronizzazioni dell'agent

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:



| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |
| **3** | Barre con i pulsanti della finestra.<br>Di seguito la descrizione:<br>  Invia all'agent scout l'agent vero e proprio (elite o soldier), oppure aggiorna il software dell'agent con l'ultima versione ricevuta dall'assistenza HackingTeam.<br>  ***PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene trasmessa agli agent alla successiva sincronizzazione.***<br>  **IMPORTANTE: per Android, per aggiornare l'agent è necessario ottenere i privilegi di root.** ***Vedi "Cose da sapere su Android" a pagina 144.***<br>  Elimina le evidence sul dispositivo non ancora trasferite a RCS.<br>Parametri:<br>• **Data**: elimina le evidence registrate in data antecedente a quella impostata.<br>• **Dimensione**: elimina le evidence con dimensione maggiore di quella impostata. |
| **4** | Azioni possibili sull'agent. Di seguito la descrizione:<br>  Mostra lo storico delle configurazioni dell'agent, permettendo di modificare la configurazione attuale o una precedente e salvarla come nuova. *Vedi "Dati dello storico configurazioni di un agent" nella pagina di fronte*.<br>  Mostra lo storico degli eventi dell'agent (Info). *Vedi "Dati dello storico eventi di un agent" nella pagina di fronte*<br>  Mostra il risultato dei comandi lanciati sul dispositivo tramite azioni **Execute**. *Vedi "Pagina dei comandi" a pagina 41*.<br>  Mostra lo storico sincronizzazioni dell'agent. *Vedi "Dati dello storico sincronizzazioni dell'agent" nella pagina di fronte*.<br>  Apre la funzione per caricare o scaricare file dal dispositivo del target. *Vedi "Trasferimento file da/a il target" a pagina 42* |
| **5** | Dettagli dell'agent. |
| **6** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *vedi "Elementi e azioni comuni dell'interfaccia" a pagina 11*.
Per saperne di più sugli agent *vedi "Cose da sapere sugli agent" a pagina 35*.

## Dati dello storico configurazioni di un agent

Di seguito la descrizione:

| *Campo* | *Descrizione* |
|---|---|
| **Descrizione** | Descrizione libera della configurazione. |
| **Utente** | Nome utente che ha creato la configurazione. |
| **Salvato** | Data salvataggio della configurazione. |
| **Ora di invio** | Data spedizione della configurazione tramite sincronizzazione.<br>  **AVVERTENZA: se questo valore è nullo, l'agent non ha ancora ricevuto la configurazione.** |
| **Attivato** | Data installazione nuova configurazione nell'agent. |

## Dati dello storico eventi di un agent

Di seguito la descrizione:

| *Campo* | *Descrizione* |
|---|---|
| **Acquisizione** | Data-ora dell'evento acquisito sul dispositivo.<br>È possibile filtrare. **Ultime 24 ore** è l'impostazione predefinita. |
| **Recezione** | Data-ora dell'evento registrato in RCS.<br>È possibile filtrare. **Ultime 24 ore** è l'impostazione predefinita. |
| **Contenuto** | Informazione di stato inviata dall'agent. |

## Dati dello storico sincronizzazioni dell'agent

Di seguito la descrizione:

| *Campo* | *Descrizione* |
|---|---|
| **Fine sincronizzazione** | Data e ora di fine della sincronizzazione.<br>È possibile filtrare. **Ultime24 ore** è l'impostazione predefinita. |
| **Inizio sincronizzazione** | Data e ora di inizio della sincronizzazione. |
| **IP** | Indirizzo IP da cui è stata fatta la sincronizzazione. |

| *Campo* | *Descrizione* |
|---|---|
| **Evidence** | Numero di evidence effettivamente trasferite in quella sincronizzazione sul totale delle evidence da trasferire . |
| **Dimensione** | Dimensione totale delle evidence trasferite. |
| **Velocità** | Velocità di trasferimento. |
| **Scaduto** | Indica se la sincronizzazione è scaduta. |

# Pagina dei comandi

| | |
|---|---|
| *Per gestire i risultati dei comandi:* | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, doppio-clic su **Comandi** |

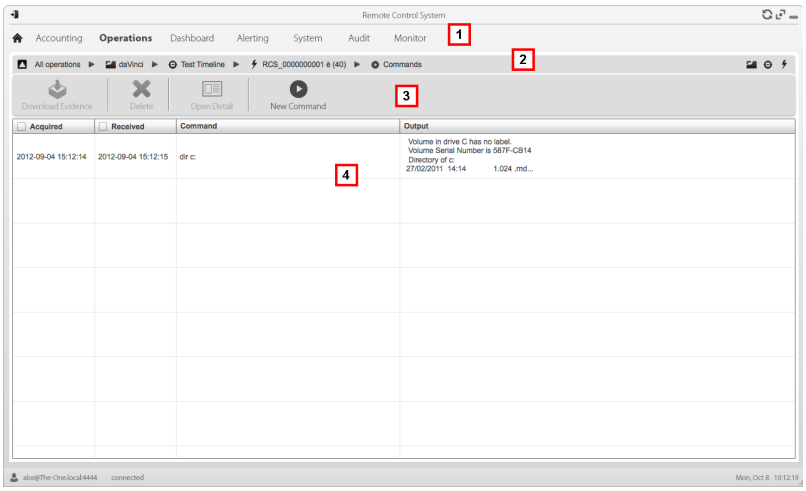
## Scopo

Questa funzione permette di:

- verificare i risultati dei comandi eseguiti dall'azione **Execute** configurata sull'agent
- verificare i risultati del file eseguibile attivato durante il trasferimento di file da/a l'agent
- lanciare uno o più comandi estemporanei a un agent

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |

| *Area* | *Descrizione* |
|---|---|
| **2** | Barra di navigazione. |
| **3** | Barre con i pulsanti della finestra.<br>Di seguito la descrizione:<br>  Esporta in un file .txt il comando selezionato.<br>  Mostra il dettaglio del comando selezionato.<br>  Apre una finestra per l'inserimento di una o più stringhe di comando. Alla successiva sincronizzazione tutti i comandi vengono inviati all'agent e il risultato viene visualizzato alla successiva ricezione.<br>  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Esecuzione comandi su agent**. |
| **5** | Elenco dei comandi in base ai filtri impostati. |
| **6** | Barra di stato di RCS. |

### Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "Elementi e azioni comuni dell'interfaccia" a pagina 11*.

# Trasferimento file da/a il target

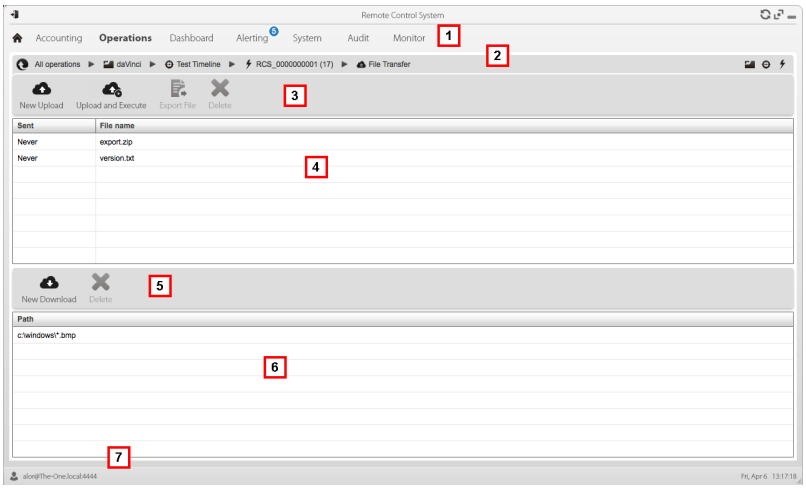
| | |
|---|---|
| ***Per trasferire file da/a l'agent:*** | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, doppio clic su **Trasferimento File** |

### Scopo

Caricare e scaricare file sul dispositivo dove è installato l'agent.

### Come si presenta la funzione

Ecco come viene visualizzata la funzione di trasferimento file da/a il target:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione per l'operation. |
| **3** | Barre con i pulsanti della finestra. Di seguito la descrizione: |

Carica un file nella cartella del dispositivo dove è installato l'agent. Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Caricamento file verso agent**.

Carica un file eseguibile nella cartella del dispositivo dove è installato l'agent e lo esegue (tramite comando **Execute**). Il risultato dell'esecuzione compare nella pagina **Comandi**. *Vedi "**Pagina dei comandi**" a pagina 41*. Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file.

**IMPORTANTE: questa funzione può essere inibita se l'utente è privo dei relativi permessi o se la licenza d'uso non la permette.**

Esporta lo storico dei caricamenti.

Elimina il caricamento selezionato. Eventuali risultati del comando eliminato vengono mantenuti.

| | |
|---|---|
| **4** | Storico dei caricamenti, con i pulsanti dei comandi. |

| *Area* | *Descrizione* |
|---|---|
| **5** | Barre con i pulsanti della finestra. Di seguito la descrizione:<br>  Scarica un file dal dispositivo. È necessario indicare il percorso incluso di nome file. Ogni scaricamento avvenuto viene registrato nello storico con il nome del file completo di percorso. Il file viene salvato nella cartella RCS Download sul desktop.<br>  Elimina dalla cartella RCS Download il file selezionato. |
| **6** | Storico degli scaricamenti, con i pulsanti dei comandi. |
| **7** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.
Per la descrizione dei dati degli agent *vedi "**Pagina dell'agent**" a pagina 38*.

# 6

# Factory e agent: configurazione base

## Presentazione

### Introduzione

La configurazione base permette di inserire moduli di acquisizione dati o di esecuzione comandi semplici, che non richiedono impostazioni complesse.

### Contenuti

Questa sezione include i seguenti argomenti:


**Cose da sapere sulla configurazione base** ..... **46**
**Configurazione base di una factory o di un agent** ..... **46**
**Dati della configurazione base** ..... **49**

# Cose da sapere sulla configurazione base

## Configurazione base

La configurazione base di una factory/agent permette di abilitare e definire rapidamente l'acquisizione delle evidence.

La configurazione base non prevede l'acquisizione di alcuni tipi di evidence, né l'impostazione dettagliata delle modalità di acquisizione

Configurazione base di default:

- L'acquisizione delle informazioni di sistema all'accensione del dispositivo (non disabilitabile)
- Un modulo per l'esecuzione della sincronizzazione tra agent e RCS ad un certo intervallo.

Per l'elenco dei tipi di moduli presenti nella configurazione base *vedi "**Dati della configurazione base**" a pagina 49*.

***PRUDENZA: se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base di default.***

## Esportazione e importazione di configurazioni

L'esportazione/importazione di una configurazione base o avanzata serve a riutilizzare una configurazione su altri sistemi RCS.

La configurazione base o avanzata viene esportata in un file .json che può essere trasferito in un altro sistema e importato durante la creazione di un agent.

## Salvataggio della configurazione come template

Il salvataggio come template di una configurazione base o avanzata serve a riutilizzare la configurazione da parte di utenti diversi dello stesso sistema RCS.

La configurazione base o avanzata viene salvata come template nel database, accompagnata da una descrizione e dal nome utente. Durante la creazione di un altro target può essere caricata da un altro utente e diventa quindi la configurazione di quell'agent.

**IMPORTANTE: i template di configurazioni base e avanzate vengono salvati separatamente nel database. I template di configurazioni base compaiono quindi durante la creazione di un agent con configurazione base, i template di configurazioni avanzatecompaiono durante la creazione di un agent con configurazione avanzata.**

# Configurazione base di una factory o di un agent

| | |
|---|---|
| ***Per configurare factory e agent:*** | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory<br>• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent |

## Scopo

Questa funzione permette di:

- configurare la factory/agent indicando se è richiesta la sincronizzazione online e quali dati si desidera acquisire
- aprire la funzione di compilazione della factory (*vedi "**Compilazione di una factory**" a pagina 31*.
- aprire la funzione di configurazione avanzata (*vedi "**Configurazione avanzata di una factory o di un agent**" a pagina 55*)

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Configurazione agent**.

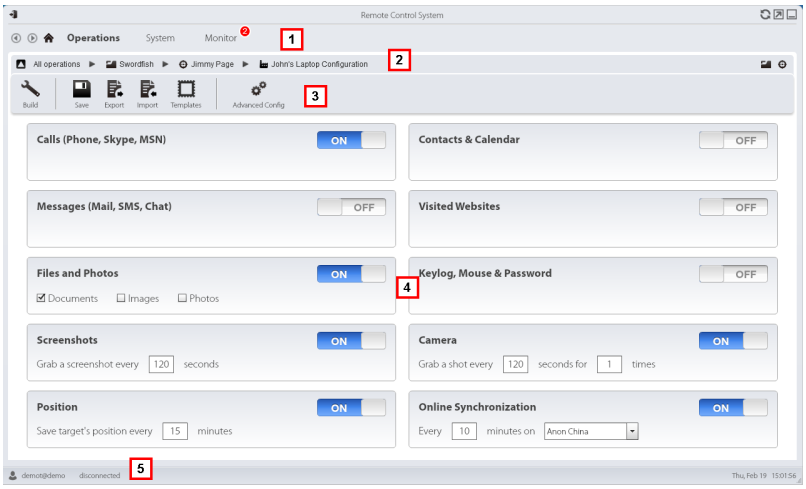
## Passi successivi

Dopo aver configurato la factory è necessario compilarla per ottenere l'agent.

Dopo aver modificato la configurazione di un agent, è sufficiente salvarla. Se l'agent è online, alla successiva sincronizzazione sarà applicata la nuova configurazione. Altrimenti occorre procedere all'installazione fisica.

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |

| *Area* | *Descrizione* |
|---|---|
| **3** | Barre con i pulsanti della finestra. Di seguito la descrizione:<br>  Compila la configurazione in uno o più agent da installare, in base ai vettori di installazione scelti. *Vedi "**Compilazione di una factory**" a pagina 31*<br>  Salva la configurazione: la configurazione di un agent viene registrata nello storico e alla successiva sincronizzazione viene inviata all'agent. *Vedi "**Dati dello storico configurazioni di un agent**" a pagina 40*<br>  Esporta la configurazione in un file .json.<br>  Importa la configurazione da un file .json.<br>  Carica il template di una configurazione base o salva la configurazione attuale come template. *Vedi "**Cose da sapere sulla configurazione base**" a pagina 46*.<br>  Apre la finestra della configurazione avanzata. *Vedi "**Configurazione avanzata di una factory o di un agent**" a pagina 55*.<br>  ***PRUDENZA: se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base.*** |
| **4** | Elenco dei tipi di acquisizione disponibili e relativo stato di attivazione.<br>  NOTA: l'elenco dei moduli varia in base al tipo di dispositivo. |
| **5** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per saperne di più sulla configurazione base *vedi "**Cose da sapere sulla configurazione base**" a pagina 46*.

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati della configurazione base**" nella pagina di fronte*.

Per l'elenco dei moduli disponibili nelle due configurazioni *vedi "**Elenco dei moduli**" a pagina 130*

## Configurare una factory o un agent

Per attivare o disattivare la raccolta delle evidence:

| *Passo* | *Azione* |
|---|---|
| 1 | • Fare clic su **OFF** in corrispondenza dell'evidence da acquisire: il pulsante diventa **ON** e le opzioni di configurazione, dove disponibili, possono essere impostate. |
| 2 | • In **Online Synchronization** lasciare **ON** se il dispositivo target avrà accesso a Internet. Questo permette di impostare le opzioni gradualmente. Lasciare **OFF** se il dispositivo target non avrà accesso a Internet o se si desidera acquisire manualmente le evidence dal target.<br>• Fare clic su **Salva** per salvare la configurazione corrente. |
| 3 | Proseguire in modo diverso: |

| *Se si sta configurando...* | *Allora...* |
|---|---|
| una factory | fare clic su **Crea** per compilarla e ottenere gli agent per diverse piattaforme. *Vedi "Compilazione di una factory" a pagina 31.* |
| un agent | alla prossima sincronizzazione l'agent aggiorna automaticamente la propria configurazione. |

# Dati della configurazione base

Di seguito i tipi di registrazioni attivabili nella configurazione base di una factory o di un agent.

| *Registrazione* | *Descrizione* |
|---|---|
| **Calls** | Registra chiamate.<br>NOTA: non disponibile per agent di livello soldier. |
| **Messages** | Registra messaggi. |
| **Files & Photos** | **Documenti:** abilita la cattura dei documenti aperti dal target (solo desktop)<br>**Immagini**: abilita la cattura delle immagini aperte dal target (solo desktop)<br>**Fotografie**: abilita la cattura delle foto nella libreria del target (desktop e mobile)<br>NOTA: non disponibile per agent di livello soldier. |
| **Screenshots** | Registra la schermata attiva sul display del target.<br>**Cattura una schermata ogni**: intervallo acquisizione immagine. |

| *Registrazione* | *Descrizione* |
|---|---|
| **Position** | Registra la posizione geografica del target.<br>**Salva la posizione del target ogni**: intervallo acquisizione posizione. |
| **Contacts & Calendar** | Registra i contatti e il calendario. |
| **Visited websites** | Registra l'indirizzo URL delle pagine web visitate. |
| **Keylog** | (solo mobile) Registra i tasti premuti sulla tastiera. |
| **Keylog, Mouse & Password** | (solo desktop) Registra i tasti premuti sulla tastiera, le password salvate sul sistema e i clic del mouse. |
| **Camera** | Registra le immagini della webcam.<br>**Cattura una immagine ogni**: intervallo acquisizione immagine.<br>**per … volte**: ripetizioni dell'acquisizione. |
| **Online Synchronization** | Abilitata di default. Se abilitata, l'agent contatta il server per l'invio dei dati e la ricezione delle nuove configurazioni, aggiornamenti e così via.<br>**Ogni**: intervallo di sincronizzazione<br>**minuti in**: nome o indirizzo IP dell'Anonymizer o del Collector. È possibile inserire manualmente il nome o indirizzo IP. |

# 7

# Factory e agent: configurazione avanzata

## Presentazione

### Introduzione

La configurazione avanzata permette di impostare opzioni avanzate di configurazione. Oltre ad abilitare la raccolta delle evidence, gli eventi possono essere collegati ad azioni, per attivare reazioni specifiche dell'agent e cambiare certe condizioni nel dispositivo (es.: avvio del salva schermo). Le azioni possono avviare o fermare moduli e abilitare o disabilitare altri eventi. Inoltre tutti gli eventi, azioni e le opzioni dei moduli possono essere impostati individualmente.

### Contenuti

Questa sezione include i seguenti argomenti:

**Cose da sapere sulla configurazione avanzata** ..... **52**
**Configurazione avanzata di una factory o di un agent** ..... **55**

# Cose da sapere sulla configurazione avanzata

## Configurazione avanzata

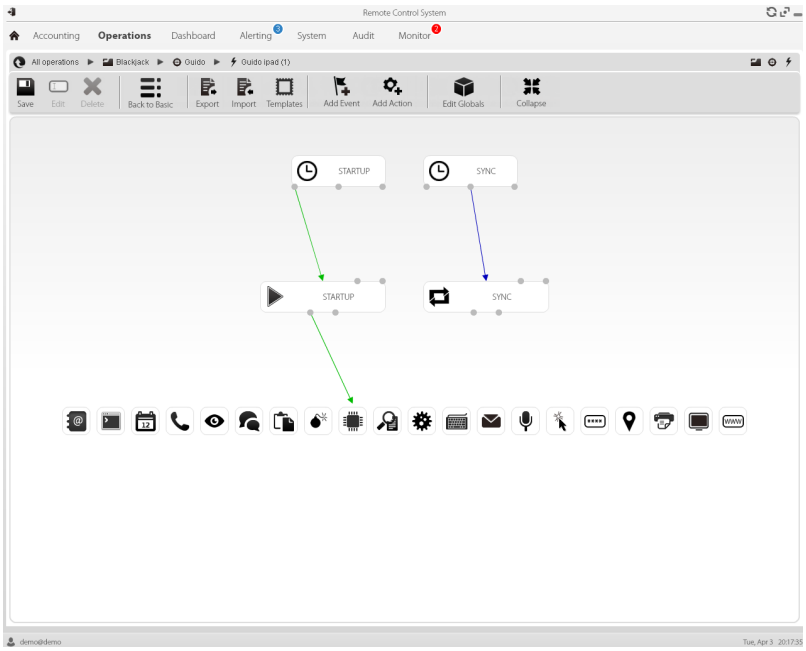
La configurazione avanzata di una factory/agent permette di creare delle sequenze complesse di attivazione tramite una semplice interfaccia grafica.

La sequenza avrà lo scopo di avviare/fermare le la raccolta delle evidence, e/o eseguire un'azione al verificarsi di un evento.

La configurazione avanzata include sempre due sequenze base:

- A ogni sincronizzazione (evento Ripetitivo) acquisisce le informazioni sul dispositivo (azione Start module + modulo Device)
- Allo scadere dell'intervallo di sincronizzazione (evento Timer-Ripetitivo) esegui la sincronizzazione tra agent e RCS (azione Synchronize)

Di seguito l'immagine che descrive le due sequenze base suggerite per l'acquisizione dati da remoto:




NOTA: queste due sequenze base sono impostate di default e sono suggerite per il minimo funzionamento dell'agent.

## Componenti della configurazione avanzata

I componenti della configurazione avanzata sono:

- gli *eventi* che scatenano un'azione (es.: una chiamata ricevuta sul dispositivo)
- le *azioni* eseguite a fronte di un evento (es.: avvio della registrazione di una chiamata)
- le *sotto-azioni* eseguite a fronte di un evento (es.: invio di un SMS nascosto con la posizione del dispositivo)
- i *moduli* che a fronte dell'azione iniziano a raccogliere le prove desiderate o eseguono altre azioni sul dispositivo (es.: registrazione dell'audio della chiamata)
- le *sequenze*, ovvero l'insieme di eventi, azioni, sotto-azioni e moduli.

NOTA: alcuni eventi, azioni e moduli possono essere impostati solo nella configurazione avanzata.

## Lettura delle sequenze

Le sequenze complesse possono essere lette così:

- Alla connessione del dispositivo all'alimentazione (evento)...
- ...manda un SMS (sotto-azione) e...
- ...avvia la registrazione della posizione (azione verso modulo) e...
- ...disabilita l'evento scatenato al cambio della SIM (azione che disabilita un evento)
- ...e così via

Le possibili combinazioni tra eventi, azioni, sotto-azioni e moduli sono infinite. Di seguito la spiegazione dettagliata delle regole di progettazione corrette.

## Eventi

Gli eventi vengono controllati dall'agent e possono avviare, ripetere o concludere un'azione.

NOTA: non è possibile avviare un modulo direttamente da un evento.

Per esempio un evento **Window** (apertura di una finestra sul dispositivo) può avviare un'azione. Sarà poi l'azione che avvierà/fermerà un modulo.

Sono disponibili diversi tipi di eventi. Per l'elenco completo *vedi "Elenco degli eventi" a pagina 122.*

La relazione tra un evento e una o più azioni è rappresentata da un connettore:

| ***Relazione tra evento e azione*** | ***Descrizione*** | ***Connettore*** |
|---|---|---|
| **Start** | Avvia un'azione quando accade l'evento. |  |
| **Repeat** | Ripete un'azione. È possibile specificare l'intervallo e il numero di ripetizioni. |  |
| **End** | Avvia un'azione quando l'evento si conclude. |  |

NOTA: un evento può gestire fino a tre azioni distinte contemporaneamente. L'azione **Start** viene avviata quando l'evento accade sul dispositivo (es.: l'evento **Standby** scatena la **S tart** quando il dispositivo entra in standby). L'azione **Repeat** viene scatenata all'intervallo definito per tutta la durata dell'evento. L'azione **Stop** viene avviata quando l'evento si conclude (es.: l'evento **StandBy** scatena la **End** quando il dispositivo esce dalla modalità di standby).

## Azioni

Le azioni sono innescate dall'accadere di un evento. Possono:

- avviare o fermare un modulo
- abilitare e disabilitare un evento
- eseguire una sotto-azione

Per esempio un'azione (vuota) può disabilitare l'evento **Process** (avvio di un processo di sistema) che l'ha innescata e abilitare il modulo **Position** (registra posizione GPS). Se necessario l'azione può anche eseguire una sotto-azione **SMS** (invio messaggio a un numero telefonico specificato).

Sono disponibili diverse *sotto-azioni* che possono essere combinate tra loro senza limitazioni (es.: eseguire un comando + creare un messaggio di Alert). Per l'elenco completo *vedi "Elenco delle sotto-azioni" a pagina 116*

## Relazioni tra azioni e moduli

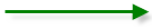
Un'azione può agire su un modulo in modi diversi. La relazione tra un'azione e uno e più moduli è rappresentata da un connettore:

| *Relazione tra azione e moduli* | *Descrizione* | *Connettore* |
|---|---|---|
| **Start modules** | Avvia un modulo. |  |
| **Stop modules** | Ferma un modulo. |  |

Un'azione può avviare/fermare più moduli contemporaneamente.

## Relazioni tra azioni e eventi

La relazione tra un'azione e uno e più eventi è rappresentata da un connettore:

| *Relazione tra azione e eventi* | *Descrizione* | *Connettore* |
|---|---|---|
| **Enable events** | Abilita un evento. |  |
| **Disable events** | Disabilita un evento. |  |

NOTA: un'azione può abilitare/disabilitare più eventi contemporaneamente.

### Moduli

Ogni modulo abilita la raccolta di una specifica evidence dal dispositivo del target. Possono essere avviati/fermati da un'azione e producono le evidence.

Per esempio un modulo **Position** (registra posizione GPS) può essere avviato da un'azione innescata da un evento **Call** (è stata ricevuta/effettuata una chiamata).

Sono disponibili diversi moduli che possono essere avviati/fermati (es.: avvia modulo posizione + ferma modulo screenshot). Per l'elenco completo *vedi "Elenco dei moduli" a pagina 130*.

### Esportazione e importazione di configurazioni

L'esportazione/importazione di una configurazione base o avanzata serve a riutilizzare una configurazione su altri sistemi RCS.

La configurazione base o avanzata viene esportata in un file .json che può essere trasferito in un altro sistema e importato durante la creazione di un agent.

### Salvataggio della configurazione come template

Il salvataggio come template di una configurazione base o avanzata serve a riutilizzare la configurazione da parte di utenti diversi dello stesso sistema RCS.

La configurazione base o avanzata viene salvata come template nel database, accompagnata da una descrizione e dal nome utente. Durante la creazione di un altro target può essere caricata da un altro utente e diventa quindi la configurazione di quell'agent.

**IMPORTANTE: i template di configurazioni base e avanzate vengono salvati separatamente nel database. I template di configurazioni base compaiono quindi durante la creazione di un agent con configurazione base, i template di configurazioni avanzatecompaiono durante la creazione di un agent con configurazione avanzata.**

# Configurazione avanzata di una factory o di un agent

| | |
|---|---|
| ***Per aprire la configurazione avanzata:*** | • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio clic sulla factory, fare clic su **Config avanzata**<br>• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio clic sull'agent, fare clic su **Config avanzata** |

### Scopo

Questa funzione permette di:

- creare sequenze di attivazione dei moduli scatenate da eventi che si verificano sul dispositivo del target. Ogni sequenza può essere composta di una o più sotto-azioni.
- Impostare i parametri generali di una factory/agent.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Configurazione agent**.

NOTA: la configurazione avanzata non è disponibile per agent di livello soldier.

***PRUDENZA:*** *se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base di default.*

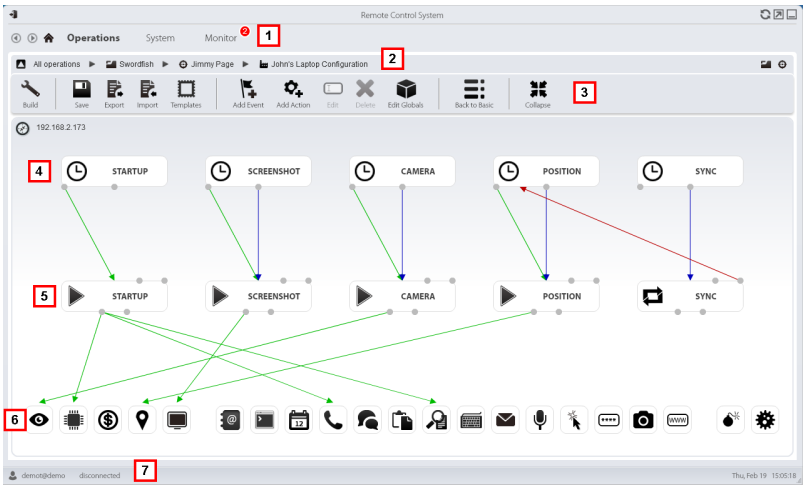
## Passi successivi

Per una factory, terminare la sua configurazione e compilarla per ottenere l'agent da installare.*Vedi "Compilazione di una factory" a pagina 31*

Per un agent, terminare la sua configurazione e salvarla. Alla successiva sincronizzazione la nuova configurazione sarà inviata all'agent.

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Barra di navigazione. |

| *Area* | *Descrizione* |
|---|---|
| **3** | Barre con i pulsanti della finestra. Di seguito la descrizione:<br>  Compila la configurazione in uno o più agent, in base ai vettori di installazione scelti. *Vedi "**Compilazione di una factory**" a pagina 31*<br>  Salva la configurazione corrente.<br>  Esporta la configurazione in un file .json.<br>  Importa la configurazione da un file .json.<br>  Carica il template di una configurazione avanzata o salva la configurazione attuale come template. *Vedi "**Cose da sapere sulla configurazione avanzata**" a pagina 52*.<br>  Inserisce un evento.<br>  Inserisce un'azione.<br>  Modifica l'evento o l'azione selezionati.<br>  Elimina l'evento, l'azione o la connessione logica selezionati.<br>  Modifica i dati globali dell'agent *vedi "**Dati globali dell'agent**" a pagina 59*.<br>  Torna alla configurazione di base<br>  ***PRUDENZA: tutte le impostazioni vengono perse.***<br>  Comprime/Espande i widget degli eventi e delle azioni per permettere una migliore visione della configurazione corrente. |
| **4** | Area degli eventi. Gli eventi **STARTUP** e **SYNC** sono abilitati di default. |
| **5** | Area delle azioni. Le azioni **STARTUP** e **SYNC** sono abilitate di default. |
| **6** | Area dei moduli di registrazione. I moduli cambiano in base al dispositivo desktop o mobile. |
| **7** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per saperne di più sulla configurazione avanzata *vedi "**Cose da sapere sulla configurazione avanzata**" a pagina 52*.

## Creare una sequenza di attivazione semplice

Per creare una sequenza semplice, ovvero acquisire prove all'accadere di un evento:

| *Passo* | *Azione* |
|---|---|
| **1** | Creare un evento:<br>• Fare clic su **Nuovo Evento**: compare la finestra di selezione e impostazione evento.<br>• In **Tipo** selezionare il tipo di evento e impostarne le opzioni. *Vedi "**Elenco degli eventi**" a pagina 122*<br>• Fare clic su **Salva**: il nuovo evento viene aggiunto all'area di lavoro |
| **2** | Creare un'azione:<br>• Fare clic su **Nuova Azione**: l'azione vuota viene aggiunta all'area di lavoro |
| **3** | Collegare l'evento all'azione, poi collegare l'azione al modulo desiderato:<br>• Fare clic sul punto di connessione **Start** dell'evento e trascinare la freccia sull'azione<br>• Fare clic sul punto di connessione **Start modules** dell'azione e trascinare la freccia sui tipi di dati che si vogliono acquisire.*Vedi "**Elenco dei moduli**" a pagina 130*. |
| **4** | Fare clic su **Salva**: la configurazione è pronta per essere compilata (se factory) o trasmessa al dispositivo alla prossima sincronizzazione (se agent). |

## Creare una sequenza di attivazione complessa

Per creare una sequenza complessa, ovvero all'accadere di un evento raccogliere le evidence, eseguire una sotto-azione ed eventualmente abilitare/disabilitare un evento:

| *Passo* | *Azione* |
|---|---|
| **1** | Creare un evento:<br>• Fare clic su **Nuovo Evento**: compare la finestra di selezione e impostazione evento.<br>• In **Tipo** selezionare il tipo di evento e impostarne le opzioni. *Vedi "**Elenco degli eventi**" a pagina 122*<br>• Fare clic su **Salva**: il nuovo evento viene aggiunto all'area di lavoro |
| **2** | Creare un'azione e definire le sotto-azioni:<br>• Fare clic su **Nuova Azione**: l'azione vuota viene aggiunta all'area di lavoro<br>• Fare doppio clic sull'azione e in **Sottoazioni** aggiungere le sotto-azioni desiderate e impostarne le opzioni. *Vedi "**Elenco delle sotto-azioni**" a pagina 116*. |
| **3** | Collegare l'evento all'azione:<br>• Fare clic su uno dei punti di connessione **Start, Repeat, End** dell'evento e trascinare la freccia sull'azione |

| *Passo* | *Azione* |
|---|---|
| **4** | Collegare l'azione al modulo:<br>• Fare clic sui punti di connessione **Start modules** , **Stop modules** dell'azione e trascinare la freccia sul modulo da avviare o fermare. *Vedi "**Elenco dei moduli**" a pagina 130.*<br><br>Suggerimento: Trascinare più frecce se più moduli devono essere abilitati.<br><br>Se si tratta di un'azione che richiede l'abilitazione/disabilitazione di un evento:<br>• Fare clic sul punto di connessione **Enable events o Disable events** dell'azione e trascinare la freccia sugli eventi da abilitare/disabilitare. |
| **5** | Fare clic su **Salva**: la configurazione è pronta per essere compilata (se factory) o trasmessa al dispositivo alla prossima sincronizzazione (se agent). |

## Dati globali dell'agent

I dati globali dell'agent sono descritti di seguito:

| *Campo* | *Descrizione* |
|---|---|
| **Spazio Disco Minimo** | Quantità minima spazio disco libero sul dispositivo. |
| **Dimensione Massima Evidence** | Quantità massima spazio occupato dalle evidence sul dispositivo del target, fino alla successiva sincronizzazione. Il default è 1 GB.<br>Al raggiungimento di questo limite, l'agent termina la registrazione in attesa della successiva sincronizzazione. Se la sincronizzazione non avviene, non vengono acquisite ulteriori evidence. |
| **Rimozione sicura agent** | Se abilitato, cancella in modo sicuro i file generati dall'agent. Nessuna traccia dell'agent sarà rilevabile in caso di un'analisi forense.<br>NOTA: questa modalità richiede un tempo maggiore rispetto alla normale eliminazione del file. |
| **Rimozione driver** | Rimuove il driver alla disinstallazione. |
| **Mostra** | *Richiede assistenza: utilizzare solo su richiesta dell'assistenza tecnica HackingTeam.* |
| **Maschera** | *Richiede assistenza: utilizzare solo su richiesta dell'assistenza tecnica HackingTeam.* |

# 8

# I Network Injector

## Presentazione

### Introduzione

I Network Injector permettono di intercettare le connessioni HTTP del target e infettare con un agent un suo dispositivo.

### Contenuti

Questa sezione include i seguenti argomenti:


**Cose da sapere su Network Injector e le sue regole** ..... **61**
**Gestione dei Network Injector** ..... **62**
**Dati delle regole di infezione** ..... **64**
**Verifica dello stato dei Network Injector** ..... **69**
**Cose da sapere su Appliance Control Center** ..... **70**
**Cose da sapere su Tactical Control Center** ..... **72**
**Cose da sapere per individuare la password di rete WiFi** ..... **77**
**Cose da sapere per lo sblocco della password del sistema operativo** ..... **78**
**Cose da sapere per l'accesso remoto al Control Center** ..... **79**
**Comandi Tactical Control Center e Appliance Control Center** ..... **81**
**Appliance Control Center** ..... **82**
**Dati Appliance Control Center** ..... **89**
**Tactical Control Center** ..... **90**
**Dati del Tactical Control Center** ..... **107**
**Altri applicativi installati sui Network Injector** ..... **109**

# Cose da sapere su Network Injector e le sue regole

## Introduzione

Network Injector controlla tutte le connessioni HTTP e seguendo le regole di infezione individua le connessioni del target e inserisce l'agent all'interno delle connessioni, agganciandolo a delle risorse che il target sta scaricando da Internet.

## Tipi di Network Injector

Esistono due tipi di Network Injector:

- Appliance: server di rete per installazioni in segmento access switch o intra-switch presso un fornitore di servizi Internet.
- Tactical: computer portatile per installazioni tattiche in reti Wifi o LAN e per sbloccare la password di sistemi operativi per infezioni fisiche (es.: tramite Silent Installer)

Entrambi i Network Injector permettono, tramite il loro software di gestione (Appliance Control Center o Tactical Control Center) di identificare automaticamente i dispositivi target e infettarli secondo le regole definite. I Tactical Network Injector permettono anche di effettuare l'identificazione manualmente. *Vedi "**Cose da sapere su Appliance Control Center**" a pagina 70, "**Cose da sapere su Tactical Control Center**" a pagina 72.*

## Tipi di risorse infettabili

Le risorse infettabili da RCS sono file di qualsiasi tipo.

NOTA: Network Injector non è in grado di monitorare connessioni FTP o HTTPS.

## Come creare una regola

Per creare la regola occorre:

1. definire il metodo per identificare le connessioni del target. Per esempio, confrontando l'indirizzo IP o MAC del target. Oppure lasciare selezionare il dispositivo all'operatore del Tactical Network Injector.
2. definire il metodo per infettare il target. Per esempio attraverso la sostituzione di un file che il target sta scaricando dalla rete, oppure attraverso l'infezione di una pagina web che il target visita abitualmente.

## Regole di identificazione automatica e da operatore

Se si conoscono già informazioni relative ai dispositivi target, è possibile creare numerose regole adattandole alle diverse abitudini del target, per poi abilitare la/le regole più efficaci a seconda dell'opportunità che si crea in un determinato momento dell'investigazione.

Se invece non si conosce nulla dei dispositivi target, occorre utilizzare il Tactical Network Injector che - con la sua presenza sul campo - permette agli operatori di osservare il target, identificare il dispositivo che sta usando e infettarlo.

Per questo tipo di gestione manuale è necessario specificare **TACTICAL** nel campo **Pattern** della regola di infezione.

### Cosa succede quando si abilita/disabilita una regola

RCS comunica regolarmente con i Network Injector per trasmettere le regole e acquisire i log. Tutte le regole abilitate in RCS Console sono inviate automaticamente ai Network Injector. Una regola disabilitata viene invece salvata, ma non sarà né inviata né più resa disponibile alla successiva sincronizzazione.

Sul Network Injector è necessario scegliere tra le regole a disposizione quali abilitare per una specifica infezione.

### Avvio dell'infezione

Dopo che Network Injector ha ricevuto le regole di infezione è pronto per iniziare un attacco.

Nella fase di sniffing controlla se tra i dispositivi presenti in rete qualcuno soddisfa le regole di identificazione. In caso affermativo invia l'agent al dispositivo identificato e lo infetta.

## Gestione dei Network Injector

*Per gestire i Network Injector:* • sezione **System, Network Injectors**

### Scopo

Durante il funzionamento di RCS, questa funzione permette di creare le regole di infezione e inviarle al Network Injector.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione regole Network Injector**.

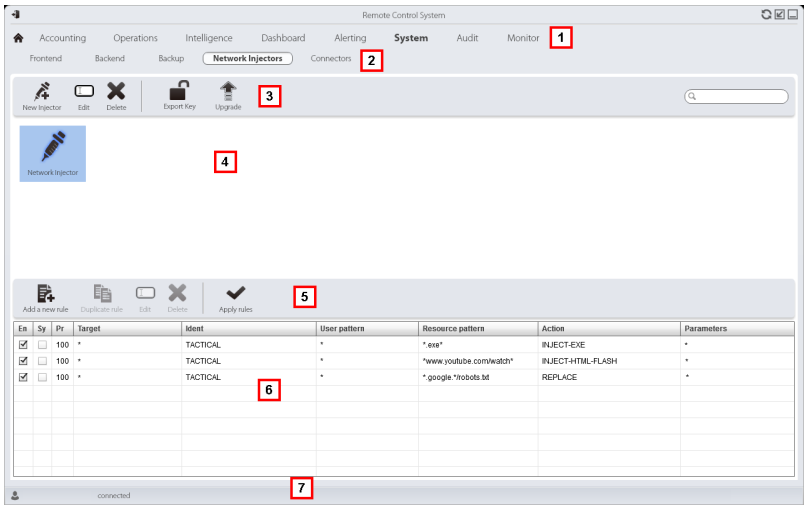
### Cosa è possibile fare

Con questa funzione è possibile:

- creare una regola di infezione di un agent su un target
- inviare le regole al Network Injector

Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS. |
| **2** | Menu **System.** |
| **3** | Barra con i pulsanti dedicati ai Network Injector. |
| **4** | Elenco dei Network Injector. |
| **5** | Barra con i pulsanti dedicati alle regole di infezione.<br>Di seguito la descrizione:<br>Aggiunge una nuova regola.<br>Duplica la regola selezionata.<br>Apre la finestra con i dati della regola.<br>Elimina la regola selezionata.<br>Invia le regole al Network Injector selezionato. L'Appliance si aggiorna automaticamente alla successiva sincronizzazione, basta che ci sia un processo di infezione attivo. Mentre con il Tactical sarà l'operatore a scegliere se aggiornare le regole. |
| **6** | Elenco delle regole del Network Injector selezionato. |
| **7** | Barra di stato di RCS. . |

## Per saperne di più

Per la descrizione degli elementi dell'interfaccia *vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per la descrizione dei dati delle regole di infezione *vedi "**Dati delle regole di infezione**" nella pagina di fronte*.

Per saperne di più sulle regole di infezione *vedi "Cose da sapere su Network Injector e le sue regole" a pagina 61*.

### Aggiungere una nuova regola di infezione

Per aggiungere una nuova regola:

| *Passo* | *Azione* |
|---|---|
| **1** | Selezionare il Network Injector per il quale si desidera aggiungere la nuova regola: compaiono i comandi e la tabella delle regole. |
| **2** | • Fare clic su **Nuova regola**: compaiono i dati da compilare.<br>• Compilare i dati richiesti. Se la regola è abilitata è già possibile inviarla al Network Injector. *Vedi "Dati delle regole di infezione" nel seguito*.<br>• Fare clic su **Salva**: nell'area di lavoro principale compare la nuova regola. |

### Inviare le regole al Network Injector

Per inviare le regole al Network Injector:

| *Passo* | *Azione* |
|---|---|
| **1** | Abilitare le regole da inviare al Network Injector selezionando la casella di controllo **Ab** nella tabella. |
| **2** | Fare clic su **Applica regole**: RCS prende in carico la richiesta di inviare le regole al Network Injector selezionato. La barra di avanzamento nell'area download mostra l'avanzamento dell'operazione.<br>**IMPORTANTE: Network Injector riceve le regole aggiornate solo quando è sincronizzato con il server RCS. *Vedi "Verifica dello stato dei Network Injector " a pagina 69*.** |

# Dati delle regole di infezione

### Dati delle regole

Di seguito la descrizione dei dati che definiscono le regole di infezione disponibili:

| *Dato* | *Descrizione* |
|---|---|
| **Abilitato** | Se selezionato, la regola sarà inviata al Network Injector.<br>Se non selezionato, la regola viene salvata, ma non inviata. |
| **Disabilita alla sync** | Se selezionato, la regola viene disabilitata alla prima sincronizzazione dell'agent definito nella regola.<br>Se non selezionato, Network Injector continua ad applicare la regola, anche dopo la prima sincronizzazione. |

| *Dato* | *Descrizione* |
|---|---|
| **Probabilità** | Probabilità (in percentuale) di applicazione delle regole dopo la prima risorsa infettata.<br>**0%**: dopo aver infettato la prima risorsa, Network Injector non applica più questa regola.<br>**100%**: dopo aver infettato la prima risorsa, Network Injector continua ad applicare questa regola.<br>  Suggerimento: se si applica un valore superiore al 50%, si consiglia di utilizzare l'opzione **Disabilita alla sync**. |
| **Target** | Nome del target da infettare. |
| **Ident** | Metodo di identificazione delle connessioni HTTP del target.<br>  NOTA: Network Injector non può monitorare connessioni FTP o HTTPS.<br>*Vedi "**Metodi di identificazione delle connessioni HTTP**" nel seguito* |
| **Pattern** | Metodo di identificazione del traffico del target. Il formato dipende dal tipo di **Ident** selezionato.<br>*Vedi "**Metodi di identificazione del traffico**" nella pagina di fronte* |
| **Azione** | Metodo di infezione che verrà applicato sulla risorsa indicata in **Pattern risorsa**.<br>*Vedi "**Metodi di infezione**" a pagina 67* |
| **Pattern risorsa** | Metodo di identificazione della risorsa da infettare, applicato all'URL della risorsa Web. Il formato dipende dal tipo di **Azione** selezionata. |
| **Factory** | Per tutte le azioni tranne le **REPLACE**. Agent da iniettare nella risorsa web selezionata. |
| **File** | Solo per azione **REPLACE** . File da sostituire a quello indicato in **Pattern risorsa**. |

### Metodi di identificazione delle connessioni HTTP

Di seguito la descrizione di ogni metodo:

| *Dato* | *Descrizione* |
|---|---|
| **STATIC-IP** | IP statico assegnato al target. |
| **STATIC-RANGE** | Range di indirizzi IP assegnati al target. |

| *Dato* | *Descrizione* |
|---|---|
| **STATIC-MAC** | Indirizzo MAC statico del target, sia Ethernet che WiFi. |
| **DHCP** | Indirizzo MAC dell'interfaccia di rete del target. |
| **RADIUS-LOGIN** | Nome utente RADIUS. User-Name (RADIUS 802.1x). |
| **RADIUS-CALLID** | Identificativo del chiamante RADIUS. Calling-Station-Id (RADIUS 802.1x). |
| **RADIUS-SESSID** | Identificativo sessione RADIUS· Acct-Session-Id (RADIUS 802.1x). |
| **RADIUS-TECHKEY** | Chiave RADIUS. NAS-IP-Address: Acct-Session-Id (RADIUS 802.1x). |
| **STRING-CLIENT** | Stringa di testo da individuare nel traffico dati proveniente dal target. |
| **STRING-SERVER** | Stringa di testo da individuare nel traffico dati destinato al target. |
| **TACTICAL** | Il target non viene identificato automaticamente, ma si demanda la sua identificazione all'intervento dell'operatore sul Tactical Network Injector. Quindi è solo quando l'operatore identifica il dispositivo, che il campo **Ident** viene "personalizzato" con i dati ricevuti dal dispositivo stesso. |

### Metodi di identificazione del traffico

Di seguito la descrizione di ogni metodo:

| *Metodo* | *Formattazione* |
|---|---|
| **DHCP STATIC-IP STATIC-MAC** | Indirizzo corrispondente (es.: "195.162.21.2"). |
| **STATIC-RANGE** | Range di indirizzi separati da '-' (es.: "195.162.21.2-195.162.21.5". |
| **STRING-CLIENT STRING-SERVER** | Stringa di testo (es.: "John@gmail.com"). |
| **RADIUS-CALLID** | ID o parte dell'ID. |
| **RADIUS-LOGIN** | Nome o parte del nome dell'utente. |

| *Metodo* | *Formattazione* |
|---|---|
| **RADIUS-SESSID** | ID o parte dell'ID. |
| **RADIUS-TECHKEY** | Chiave o parte della chiave (es.: "*.10.*"). |
| **TACTICAL** | Non è possibile impostare un valore. Il valore corretto sarà definito dall'operatore sul campo. |

### Metodi di infezione

Di seguito la descrizione di ogni metodo:

| *Metodo* | *Funzione* |
|---|---|
| **INJECT-EXE** | Infetta in tempo reale il file EXE scaricato. L'installazione dell'agent avviene nel momento in cui il target esegue il file EXE. |
| **INJECT-HTML-FILE** | Permette di aggiungere il codice HTML fornito nel file all'interno della pagina web visitata.<br>  *Richiede assistenza: contattare i tecnici HackingTeam per ulteriori dettagli.* |
| **INJECT-HTML-FLASH** | Blocca i siti web supportati e richiede all'utente di installare un finto aggiornamento di Flash per visualizzarli. L'agent viene installato quando il target installa l'aggiornamento. |
| **REPLACE** | Sostituisce la risorsa definita in **Pattern risorsa** con il file fornito.<br>  Suggerimento: questo tipo di azione è molto efficace se usata in combinazione con i documenti generati da Exploit. |

### Metodi di identificazione della risorsa da infettare

Di seguito la descrizione di ogni metodo:

| *Tipo azione* | *Contenuto di Pattern risorsa* |
|---|---|
| **INJECT-EXE** | URL del file eseguibile da infettare. Utilizzare le wildcard per aumentare il numero di URL corrispondenti.<br>Esempi di formati possibili:<br>`*[nomeExe]*.exe`<br>`www.mozilla.org/firefox/download/firefoxsetup.exe`<br>  NOTA: quando si specifica un path completo, fare attenzione agli eventuali mirror utilizzati dai siti web per lo scaricamento dei file (es.: "firefox.exe?mirror=it").<br>  Suggerimento: digitare *.exe* per infettare tutti gli eseguibili, indipendentemente dall'URL.<br>  **IMPORTANTE:IMPORTANTE: se si digita per esempio: *exe*, senza il carattere '.' dell'estensione del file, saranno infettate tutte le pagine che contengono accidentalmente le lettere "exe".** |
| **INJECT-HTML-FILE** | URL della pagina web da infettare.<br>Esempi di formati possibili:<br>`www.oracle.com/`<br>`www.oracle.com/index.html`<br>  NOTA: se non si specifica una pagina HTML o dinamica, includere nell'indirizzo del sito il carattere '/' finale (es.: "`www.oracle.com/`").<br>  NOTA: non è possibile infettare una pagina di redirect. Verificare sul browser il path corretto del sito web prima di indicarlo nella regola. |
| **INJECT-HTML-FLASH** | Preconfigurato per i siti web supportati e non modificabile dall'utente. |
| **REPLACE** | URL della risorsa da sostituire. |

# Verifica dello stato dei Network Injector

## Introduzione

I Network Injector si sincronizzano con il server RCS per scaricare versioni del software di gestione aggiornate, le regole di identificazione e di infezione e - contestualmente - spedire i loro log.

Dalla RCS Console è possibile monitorare lo stato del Network Injector.

In particolare:

- nella sezione **Monitor**: per individuare i momenti in cui il Network Injector è sincronizzato e quindi richiede scambio di dati.

## Individuare quando il Network Injector è sincronizzato

Di seguito la procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Nella sezione **Monitor**, selezionare la riga corrispondente all'oggetto Network Injector che si vuole analizzare. Controllare la colonna **Stato**: se è presente un segno di spunta verde il Network Injector è sincronizzato.<br>Questa situazione si verifica quando dal software Control Center (Appliance o Tactical):<br>• è stato premuto il pulsante **Configure**, l'operatore manualmente ha richiesto di verificare la presenza di regole nuove o aggiornamenti;<br>• è stato premuto il tasto **Start** o comunque è in corso una infezione.<br>  **IMPORTANTE: solo quando il Network Injector è sincronizzato può ricevere da RCS le regole applicate e gli aggiornamenti.** |

# Cose da sapere su Appliance Control Center

## Introduzione

Appliance Control Center è un applicativo installato sul Network Injector Appliance.

Riesce a infettare dispositivi presenti in una rete cablata grazie alle regole di identificazione e infezione di RCS.

## Funzionamento di Appliance Control Center

Con Appliance Control Center è possibile:

- Abilitare la sincronizzazione con RCS, tramite un Anonymizer o catena di Anonymizer, per ricevere le regole di identificazione e di infezione aggiornate e inviare log.
- Aggiornare Appliance Control Center con l'ultima versione fornita da RCS Console.
- Identificare automaticamente i dispositivi connessi tramite le regole e infettarli.
- Configurare l'accesso remoto all'applicativo.

## Sincronizzazione con il server RCS

Appliance Control Center si sincronizza con RCS per ricevere le regole di infezione aggiornate, per controllare se è disponibile una nuova versione del Appliance Control Center e per inviare i log.

La sincronizzazione può avvenire in due modi:

- manualmente, almeno la prima volta per ricevere le regole di infezione.
- automaticamente con una infezione in corso.

Durante la sincronizzazione, il Network Injector comunica con RCS a intervalli di tempo prestabiliti (circa 30 sec.).

La comunicazione avviene tramite un Anonymizer. Da Appliance Control Center, dalla scheda **System Management** si configura l'Anonymizer da utilizzare per la sincronizzazione con RCS e si può decidere quando abilitare la sincronizzazione.

## Chiave di autenticazione

Per comunicare in sicurezza con il server RCS, sul Network Injector deve essere installata una chiave di autenticazione. La chiave deve essere generata quando si crea l'oggetto Network Injector sulla RCS Console e installata tramite Appliance Control Center alla prima sincronizzazione del Network Injector con RCS.

## Aggiornamento delle regole di infezione

Se il traffico generato dal target non è infettabile con le regole presenti nel Network Injector è necessario richiedere l'intervento di un operatore sulla RCS Console per generare nuove regole e aggiornare il Network Injector. Alla successiva sincronizzazione Appliance Control Center riceve le nuove regole e sarà possibile visualizzarle e abilitarle per l'infezione.

## Utilizzo delle interfacce di rete

In fase di attacco sono disponibili due diverse interfacce di rete, una per lo sniffing e una per l'infezione. L'utilizzo di due interfacce separate è indicato per garantire una continuità soprattutto nello sniffing.

Le interfacce di sniffing possono essere ad alta o a bassa velocità.

## Indirizzo IP dell'interfaccia di infezione

Se il server Appliance e il target non appartengono alla stessa sottorete (indirizzi IP con prefissi di routing differenti), l'interfaccia di infezione deve avere un indirizzo pubblico, altrimenti il target non riuscirà mai a vederla e l'infezione non potrà avvenire.

Con Appliance Control Center è possibile in una prima fase utilizzare l'indirizzo preimpostato sull'interfaccia (con **Public IP** = "auto"), attendere un eventuale messaggio che segnala che quell'indirizzo è privato e in quel caso impostare un indirizzo pubblico per il rendirizzamento dell'indirizzo privato (**Public IP** = "xxx.xxx.xxx.xxx").

Lo sniffing invece, può essere fatto tramite una interfaccia di rete con indirizzo IP privato.

## Processo di infezione tramite identificazione automatica

Di seguito i passaggi tipici per infettare dispositivi identificati automaticamente dalle regole di RCS. L'attacco può essere sferrato solo su reti cablate:

| *Fase* | *Descrizione* | *Dove* |
|---|---|---|
| **1** | Preparare le regole di identificazione e infezione per i dispositivi target conosciuti che si vogliono attaccare. Inviare le regole al Network Injector Appliance. | *RCS Console, System, Network Injectors* |
| **2** | Abilitare la sincronizzazione con RCS per ricevere le regole aggiornate e abilitare le regole da utilizzare per l'infezione. | *Network Injector Appliance, Network Injector* |
| **3** | Il sistema fa lo sniffing del traffico, identifica i dispositivi target grazie alle regole di identificazione e li infetta grazie alle regole di infezione. | *Network Injector Appliance, Network Injector* |

## Infezione tramite identificazione automatica

Questa modalità di lavoro si adatta a scenari dove si hanno già alcune informazioni sul dispositivo target (es.: indirizzo IP, MAC o RADIUS).

Le regole di infezione provenienti da RCS contengono già tutti i dati necessari per identificare automaticamente i dispositivi target. Per ogni infezione è importante abilitare tutte e solo le regole utili in quel momento.

L'avvio dell'identificazione automatica da parte della funzione **Network Injector** mette mano a mano in evidenza i dispositivi target che vengono subito infettati dalle regole di infezione.

**Accesso remoto ad Appliance Control Center**

È possibile accedere ad Appliance Control Center da remoto. Per saperne di più *vedi "**Cose da sapere per l'accesso remoto al Control Center**" a pagina 79*.

# Cose da sapere su Tactical Control Center

## Introduzione

Tactical Control Center è un applicativo installato su computer portatile, chiamato Tactical Network Injector.

Riesce a infettare dispositivi presenti in una rete WiFi o cablata grazie alle regole di identificazione e infezione di RCS. L'identificazione dei dispositivi può essere automatica o manuale. In questo secondo caso è l'operatore che riconosce il dispositivo da infettare e dà il comando di applicare le regole di infezione a quel dispositivo.

**IMPORTANTE: la modalità di identificazione va concordata con la sede operativa.**

## Funzionamento del Tactical Control Center

Con Tactical Control Center è possibile:

- Abilitare la sincronizzazione con RCS, tramite un Anonymizer o catena di Anonymizer, per la ricezione delle regole di identificazione e di infezione aggiornate e inviare log.
- Aggiornare Tactical Control Center, fondamentale per aggiornare gli agent sui dispositivi.
- Identificare automaticamente i dispositivi presenti in una rete cablata o WiFi e infettarli tramite le regole di identificazione e infezione di RCS.
- Identificare manualmente i dispositivi presenti in una rete cablata o WiFi e infettarli tramite le regole di infezione di RCS (l'identificazione è a carico dell'operatore).
- Connettersi a una rete WiFi protetta per ottenerne la password.
- Emulare un Access Point di una rete WiFi utilizzata normalmente dal target.
- Sbloccare la password del sistema operativo del computer del target.
- Configurare l'accesso remoto all'applicativo.

NOTA: la rete di infezione può essere una rete esterna oppure una rete WiFi aperta simulata dallo stesso Tactical Control Center.

## Sincronizzazione con il server RCS

Tactical Control Center si sincronizza con RCS per ricevere le regole di infezione aggiornate, per controllare se è disponibile una nuova versione del Appliance Control Center e per inviare i log.

La sincronizzazione può avvenire in due modi:

- manualmente, almeno la prima volta per ricevere le regole di infezione.
- automaticamente con una infezione in corso.

Durante la sincronizzazione, il Network Injector comunica con RCS a intervalli di tempo prestabiliti (circa 30 sec.).

La comunicazione avviene tramite un Anonymizer. Da Tactical Control Center, dalla scheda **System Management** si configura l'Anonymizer da utilizzzare per la sincronizzazione con RCS e si può decidere quando abilitare la sincronizzazione.

## Chiave di autenticazione

Per comunicare in sicurezza con il server RCS, sul Network Injector deve essere installata una chiave di autenticazione. La chiave deve essere generata quando si crea l'oggetto Network Injector sulla RCS Console e installata tramite Tactical Control Center alla prima sincronizzazione del Network Injector con RCS.

## Aggiornamento delle regole di infezione

Se il traffico generato dal target non è infettabile con le regole presenti nel Network Injector è necessario richiedere l'intervento di un operatore sulla RCS Console per generare nuove regole e aggiornare il Network Injector. Alla successiva sincronizzazione Tactical Control Center riceve le nuove regole e sarà possibile visualizzarle e abilitarle per l'infezione.

## Utilizzo delle interfacce di rete

In fase di attacco sono disponibili due diverse interfacce di rete, una per lo sniffing e una per l'infezione. L'utilizzo di due interfacce separate è indicato per garantire una continuità soprattutto nello sniffing.

In fase di emulazione dell'Access Point e in fase di acquisizione della password di rete si lavora con la sola interfaccia di sniffing.

Le interfacce di sniffing possono essere interne o esterne: le interfacce esterne sono indicate per lo sniffing perché la velocità di trasmissione è migliore.

## Processo di infezione tramite identificazione automatica

Di seguito i passaggi tipici per infettare dispositivi identificati automaticamente dalle regole di RCS. L'attacco può essere sferrato su reti cablate o WiFi:

| *Fase* | *Descrizione* | *Dove* |
|---|---|---|
| **1** | Preparare le regole di identificazione e infezione per i dispositivi target conosciuti che si vogliono attaccare. Inviare le regole al Tactical Network Injector. | *RCS Console, System, Network Injectors* |
| **2** | Abilitare la sincronizzazione con RCS per ricevere le regole aggiornate e abilitare le regole da utilizzare per l'infezione. | *Tactical Network Injector, Network Injector* |
| **3** | Se i dispositivi target sono connessi a una rete WiFi protetta acquisirne la password. | *Tactical Network Injector, Wireless Intruder* |

| *Fase* | *Descrizione* | *Dove* |
|---|---|---|
| **4** | Il sistema fa lo sniffing del traffico, identifica i dispositivi target grazie alle regole di identificazione e li infetta grazie alle regole di infezione. | *Tactical Network Injector, Network Injector* |
| **5** | Se necessario, forzare una ri-autenticazione di eventuali dispositivi che le regole non sono riuscite a individuare. | |

## Processo di infezione tramite identificazione manuale

Di seguito i passaggi tipici per infettare dispositivi identificati manualmente. L'obiettivo dell'operatore è individuare i dispositivi target.

L'attacco può essere sferrato su reti cablate o WiFi:

| *Fase* | *Descrizione* | *Dove* |
|---|---|---|
| **1** | Preparare le regole di identificazione che prevedono l'intervento manuale e le regole di infezione per tutti i tipi di dispositivi target che si vogliono attaccare. Inviare le regole al Tactical Network Injector. | *RCS Console, System, Network Injectors* |
| **2** | Abilitare la sincronizzazione con RCS per ricevere le regole aggiornate e abilitare le regole da utilizzare per l'infezione. | *Tactical Network Injector, Network Injector* |
| **3** | Se i dispositivi target sono connessi a una rete WiFi protetta acquisirne la password. | *Tactical Network Injector, Wireless Intruder* |
| **4** | Se i dispositivi target possono connettersi a una rete WiFi aperta, provare a emulare un Access Point conosciuto dai target. | *Tactical Network Injector,Fake Access Point* |
| **5** | Il sistema propone tutti i dispositivi connessi all'interfaccia di rete selezionata. Utilizzare i filtri per cercare i dispositivi target oppure controllare la cronologia web di ogni dispositivo. | *Tactical Network Injector, Network Injector* |
| **6** | Selezionare i dispositivi e infettarli. | |

## Acquisizione password di rete WiFi protetta

Se il dispositivo target è collegato a una rete WiFi protetta occorre ottenerne la password di accesso per poter entrare.

La funzione **Wireless intruder** permette di collegarsi a una rete WiFi e fare il cracking della password. Per le reti con protezioni WPA e WPA 2, oltre al dizionario standard è possibile caricare un dizionario aggiuntivo. La password viene visualizzata e l'operatore la può copiare per utilizzarla con la funzione di sniffing e infezione (funzione **Network Injector**).

## Forzatura dell'autenticazione dei dispositivi sconosciuti

In una rete WiFi protetta con password, è probabile non riuscire ad agganciare qualche dispositivo. I dispositivi di questo tipo compariranno nell'elenco come sconosciuti.

In questo caso è possibile forzare una loro autenticazione: il dispositivo si disconnette dalla rete per riconnettersi ed essere identificato.

## Infezione tramite identificazione automatica

Questa modalità di lavoro si adatta a scenari dove si hanno già alcune informazioni sul dispositivo target (es.: indirizzo IP).

In questo caso le regole di infezione provenienti da RCS contengono già tutti i dati necessari per identificare automaticamente i dispositivi target. Per ogni infezione è importante abilitare tutte e solo le regole utili in quel momento.

L'avvio dell'identificazione automatica da parte della funzione **Network Injector** mette mano a mano in evidenza i dispositivi target che vengono subito infettati dalle regole di infezione.

## Infezione tramite identificazione da operatore

Nelle regole di identificazione provenienti da RCS è possibile indicare che l'identificazione sarà a cura dell'operatore. Questa prassi è frequente quando a priori non si hanno informazioni sul dispositivo da infettare e occorre identificarlo direttamente sul campo.

In questo caso l'operatore ha a disposizione una serie di funzioni per selezionare i dispositivi connessi alla rete:

- può impostare dei filtri sul traffico intercettato: solo i dispositivi che rispondono ai criteri vengono infettati.
- può controllare la cronologia di ogni dispositivo per determinare se è quello da infettare.

Una volta determinati i dispositivi target è sufficiente selezionarli e avviare l'infezione: le regole di identificazione vengono "personalizzate" con i dati dei dispositivi per permettere alle regole di infezione di agire.

NOTA: è comunque possibile infettare manualmente dispositivi che sono già stati infettati tramite identificazione automatica.

## Impostazione di filtri sul traffico intercettato

Nel caso di identificazione dei target tramite operatore, ci si potrebbe trovare in uno scenario con una rete con diversi dispositivi connessi dei quali però non si riesce a individuare il dispositivo target. In questo caso è possibile utilizzare la funzione **Network Injector** per impostare dei filtri sul traffico intercettato.

Tactical Control Center mette a disposizione due tipi di filtri:

- espressioni regolari
- BPF (Berkeley Packet Filter) di rete

**Filtro con espressioni regolari**

Le espressioni regolari sono un filtro ad ampio spettro. Per esempio se il nostro target sta consultando una pagina di Facebook e sta parlando di windsurf è sufficiente inserire la parola "facebook" oppure la parola "windsurf".

Tactical Network Injector intercetta tutto il traffico dati e cerca le parole inserite.

Per una descrizione dettagliata di tutte le espressioni regolari ammesse fare riferimento a https://en.wikipedia.org/wiki/Regular_expression.

**Filtro BPF (Berkeley Packet Filter) di rete**

Serve per filtrare con maggiore precisione i dispositivi utilizzando la sintassi BPF. Questa sintassi prevede l'inserimento di parole chiave accompagnate da qualificatori:

- *qualificatori di tipo* (es.: **host**, **net**, **port**) indicano il tipo dell'oggetto cercato
- *qualificatori di direzione* (es.: **src**, **dst**) indicano la direzione dei dati cercati
- *qualificatori di protocollo* (es.: **ether**, **wlan**, **ip**) indicano il protocollo usato dall'oggetto cercato

*Es.: se il nostro target sta consultando una pagina di Facebook possiamo inserire "**host** facebook.com".*

Per conoscere nel dettaglio tutti i qualificatori della sintassi fare riferimento alla pagina http://wiki.wireshark.org/CaptureFilters.

## Individuazione del target tramite l'analisi della cronologia

Una ulteriore possibilità per filtrare e ridurre l'elenco dei possibili target, è analizzare il traffico web di ogni dispositivo per riconoscerlo come target.

## Emulazione di un Access Point conosciuto dal target

In certi scenari è necessario attrarre i dispositivi target per potere intercettare i loro dati, identificarli e infettarli.

Per farlo Tactical Network Injector emula un Access Point già registrato sul dispositivo target.

In questo modo, se il dispositivo è abilitato alla connessione automatica alle reti WiFi disponibili, appena entra nell'area WiFi si connette automaticamente all'Access Point emulato dal Tactical Network Injector.

**Sblocco della password di un sistema operativo**

È possibile sbloccare la password di un sistema operativo. Per saperne di più *vedi "**Cose da sapere per lo sblocco della password del sistema operativo**" a pagina 78*.

**Accesso remoto al Tactical Control Center**

È possibile accedere al Tactical Control Center da remoto. Per saperne di più *vedi "**Cose da sapere per l'accesso remoto al Control Center**" a pagina 79*.

# Cose da sapere per individuare la password di rete WiFi

## Introduzione

Il Tactical Control Center prevede tre tipi di attacco per individuare della password di reti WiFi protette (**Wireless Intruder**):

- WPA/WPA2 dictionary attack
- WEP bruteforce attack
- WPS PIN bruteforce attack

## WPA/WPA2 dictionary attack

Per eseguire questo attacco, il sistema individua gli handshake tra il client e il punto di accesso e cerca di scoprire la password utilizzando un dizionario di parole comuni.

L'handshake viene salvato nella cartella /opt/td-config/run/besside/wpa.cap. Se necessario, è possibile copiare l'handshake e provare l'attacco con un'altra macchina più potente.

Una volta che il sistema ha individuato l'handshake, l'attacco può continuare anche senza rimanere nel raggio di copertura della rete WiFi.

L'attacco può richiedere molto tempo, proporzionale alla lunghezza del dizionario. L'attacco fallisce se la password non si trova all'interno del dizionario di parole comuni.

## WEP bruteforce attack

Per eseguire questo attacco, il sistema fa una infezione simulando uno dei client connessi alla rete e raccoglie i dati per forzare la password cifrata. Nella rete deve quindi esserci collegato almeno un client.

L'attacco dura tra i 10 e i 15 minuti circa e per tutta la sua durata, il portatile deve rimanere nel raggio di copertura della rete WiFi.

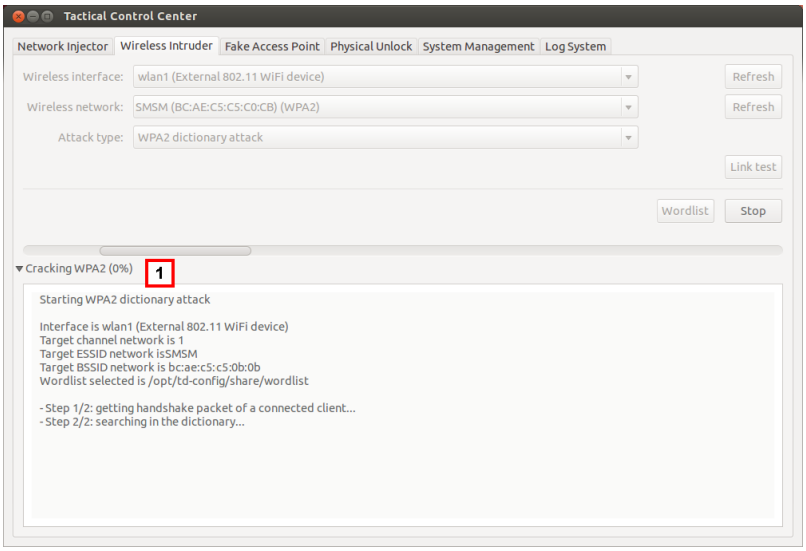
## WPS PIN bruteforce attack

Per eseguire questo attacco, il sistema prova tutte le possibili combinazioni per recuperare la configurazione del punto di accesso tramite un protocollo WiFi Protected Setup.

L'attacco può richiedere molto tempo e per tutta la sua durata il portatile deve rimanere nel raggio di copertura della rete WiFi.

## Stato di avanzamento dell'attacco

Nella scheda **Wireless Intruder** dell'applicativo **Tactical Control Center** è possibile visualizzare la percentuale di avanzamento dell'attacco **[1]** (WPA/WPA2 e WPS) o il numero di Vettori di Inizializzazione catturati (WEP).




# Cose da sapere per lo sblocco della password del sistema operativo

## Introduzione

Tramite connessione FireWire o Thunderbolt con il computer target, Tactical Network Injector può accedere alla RAM del computer del target per individuare e sbloccare la password del sistema operativo. Il computer può essere così, per esempio, attaccato con infezioni fisiche (es. tramite Silent Installer).

NOTA: questa operazione coinvolge solo la RAM del computer target: se il computer viene spento e/o riavviato non rimane traccia dell'operazione eseguita.

La scheda **Physical Unlock** del Tactical Control Center permette di eseguire l'operazione di sblocco ed eventuale blocco della password.

## Requisiti del Tactical Network Injector

A seconda del tipo di connessione che si vuole realizzare (FireWire o Thunderbolt) devono essere utilizzati gli accessori specifici:

- adattatore ExpressCard/34
- cavo

## Requisiti del computer target

L'operazione può avvenire con successo solo se il computer del target risponde ai seguenti requisiti:

- memoria RAM di dimensione massima 4 GB
- attacco per la connessione FireWire o Thunderbolt (porta integrata o con adattatore)

### Processo standard

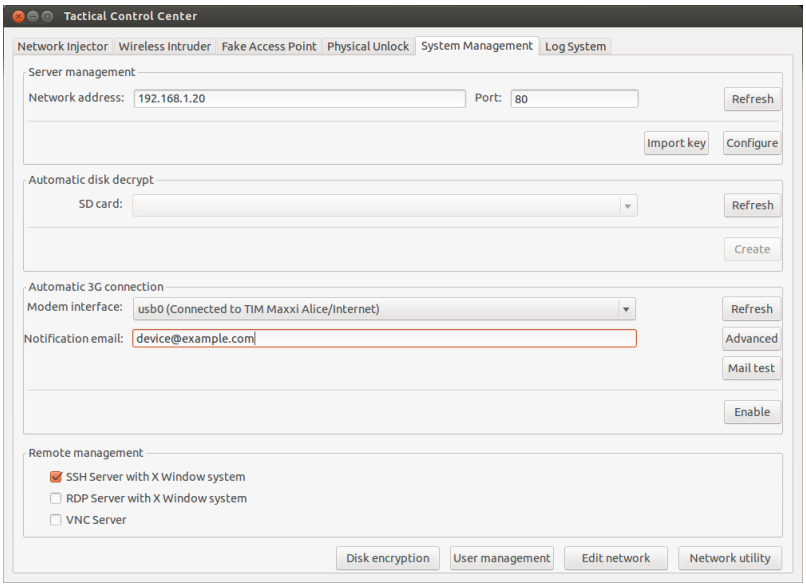
| *Fase* | *Descrizione* |
|---|---|
| **1** | L'operatore:<br>• collega fisicamente Tactical Network Injector e il computer del target tramite connessione FireWire o Thunderbolt<br>• avvia la procedura di sblocco della password del sistema operativo tramite la scheda **Physical Unlock** del Tactical Control Center |
| **2** | Tactical Network Injector:<br>• legge la memoria RAM del computer (*memory dump*)<br>• individua la porzione di memoria dedicata alla password del sistema operativo<br>• utilizza questa informazione per sbloccare il sistema operativo e comunica all'operatore il risultato dell'operazione |
| **3** | L'operatore:<br>• accede al computer del target utilizzando una password vuota (premendo semplicemente Enter nella pagina di login) oppure una password qualsiasi di almeno 8 caratteri.<br>• effettua le operazioni sul computer del target, per esempio infezione fisica (es.: tramite Silent Installer)<br>• se lo desidera, avvia la procedura di blocco con password del sistema operativo tramite la scheda **Physical Unlock** del Tactical Control Center |

# Cose da sapere per l'accesso remoto al Control Center

## Introduzione

È possibile accedere al Tactical Control Center e all'Appliance Control Center da remoto. La scheda **System Management** degli applicativi permette di configurare questa possibilità.

Ecco come si presenta, per esempio, la scheda nel Tactical Control Center.




In particolare, per l'accesso remoto sono necessari:

- Password del disco cifrato (solo Tactical Control Center)
- Modem 3G per la connessione
- Indirizzo IP del dispositivo
- Protocollo di rete

## Password del disco (solo Tactical Control Center)

Il portatile Tactical Network Injector ha il disco cifrato e a ogni riavvio richiede la password del disco. Per non dovere inserire manualmente la password è possibile salvarla su una scheda di memoria SD e lasciare la scheda inserita (preferibilmente nello slot schede SD integrato nel portatile).

NOTA: la password non corrisponde a quella del sistema. Quindi la scheda SD non contiene informazioni che possono essere utilizzate da estranei per accedere al sistema operativo.

Per cambiare la password è sufficiente generarne una nuova.

## Modem 3G per la connessione

Il modem 3G definito in **Modem Interface** viene utilizzato per connettere alla rete il dispositivo.

Con il modem abilitato, se il sistema si disconnette o si riavvia, la connessione viene ristabilita automaticamente.

Suggerimento: per maggiore sicurezza, utilizzare il modem 3G integrato nel portatile piuttosto che modem esterni.

### Indirizzo IP del dispositivo

Se configurato, ogni volta che il sistema si connette invia una e-mail all'indirizzo specificato in **Notification email** con l'indirizzo IP del dispositivo.

Se l'indirizzo IP è dinamico, è necessario attendere una e-mail con l'indirizzo a cui collegarsi.

Se l'indirizzo IP è statico, si può decidere comunque di abilitare l'invio della e-mail per essere informati che il dispositivo è connesso.

### Modalità di invio dell'e-mail con l'indirizzo IP

Per inviare l'e-mail si può utilizzare la configurazione automatica che prevede come server di posta il dispositivo stesso, oppure specificare manualmente un server di posta.

Se viene utilizzata la configurazione automatica l'indirizzo e-mail mittente è `root@hostname.local`, dove `hostname` è l'host del dispositivo. Altrimenti sarà quello specificato.

Per verificare se la comunicazione avviene in modo corretto, inviare una e-mail di prova.

### Protocollo di rete

La comunicazione avviene attraverso il protocollo di rete specificato nella sezione **Remote Management**.

### Altre funzioni utili

Dalla scheda **System Management** è possibile accedere direttamente ad alcuni pannelli utili del sistema operativo, attraverso i seguenti pulsanti:

- **Disk encryption**: per cambiare la password di protezione del disco (solo Tactical Control Center)
- **User management**: per modificare utenti e gruppi di utenti
- **Edit Network**: per modificare le impostazioni di rete
- **Network utility**: per eseguire diagnostiche di rete

# Comandi Tactical Control Center e Appliance Control Center

### Introduzione

Sono disponibili alcuni comandi da terminale per gestire gli applicativi Tactical Control Center e Appliance Control Center.

NOTA: per eseguire i comandi è necessario possedere i privilegi di Amministratore.

### Comandi

Di seguito i comandi disponibili per Tactical Control Center e per Appliance Control Center:

| *Comando Tactical Control Center* | *Comando Appliance Control Center* | *Funzione* |
|---|---|---|
| `tactical` | `appliance` | Avvia l'applicativo. |
| `tactical -d` oppure `tactical --desync` | `appliance -d` oppure `appliance --desync` | Dissocia il sistema dal server RCS con cui è attualmente sincronizzato. |
| `tactical -l` oppure `tactical --log` | `appliance -l` oppure `appliance --log` | Visualizza i log del processo di infezione in corso.<br>NOTA: la finestra dell'applicativo deve essere aperta. |
| `tactical -s` oppure `tactical --show-logs` | `appliance -s` oppure `appliance --show-logs` | Visualizza tutti i file di log salvati nel file system. |
| `tactical - r` oppure `tactical --report` | `appliance - r` oppure `appliance --report` | Crea un report del sistema e lo salva nella cartella Home dell'utente. |
| `tactical - v` oppure `tactical --version` | `appliance - v` oppure `appliance --version` | Visualizza la versione dell'applicativo. |
| `tactical -h` oppure `tactical --help` | `appliance -h` oppure `appliance --help` | Visualizza i comandi disponibili. |

# Appliance Control Center

## Scopo

Appliance Control Center permette di:

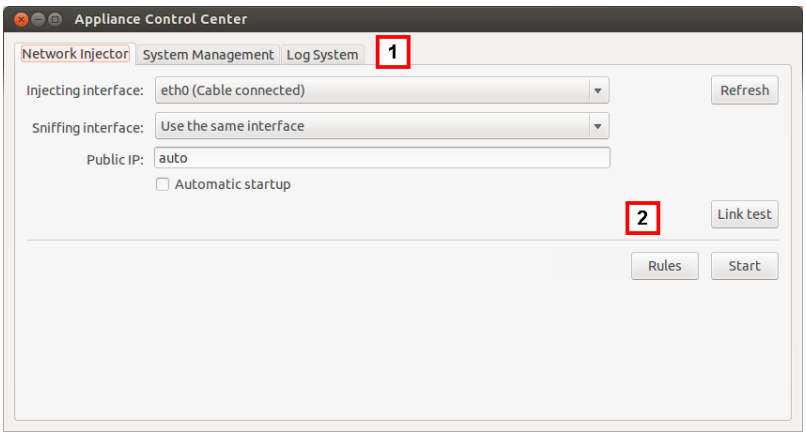
- gestire le infezioni del Network Injector Appliance
- sincronizzare il Network Injector Appliance con il server RCS per ricevere aggiornamenti e inviare log
- configurare l'accesso remoto all'applicativo

## Richiesta della password

All'avvio Appliance Control Center chiede la password di accesso, la stessa del portatile su cui si sta lavorando.

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Schede per l'accesso alle singole applicazioni. Di seguito la descrizione: |

| *Funzione* | *Descrizione* |
|---|---|
| **Network Injector** | Gestisce lo sniffing e l'infezione dei dispositivi del target, sincronizza le regole RCS e aggiorna i dispositivi Appliance. |
| **System Management** | Configura l'Anonymizer per la comunicazione con RCS, abilita la sincronizzazione manuale con RCS e configura l'accesso remoto all'applicativo. |
| **Log System** | Visualizza i log. |

| | |
|---|---|
| **2** | Area con i pulsanti specifici della scheda. |

## Per saperne di più

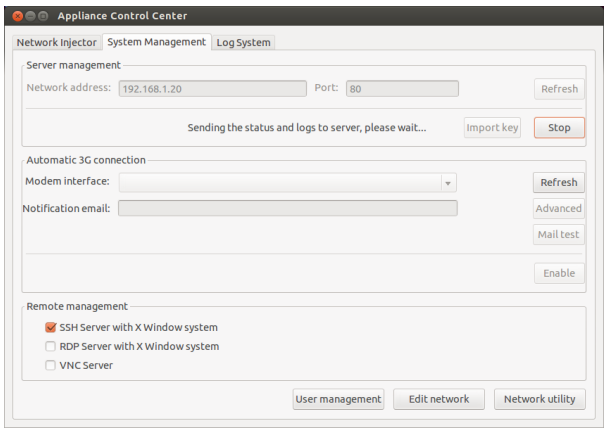
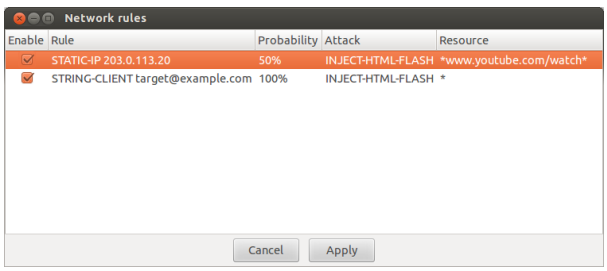
Per saperne di più sul Appliance Control Center *vedi "Cose da sapere su Appliance Control Center" a pagina 70*.

Per la descrizione dei dati del Appliance Control Center*vedi "Dati Appliance Control Center" a pagina 89*

## Abilitare la sincronizzazione con il server RCS per ricevere nuove regole

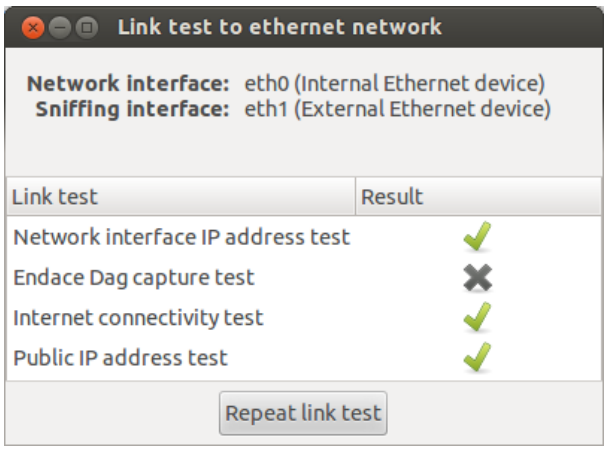
Di seguito la procedura per abilitare la sincronizzazione con il server RCS per ricevere le regole aggiornate:

NOTA: se è in corso una infezione il Network Injector è già sincronizzato con il server RCS e quindi le regole vengono caricate automaticamente. Andare direttamente al passo 4.
*Vedi "Verifica dello stato dei Network Injector " a pagina 69*

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **System Management** fare clic sul pulsante **Configure**: la sincronizzazione viene abilitata.<br>2. Durante la sincronizzazione, il Network Injector interroga RCS ogni 30 secondi. Allo scadere del primo intervallo saranno ricevute le regole di infezione inviate. |  |
| **IMPORTANTE: gli aggiornamenti vengono ricevuti solo se è stato fatto l'invio da RCS Console.** ***Vedi "Gestione dei Network Injector" a pagina 62*** | |
| **IMPORTANTE: abilitare regolarmente la sincronizzazione per garantire un aggiornamento costante dalla sede operativa.** | |
| 3. Per interrompere la sincronizzazione fare clic su **Stop**.<br>4. Per visualizzare le regole ricevute da RCS Console, nella scheda **Network Injector** fare clic su **Rules**: compaiono tutte le regole per il Network Injector. |  |
| **IMPORTANTE: controllare l'effettiva sincronizzazione delle regole dopo aver chiesto a RCS Console un loro aggiornamento.** | |

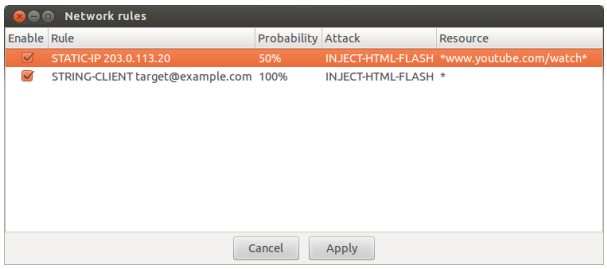
## Avviare un test della rete

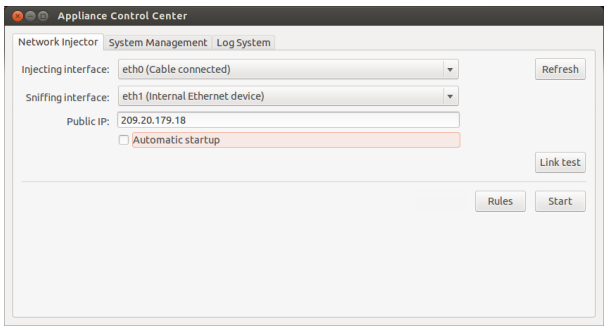
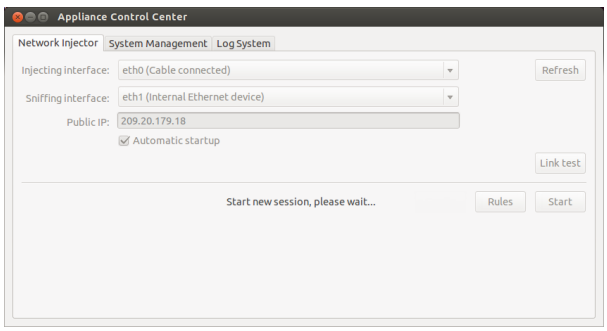
Di seguito la procedura per verificare la rete per lo sniffing e/o infezione:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** selezionare l'interfaccia di rete.<br>2. Fare clic sul pulsante **Link test**: compare una finestra con i risultati del test.<br>3. Se il test non ha successo, rivedere la configurazione di rete desiderata e ripetere il test.<br><br>**IMPORTANTE: l'attacco non può andare a buon fine se il test non ha successo.** |  |

## Infettare i target tramite identificazione automatica

Per avviare l'identificazione e l'infezione automatica:

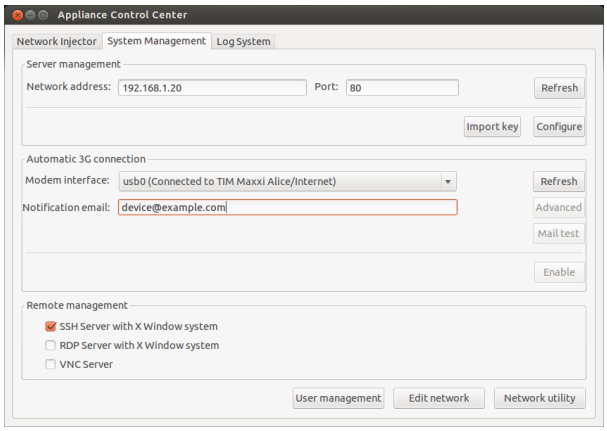
| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** fare clic su **Rules**: compaiono tutte le regole disponibili per il Network Injector.<br>2. Abilitare tutte e solo le regole che si vogliono utilizzare per l'infezione, selezionando la casella di controllo **Enable** corrispondente.<br>3. Per confermare, fare clic su **Apply**. |  |

| *Passi* | *Risultato* |
|---|---|
| 4. Selezionare nella casella di riepilogo **Injecting Interface** l'interfaccia di rete per l'infezione.<br>5. Nella casella di riepilogo **Sniffing interface** selezionare una diversa interfaccia di rete da usare per lo sniffing oppure scegliere la stessa interfaccia usata per l'infezione.<br>Suggerimento: usare due interfacce di rete diverse garantisce una migliore identificazione dei dispositivi.<br>NOTA: le interfacce Endace (DAG), ovvero le interfacce di sniffing compaiono in **Sniffing Interface**.<br>6. Fare clic su **Automatic Startup** se si desidera che l'infezione riparta automaticamente senza alcun intervento umano anche in seguito di riavvio o spegnimento dell'Appliance Network Injector.<br>7. Fare clic su **Start**.<br>**IMPORTANTE: Appliance Control Center permette di configurare, avviare l'infezione e chiudere lo stesso Appliance Control Center lasciando l'infezione in corso. Alla successiva riapertura con infezione in corso comparirà il pulsante Stop invece del pulsante Start. Questo permette di configurare una nuova infezione e avviarla .**<br>NOTA: è possibile abilitare/disabilitare le regole anche con l'infezione in corso, facendo clic su **Rules**. |  <br>  |

| *Passi* | *Risultato* |
|---|---|
| 8. Per fermare l'infezione fare clic su **Stop**. Oppure chiudere la finestra se si desidera lasciare attiva l'infezione. | |
| Suggerimento: chiudere la finestra per permettere al sistema di avviare in automatico eventuali aggiornamenti dell'Appliance Control Center. | - |

## Configurare l'accesso remoto all'applicativo

Per poter accedere all'Appliance Control Center da remoto:

| *Passi* | *Risultato* |
|---|---|
| 1. Collegare il modem al dispositivo.<br>2. Nella scheda **System Management** fare clic su **Refresh**: il sistema riconosce il modem e lo visualizza in **Modem Interface**.<br>3. Se sono presenti più modem, selezionare nella casella di riepilogo **Modem Interface** il modem desiderato.<br>4. Se si desidera abilitare l'invio dell'e-mail con l'indirizzo IP del dispositivo a ogni connessione, eseguire i seguenti passi:<br>a. In **Notification e-mail** inserire l'indirizzo e-mail a cui inviare l'e-mail.<br>b. Fare clic su **Mail test** per inviare una e-mail di prova.<br>c. Se l'e-mail non arriva, fare clic su **Advanced** per configurare manualmente il server di posta: appare la finestra **Email advanced configuration.**<br>d. Inserire i dati richiesti e fare clic su **Save.**<br>e. Fare clic su **Mail test** per inviare una e-mail di prova con il server configurato.<br>5. Per abilitare la connessione automatica con il modem selezionato, fare clic su **Enable.**<br>6. Selezionare il protocollo di rete da utilizzare per l'accesso remoto.<br>NOTA: è possibile accedere direttamente ad alcuni pannelli utili del sistema operativo attraverso i pulsanti in basso nella scheda. *Vedi "**Cose da sapere per l'accesso remoto al Control Center**" a pagina 79.* |  |

## Visualizzare i dettagli dell'infezione

Per visualizzare i log della sessione corrente selezionare la scheda **Log System**.

Per visualizzare tutti i file di log, nella scheda **Log System**, fare clic su **Show logs**.

NOTA: tutti i file di log sono salvati nel file system in /var/log/td-config .

# Dati Appliance Control Center

## Dati della scheda Network Injector

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Injecting interface** | Elenco delle interfacce di rete già connesse. Selezionare l'interfaccia di infezione connessa alla rete dove è collegato il dispositivo da attaccare. |
| **Sniffing interface** | Come **Injecting Interface** oppure altra interfaccia di rete da utilizzare solo per lo sniffing.<br>NOTA: Se il sistema dispone di una scheda Endace DAG per connessioni Gigabit, la scheda sarà rilevata e visualizzata in questo elenco. |
| **Public IP** | Permette di specificare un indirizzo IP pubblico da mappare sull'indirizzo IP privato dell'interfaccia di infezione. Se si inserisce "auto", il sistema utilizza l'indirizzo IP preconfigurato sull'interfaccia di infezione e segnala con un messaggio se si tratta di un indirizzo IP privato. |
| **Automatic Startup** | Fa ripartire automaticamente l'infezione senza alcun intervento umano anche in seguito di riavvio o spegnimento dell'Appliance Network Injector.<br>**IMPORTANTE: Se questa opzione non viene selezionata non ci sarà alcuna partenza automatica dell'infezione.** |

## Dati scheda System Management

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Network address** | Indirizzo IP dell'Anonymizer utilizzato per comunicare con il server RCS. |
| **Port** | Porta di comunicazione con l'Anonymizer. |
| **Modem interface** | Modem 3G per la connessione del dispositivo. |

| *Dato* | *Descrizione* |
|---|---|
| **Notification email** | Indirizzo e-mail a cui inviare l'indirizzo IP del dispositivo ogni volta che si connette alla rete.<br>**IMPORTANTE: campo da compilare obbligatoriamente in caso di indirizzo IP dinamico.** |
| **Remote management** | Protocollo di rete per l'accesso remoto. |

# Tactical Control Center

## Scopo

Tactical Control Center permette di:

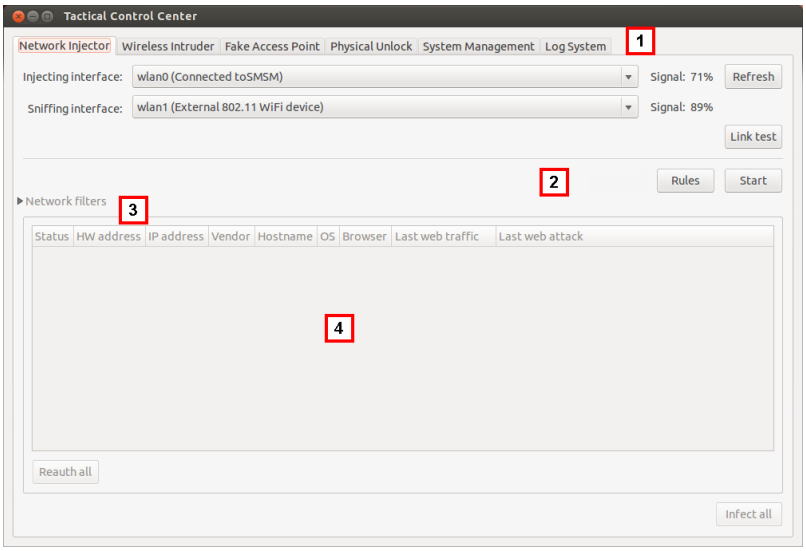
- gestire le infezioni del Tactical Network Injector
- sincronizzare il Network Injector Appliance con il server RCS per ricevere aggiornamenti e inviare log
- sbloccare la password del sistema operativo del computer del target
- configurare l'accesso remoto all'applicativo

## Richiesta della password

All'avvio Tactical Control Center chiede la password di accesso, la stessa del portatile su cui si sta lavorando.

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:



| *Area* | *Descrizione* |
|---|---|
| **1** | Schede per l'accesso alle singole applicazioni. Di seguito la descrizione: |

| *Funzione* | *Descrizione* |
|---|---|
| **Network injector** | Gestisce lo sniffing e l'infezione dei dispositivi del target, sincronizza le regole RCS, aggiorna i dispositivi Tactical e mostra le regole attualmente presenti sul Tactical Network Injector. |
| **Wireless Intruder** | Entra in una rete WiFi protetta tramite individuazione password. |
| **Fake Access Point** | Emula un Access Point. |
| **Physical Unlock** | Sblocca la password di un sistema operativo. |
| **System Management** | Configura l'Anonymizer per la comunicazione con RCS, abilita la sincronizzazione manuale con RCS e configura l'accesso remoto all'applicativo. |
| **Log System** | Visualizza i log. |

| | |
|---|---|
| **2** | Area con i pulsanti specifici della scheda. |
| **3** | Filtri per filtrare traffico in Internet dei dispositivi. |
| **4** | Area con l'elenco dei dispositivi. |

## Per saperne di più

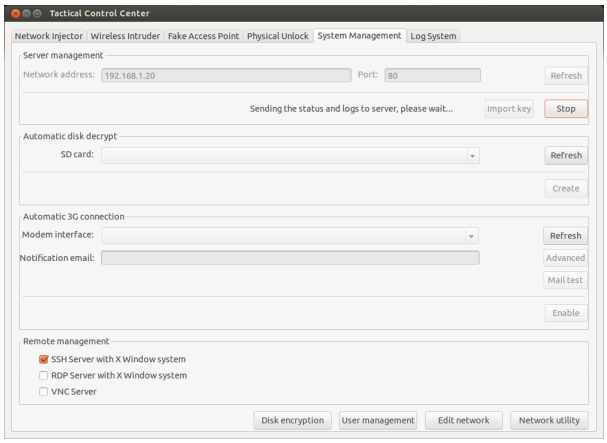
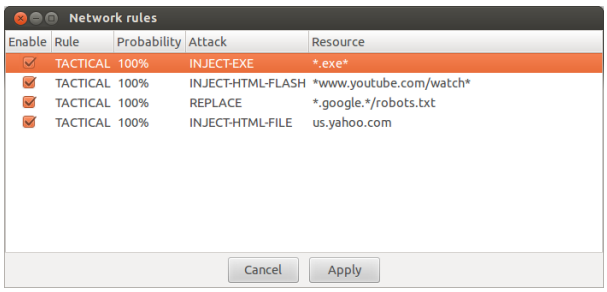
Per la descrizione dei dati del Tactical Control Center *vedi "**Dati del Tactical Control Center**" a pagina 107*.

Per saperne di più sul Tactical Control Center *vedi "**Cose da sapere su Tactical Control Center**" a pagina 72*.

## Abilitare la sincronizzazione con il server RCS per ricevere nuove regole

NOTA: se è in corso una infezione il Network Injector è già sincronizzato con il server RCS e quindi le regole vengono caricate automaticamente. Andare direttamente al passo 4.
*Vedi "**Verifica dello stato dei Network Injector** " a pagina 69*

Di seguito la procedura per abilitare la sincronizzazione con RCS per ricevere le regole aggiornate:

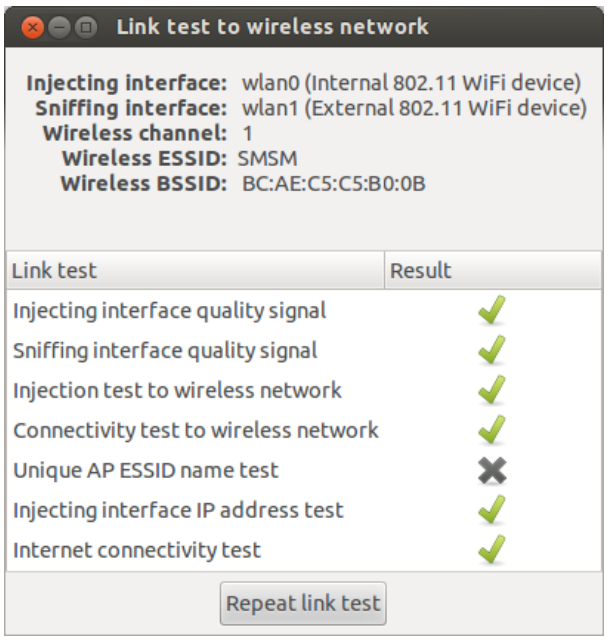
| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **System Management** fare clic sul pulsante **Configure**: la sincronizzazione viene abilitata. | |
| 2. Durante la sincronizzazione, il Network Injector interroga RCS ogni 30 secondi. Allo scadere del prossimo intervallo saranno ricevute le regole di infezione inviate. |  |
| **IMPORTANTE: gli aggiornamenti vengono ricevuti solo se è stato fatto l'invio da RCS Console.** ***Vedi "Gestione dei Network Injector" a pagina 62*** | |
| **IMPORTANTE: abilitare regolarmente la sincronizzazione per garantire un aggiornamento costante dalla sede operativa.** | |
| 3. Per interrompere la sincronizzazione fare clic su **Stop**. | |
| 4. Per visualizzare le regole ricevute da RCS Console, nella scheda **Network Injector** fare clic su **Rules**: compaiono tutte le regole per il Network Injector. |  |
| **IMPORTANTE: controllare l'effettiva sincronizzazione delle regole dopo aver chiesto a RCS Console un loro aggiornamento.** | |





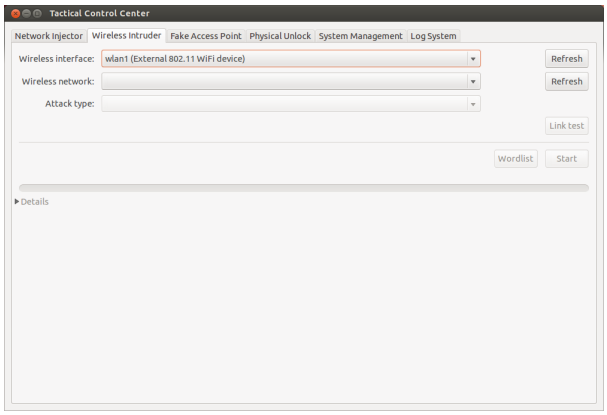
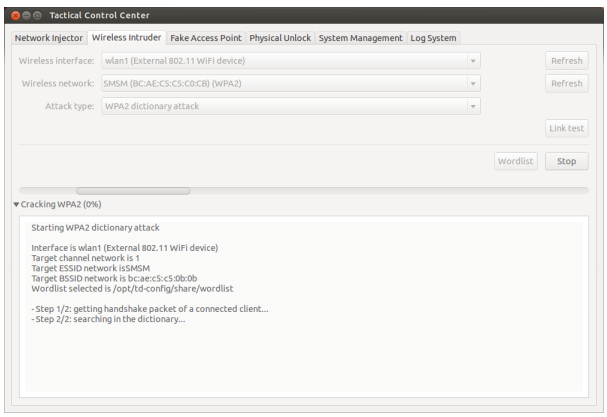
## Avviare un test della rete

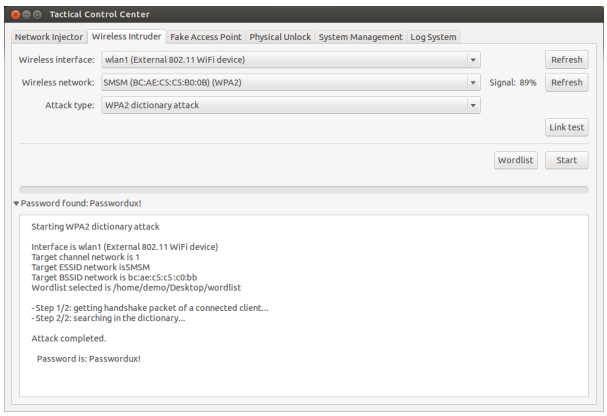
Di seguito la procedura per verificare la rete per lo sniffing e/o infezione:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** o nella scheda **Wireless Intruder** o nella scheda **Fake Access Point** selezionare l'interfaccia di rete.<br>2. Fare clic sul pulsante **Link test**: compare una finestra dove compariranno i risultati del test.<br>3. Se il test non ha successo, spostarsi in una posizione migliore dove il segnale è più forte e ripetere il test.<br><br>**IMPORTANTE: l'attacco non può andare a buon fine se il test non ha successo.** |  |

## Acquisire la password di una rete WiFi protetta

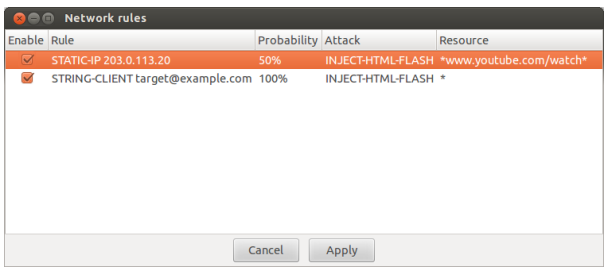
Di seguito la procedura per acquisire la password di una rete WiFi protetta:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Wireless Intruder** selezionare in **Wireless interface** l'interfaccia di rete WiFi.<br>2. Selezionare in **ESSID network** la rete di cui individuare la password.<br><br>NOTA: gestire da sistema operativo eventuale connessione/disconnessione di interfacce di rete e premere il pulsante **Refresh**.<br><br>3. In **Attack type** scegliere il tipo di attacco.<br>4. Se necessario fare clic su **Wordlist** per caricare un dizionario aggiuntivo per attaccare reti con protezione WPA o WPA 2.<br><br>**IMPORTANTE:**<br>**IMPORTANTE: il dizionario aggiuntivo deve essere caricato a ogni attacco.** |  |
| 5. Fare clic su **Start**: il sistema lancia diversi attacchi per rivelare la password di accesso.<br>6. Fare clic su **Stop** per fermare l'attacco. |  |

| *Passi* | *Risultato* |
|---|---|
| 7. Se gli attacchi hanno avuto successo, compare la password sopra all'indicatore di stato. |  |
| 8. Tramite il **Network Manager** del sistema operativo aprire la connessione verso la rete WiFi di cui si conosce la password. La password sarà memorizzata dal sistema e non sarà più necessario inserirla.<br>9. Aprire la sezione **Network Injector** per iniziare l'identificazione e l'infezione. | - |

## Infettare i target tramite identificazione automatica

Per avviare l'identificazione e l'infezione automatica:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** fare clic su **Rules**: compaiono tutte le regole disponibili per il Network Injector.<br>2. Abilitare tutte e solo le regole che si vogliono utilizzare per l'infezione, selezionando la casella di controllo **Enable** corrispondente.<br>3. Per confermare, fare clic su **Apply**. |  |

| *Passi* | *Risultato* |
|---|---|

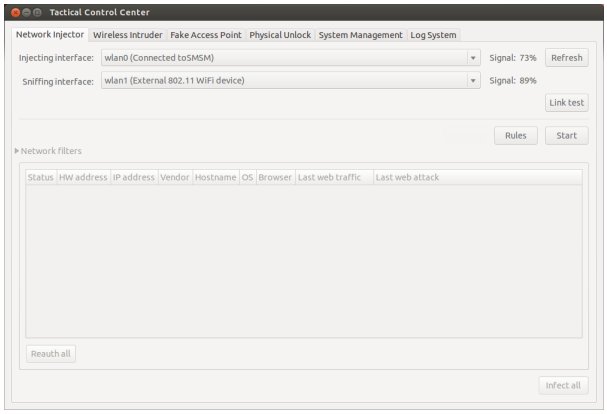
4. Nella scheda **Network Injector** selezionare nella casella di riepilogo **Injecting Interface** l'interfaccia di rete per l'infezione.
5. Nella casella di riepilogo **Sniffing interface** selezionare una diversa interfaccia di rete da usare per lo sniffing oppure scegliere la stessa interfaccia usata per l'infezione.

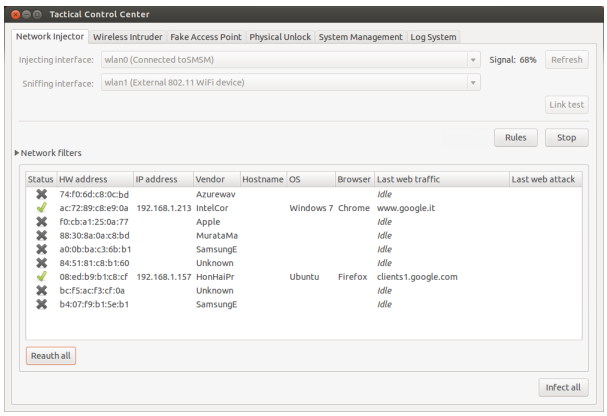
NOTA: gestire da sistema operativo eventuale connessione/disconnessione di interfacce di rete e premere il pulsante **Refresh**.

Suggerimento: usare due interfacce di rete diverse garantisce una migliore identificazione dei dispositivi.

6. Controllare la potenza del segnale e se necessario avviare il test della rete (pulsante **Link test**).

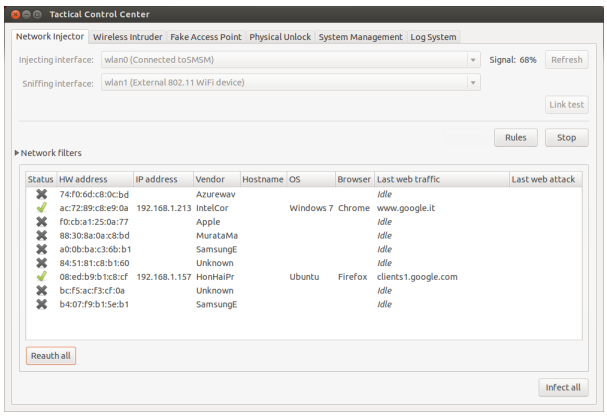
NOTA: la potenza del segnale deve essere almeno del 70%. Si avrà un unico valore se si usa la stessa interfaccia di rete per l'infezione e per lo sniffing.



| *Passi* | *Risultato* |
|---|---|
| 7. Fare clic su **Start:** si avvia il processo di sniffing della rete e compaiono tutti i dispositivi identificati come target. La colonna **Status** mostra lo stato dell'identificazione.<br><br>**AVVERTENZA: controllare bene lo stato dell'identificazione.** ***Vedi "Dati del Tactical Control Center" a pagina 107.*** |  |
| 8. I dispositivi target iniziano a essere infettati. Nel log viene registrato l'inizio dell'infezione.<br><br>NOTA: è possibile abilitare/disabilitare le regole anche con l'infezione in corso, facendo clic su **Rules**.<br><br>NOTA: i dispositivi non target non compaiono nell'elenco e sono quindi esclusi dall'infezione automatica. | |
| 9. Per fermare l'infezione fare clic su **Stop.** | - |

## Forzare l'autenticazione dei dispositivi sconosciuti

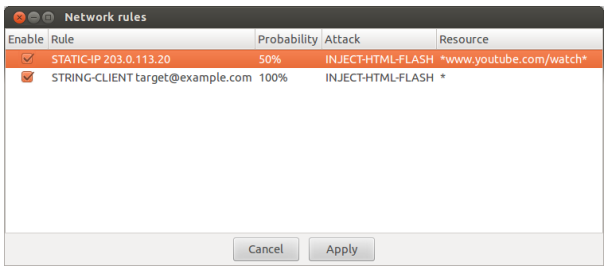
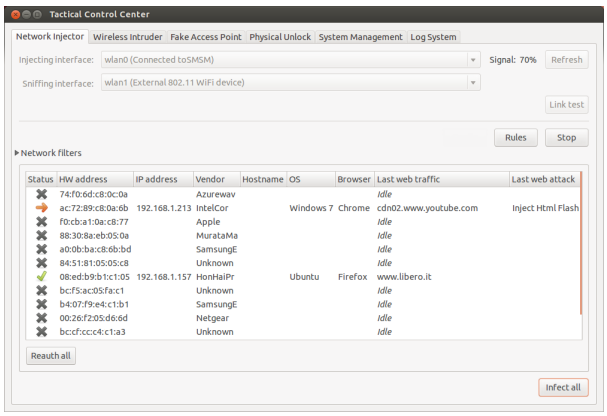
Per forzare un dispositivo sconosciuto ad autenticarsi:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector**, nell'elenco dei dispositivi, selezionare quelli sconosciuti (stato  ). |  |
| 2. Premere il pulsante **Reauth selected**: i dispositivi sono costretti a riautenticarsi.<br>  Suggerimento: in certi casi può essere necessario chiedere l'autenticazione di tutti i dispositivi presenti. Per farlo fare clic su **Reauth All**..<br>  NOTA: il pulsante **Reauth selected** è visualizzato se si selezionano dei dispositivi, **Reauth All** se nessun dispositivo è selezionato. | - |
| 3. Se la riautenticazione ha successo, viene avviata l'identificazione automatica: lo stato dei dispositivi sarà  e da adesso in poi sarà possibile infettarli. | - |



## Infettare i target tramite identificazione manuale

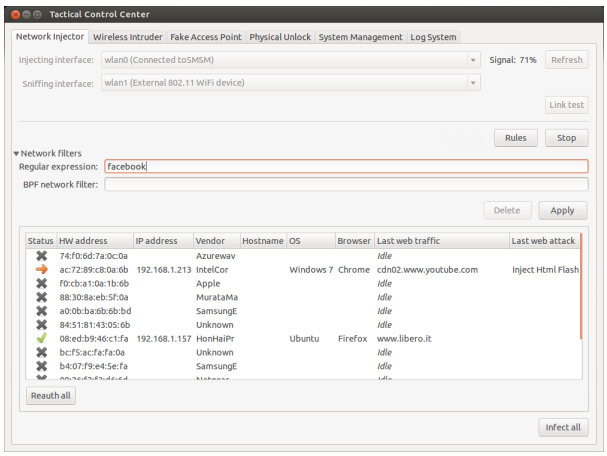
Per infettare manualmente i dispositivi in rete:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** fare clic su **Rules**: compaiono tutte le regole disponibili per il Network Injector.<br>2. Abilitare tutte e solo le regole che si vogliono utilizzare per l'infezione, selezionando la casella di controllo **Enable** corrispondente.<br>3. Per confermare, fare clic su **Apply**. |  |
| 4. In **Network Injector** nell'elenco dei dispositivi selezionare uno o più dispositivi da infettare identificandoli tramite i dati esposti.<br><br>Suggerimento: se i dispositivi nell'elenco sono tanti, usare i filtri di selezione. *Vedi "**Impostare i filtri sul traffico intercettato**" nella pagina di fronte*. |  |

| *Passi* | *Risultato* |
|---|---|
| 5. Fare clic sul pulsante **Infect selected**: tutte le regole di infezione vengono "personalizzate" con i dati del dispositivo e applicate. Nei log sarà visibile l'attacco verso i dispositivi.<br><br>**IMPORTANTE: questa operazione prevede la presenza di una regola speciale creata tramite RCS Console.**<br><br>Suggerimento: per infettare tutti i dispositivi connessi, anche quelli non target o non ancora connessi fare clic su **Infect All**.<br><br>NOTA: il pulsante **Infect selected** è visualizzato se si selezionano dei dispositivi, **Infect All** se nessun dispositivo è selezionato.<br><br>**Risultato** : se l'infezione è stata avviata con successo, lo stato dei dispositivi è  . | - |

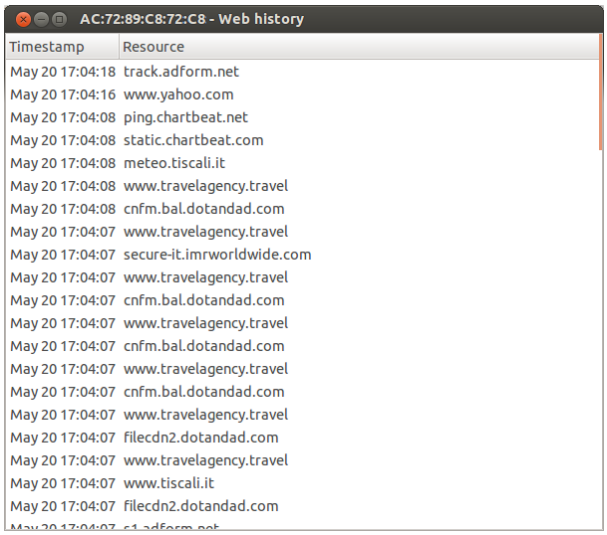
## Impostare i filtri sul traffico intercettato

Per selezionare i dispositivi target tramite filtri sul traffico dati:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector**, fare clic su **Network filters.**<br>2. Per una ricerca ad ampio raggio digitare una espressione regolare nella casella di testo **Regular expression**.<br>3. Per una ricerca più raffinata digitare una espressione BPF nella casella di testo **BPF Network Filter**.<br>**Risultato** : il sistema mostra nell'elenco solo i dispositivi filtrati. |  |
| 4. Procedere nell'infezione manuale come descritto dalla procedura *vedi "**Infettare i target tramite identificazione manuale** " a pagina 98*. | - |

## Individuare un target analizzando la cronologia web

Per individuare un target:

| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Network Injector** fare doppio clic sul dispositivo da controllare: si apre una finestra con la cronologia dei siti web visitati dal browser. |  |

| *Passi* | *Risultato* |
|---|---|
| 2. Se il dispositivo è quello target, chiudere la cronologia e procedere con la procedura *"Infettare i target tramite identificazione manuale " a pagina 98*. | - |

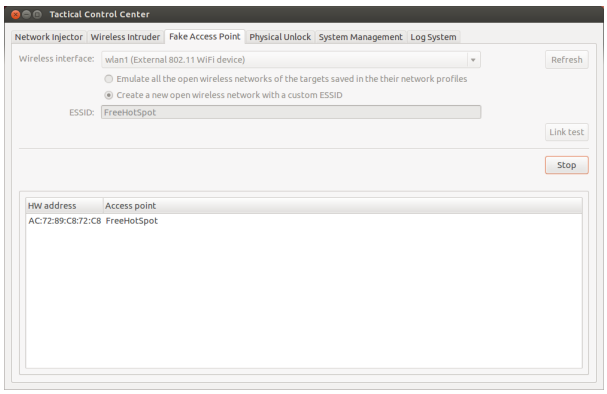
## Pulire i dispositivi erroneamente infettati

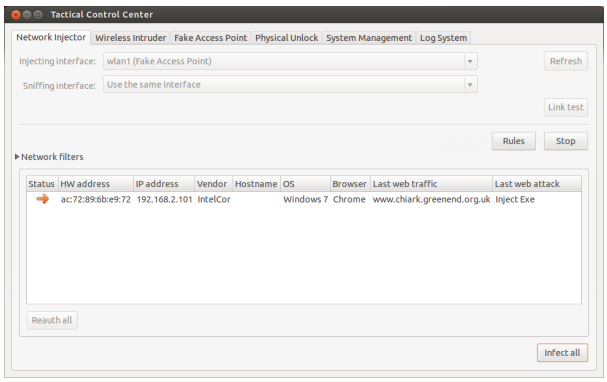
Per rimuovere l'infezione dai dispositivi è necessario agire su RCS Console, chiudendo l'agent.

## Emulare un Access Point conosciuto dal target

**IMPORTANTE: prima di attivare l'emulazione dell'Access Point, fermare un eventuale attacco attivo nella scheda Network Injector.**

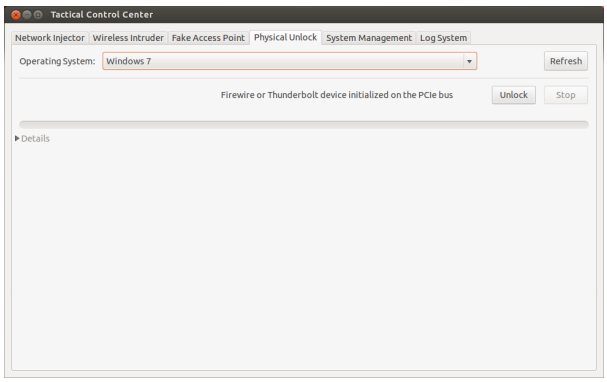
Per trasformare Tactical Network Injector in un Access Point conosciuto dai target:

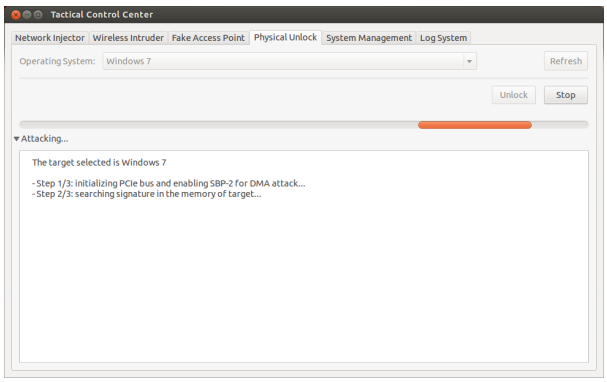
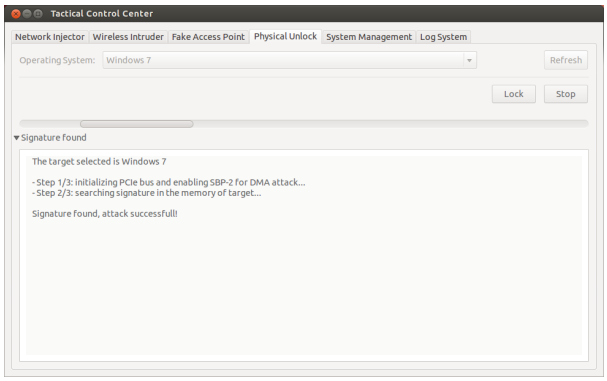
| *Passi* | *Risultato* |
|---|---|
| 1. Nella scheda **Fake Access Point** selezionare nella casella di riepilogo **Wireless Interface** l'interfaccia di rete su cui ci si vuole mettere in ascolto. |  |
| 2. Selezionare la tipologia di emulazione dell'Access Point. | - |
| 3. Fare clic su **Start**: Tactical Network Injector recupera i nomi delle reti WiFi cui i dispositivi sono soliti connettersi e li visualizza. | - |
| 4. Tactical Network Injectorstabilisce la comunicazione con i singoli dispositivi emulando l'access point di ogni rete. | |

| *Passi* | *Risultato* |
|---|---|
| 5. In **Network Injector**, nella casella di riepilogo **Injecting Interface** selezionare la stessa interfaccia di rete esposta come access point.<br>6. Fare clic su **Start**: i dispositivi connessi vengono visualizzati. |  |
| 7. Procedere nell'infezione manuale come descritto dalla procedura *vedi "**Infettare i target tramite identificazione manuale** " a pagina 98*. | - |

## Sbloccare la password di un sistema operativo

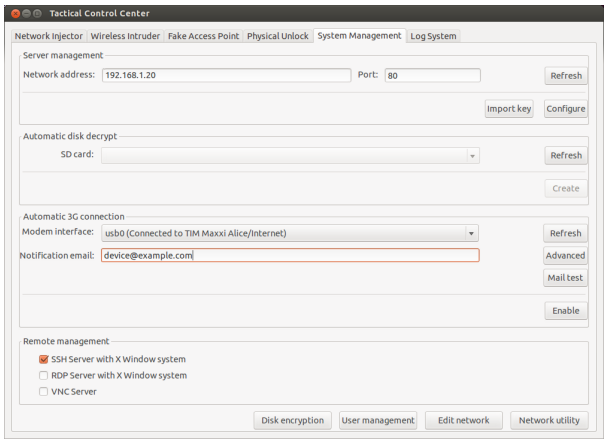
Per sbloccare la password di un sistema operativo:

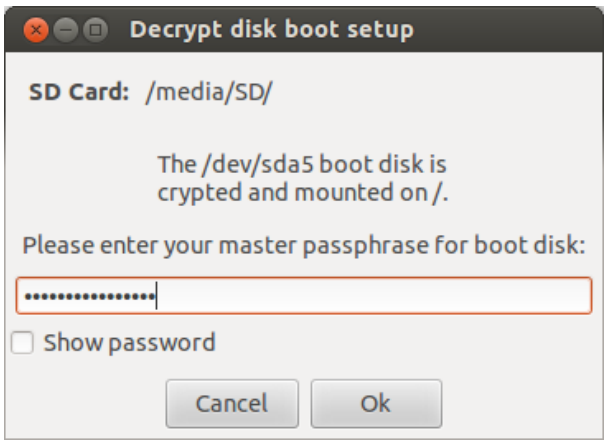
| *Passi* | *Risultato* |
|---|---|
| 1. Connettere il Tactical Network Injector tramite connessione Thunderbolt o FireWire al computer del target. Utilizzare la porta ExpressCard/34, posta sul lato del Tactical Network Injector.<br>2. Nella scheda **Physical Unlock** fare clic su **Refresh**: il sistema riconosce il sistema operativo del computer del target e lo visualizza in **Operating System**.<br>3. Nella casella di riepilogo **Operating System** selezionare la versione del sistema operativo. |  |

| *Passi* | *Risultato* |
|---|---|
| 4. Fare clic su **Unlock**: il sistema tenta di sbloccare la password e visualizza l'avanzamento dell'operazione. Al termine compare il risultato dell'operazione. |  |
| 5. Se si desidera bloccare nuovamente il sistema operativo, fare clic su **Lock**: la password viene ripristinata e il computer viene portato nella condizione precedente alla procedura di sblocco.<br>NOTA: il pulsante **Lock** compare solo se la procedura di sblocco è avvenuta con successo. |  |

## Configurare l'accesso remoto all'applicativo

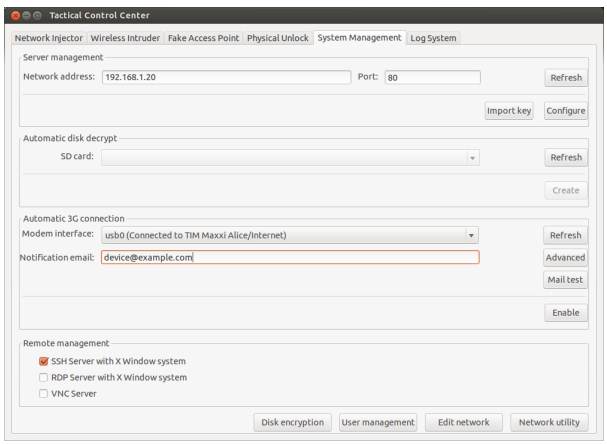
Per poter accedere al Tactical Control Center da remoto:

| *Passi* | *Risultato* |
|---|---|
| 1. Inserire una scheda di memoria SD nello slot del portatile.<br>2. Nella scheda **System Management** fare clic su **Refresh**: il sistema riconosce la scheda SD e la visualizza in **SD card**.<br>3. Se sono presenti più schede SD, selezionare nella casella di riepilogo **SD card** la scheda di memoria desiderata e fare clic su **Create**. |  |

| *Passi* | *Risultato* |
|---|---|
| 4. Inserire la password di Amministratore di sistema e fare clic su **OK**: il sistema genera una nuova password e la salva sulla scheda SD. |  |

| *Passi* | *Risultato* |
|---|---|

5. Collegare il modem al dispositivo.
6. Nella scheda **System Management** fare clic su **Refresh**: il sistema riconosce il modem e lo visualizza in **Modem Interface**.
7. Se sono presenti più modem, selezionare nella casella di riepilogo **Modem Interface** il modem desiderato.
8. Se si desidera abilitare l'invio dell'e-mail con l'indirizzo IP del dispositivo a ogni connessione, eseguire i seguenti passi:
   a. In **Notification e-mail** inserire l'indirizzo email a cui inviare l'e-mail.
   b. Fare clic su **Mail test** per inviare una e-mail di prova.
   c. Se l'email non arriva, fare clic su **Advanced** per configurare manualmente il server di posta: appare la finestra **Email advanced configurazione.**
   d. Inserire i dati richesti e fare clic su **Save.**
   e. Fare clic su **Mail test** per inviare una email di prova con il server configurato.




9. Per abilitare la connessione automatica con il modem selezionato, fare clic su **Enable.**

NOTA: il modem abilitato in questa scheda, compare anche nella scheda **Network Injector**, nella casella di riepilogo **Injecting Interface** e sarà utilizzato per infettare gli agent.

10. Selezionare il protocollo di rete da utilizzare per l'accesso remoto.

NOTA: è possibile accedere direttamente ad alcuni pannelli utili del sistema operativo attraverso i pulsanti in basso nella scheda. *Vedi "**Cose da sapere per l'accesso remoto al Control Center**" a pagina 79.*

### Spegnere il Tactical Network Injector

Non è prevista alcuna procedura particolare. Spegnere normalmente il computer.

### Visualizzare i dettagli dell'infezione

Per visualizzare i log della sessione corrente selezionare la scheda **Log System**.
Per visualizzare tutti i file di log, nella scheda **Log System**, fare clic su **Show logs**.

NOTA: tutti i file di log sono salvati nel file system in /var/log/td-config .

## Dati del Tactical Control Center

### Dati scheda Network Injector

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Injecting Interface** | Elenco delle interfacce di rete già connesse. Selezionare l'interfaccia di infezione connessa alla rete dove è collegato il dispositivo da attaccare.<br>In caso di simulazione di Access Point qui compare anche l'interfaccia utilizzata nella scheda **Fake Access Point**.<br>Qui compare anche il modem 3G configurato e abilitato per l'accesso remoto nella scheda **System Management**. |
| **Sniffing interface** | Come **Injecting Interface** oppure altra interfaccia di rete da utilizzare solo per lo sniffing. |
| **Regular expression** | Espressione usata per filtrare i dispositivi connessi alla rete. Viene applicata a tutti i dati trasmessi e ricevuti dal dispositivo tramite rete, di qualsiasi genere.<br>*Vedi "Cose da sapere su Tactical Control Center" a pagina 72.* |
| **BPF network filter** | Serve per filtrare con maggiore precisione utilizzando la sintassi BPF (Berkeley Packet Filter). Questa sintassi prevede l'inserimento di parole chiave accompagnate da qualificatori.<br>*Vedi "Cose da sapere su Tactical Control Center" a pagina 72.* |

### Dati dei dispositivi rilevati

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Status** | Stato dei dispositivi connessi alla rete:<br>  Dispositivo sconosciuto. Non può essere infettato per problematiche legate alla autenticazione. Forzare l'autenticazione.<br>  Dispositivo in fase di identificazione<br>  Dispositivo identificato, può essere infettato<br>  Dispositivo infettato |
| **HW address** | Indirizzo hardware della scheda di rete del dispositivo. |
| **IP address** | Indirizzo IP del dispositivo nella rete. |
| **Vendor** | Marca della scheda di rete (abbastanza affidabile). |
| **Hostname** | Nome del dispositivo. |
| **OS** | Sistema operativo del dispositivo. |
| **Browser** | Browser web usato dal dispositivo. |
| **Last web Traffic** | Ultimi siti visitati dal dispositivo rilevati e analizzati negli ultimi cinque minuti.<br>  NOTA: se al termine dei cinque minuti il dispositivo non genera più traffico web, allora comparirà la scritta **Idle**. Tipicamente questo accade quando nessuno sta utilizzando il dispositivo. |
| **Las web attack** | Tipo e risultato dell'ultimo attacco. Per controllare ulteriori dettagli consultare la scheda **Log System**. |

## Dati scheda Wireless Intruder

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Wireless interface** | Elenco delle interfacce di rete non connesse. Selezionare l'interfaccia da connettere alla rete WiFi protetta cui si vuole accedere. |
| **ESSID network** | Nome della rete locale in cui accedere. |
| **Attack type** | Tipi di individuazione password disponibili:<br>**WPA/WPA2 dictionary attack**<br>**WEP bruteforce attack**<br>**WPS PIN bruteforce attack**<br>*Vedi "Cose da sapere per individuare la password di rete WiFi" a pagina 77.* |

### Dati scheda Fake Access Point

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Wireless interface** | Elenco delle interfacce di rete non connesse. Selezionare l'interfaccia che si vuole esporre come rete WiFi. |
| **ESSID** | Nome rete ESSID che si intende creare. |
| **HW address** | Indirizzo hardware della scheda di rete del dispositivo. |
| **Access point** | Nome dell'Access Point atteso dal dispositivo. |

### Dati scheda System Management

Di seguito la descrizione dei dati:

| *Dato* | *Descrizione* |
|---|---|
| **Network address** | Indirizzo IP dell'Anonymizer utilizzato per comunicare con il server RCS. |
| **Port** | Porta di comunicazione con l'Anonymizer. |
| **SD card** | Scheda di memoria per la gestione della password di cifratura del disco. |
| **Modem interface** | Modem 3G per la connessione del dispositivo. |
| **Notification email** | Indirizzo e-mail a cui inviare l'indirizzo IP del dispositivo ogni volta che si connette alla rete.<br>  **IMPORTANTE: campo da compilare obbligatoriamente in caso di indirizzo IP dinamico.** |
| **Remote management** | Protocollo di rete per l'accesso remoto. |

# Altri applicativi installati sui Network Injector

## Introduzione

I Network Injector sono forniti con installati alcuni utili applicativi realizzati da altri produttori.

## Applicativi

Di seguito gli applicativi installati su Tactical Network Injector e su Network Injector Appliance:

NOTA: per istruzioni di utilizzo degli applicativi fare riferimento alla documentazione rilasciata dal produttore dell'applicativo.

| *Nome applicativo* | *Descrizione* |
|---|---|
| **Disniff** | Pacchetto di strumenti per intercettare il traffico di rete insicuro |
| **hping3** | Generatore di traffico di rete |
| **Kismet** | Strumento di monitoraggio per reti Wireless 802.11b |
| **Macchanger** | Strumento per manipolare l'indirizzo MAC delle interfacce di rete |
| **Nbtscan** | Scanner di reti per informazioni sui nomi NetBIOS |
| **Netdiscover** | Scanner di indirizzo di rete attivo/passivo utilizzando richieste ARP |
| **Ngrep** | Grep per il traffico di rete |
| **Nmap** | Network Mapper |
| **P0f** | Strumento passivo di OS fingerprinting |
| **SsIsniff** | Strumento di attacco man-in-the-middle per traffico di rete SSL/TLS |
| **SsIstrip** | Strumento di attacco man-in-the-middle e hijacking per traffico di rete SSL/TLS |
| **Tcpdump** | Analizzatore di traffico di rete da riga di comando |
| **Wireshark** | Analizzatore di traffico di rete |
| **Xprobe** | Strumento remoto per l'identificazione di OS |

# 9

# Monitoraggio del sistema

## Presentazione

### Introduzione

Il monitoraggio del sistema permette il controllo costante dello stato dei componenti e dell'uso delle licenze.

### Contenuti

Questa sezione include i seguenti argomenti:

**Monitoraggio del sistema (Monitor)** ..... **112**

# Monitoraggio del sistema (Monitor)

*Per fare il monitoraggio del sistema:* • sezione **Monitor**

## Scopo

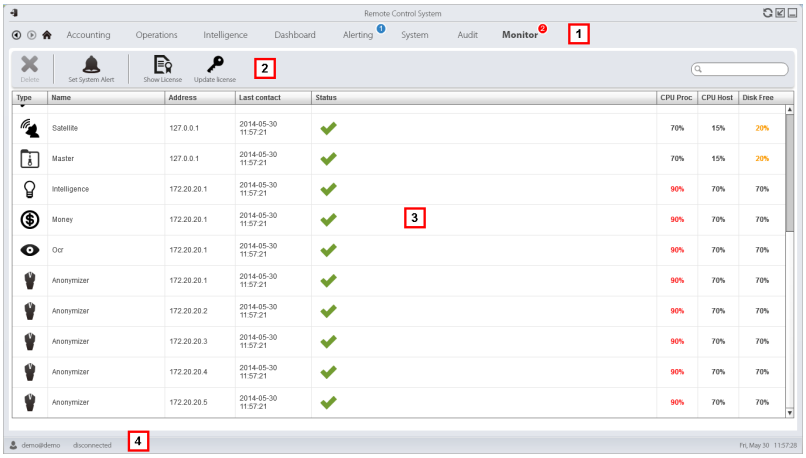
Questa funzione permette di:

- monitorare lo stato del sistema in termini di componenti hardware e software
- monitorare le licenze utilizzate rispetto a quelle acquistate

*Richiede assistenza: contattare il vostro Account Manager HackingTeam se sono necessarie licenze aggiuntive.*

## Come si presenta la funzione

Ecco come viene visualizzata la pagina:




| *Area* | *Descrizione* |
|---|---|
| **1** | Menu di RCS.<br>Monitor 1 : indica la quantità di allarmi di sistema in corso. |
| **2** | Barre con i pulsanti della finestra. |
| **3** | Elenco componenti di RCS con relativo stato:<br>Allarme (genera l'invio di una e-mail al gruppo di alerting)<br>Avvertenza<br>Componente funzionante |

| *Area* | *Descrizione* |
|---|---|
| **4** | Barra di stato di RCS. |

## Per saperne di più

Per la descrizione degli elementi dell'interfaccia *vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 11*.

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati del monitoraggio del sistema (Monitor)**" nel seguito*.

## Dati del monitoraggio del sistema (Monitor)

### Dati di monitoraggio dei componenti del sistema

Di seguito la descrizione dei dati del monitoraggio di sistema:

| *Dato* | *Descrizione* |
|---|---|
| **Tipo**<br>**Nome** | Tipo e nome del componente controllato.<br>Di seguito alcuni esempi:<br>  Anonymizer<br>  Carrier<br>  Collector<br>  Database<br>  Network Controller |
| **Indirizzo** | Indirizzo IP del componente. |
| **Ultimo contatto** | Data-ora ultima sincronizzazione. |
| **Stato** | Stato del componente dall'ultima sincronizzazione:<br>  Allarme: il componente non sta funzionando, contattare il gruppo di alerting per un intervento rapido.<br>  Avvertenza: il componente segnala una situazione di rischio, contattare l'Amministratore di sistema per le verifiche del caso.<br>  Componente funzionante. |
| **CPU Proc** | % utilizzo CPU del singolo processo. |
| **CPU Host** | % utilizzo CPU del server. |

| *Dato* | *Descrizione* |
|---|---|
| **Disco libero** | % di unità disco libera. |

### Dati di monitoraggio delle licenze

Di seguito la descrizione dei dati del monitoraggio delle licenze. Nel caso di licenze limitate il formato è "x/y" dove x è la quantità di licenze attualmente usate dal sistema e y la quantità massima di licenze.

***PRUDENZA: se la quantità di licenze si esaurisce, eventuali nuovi agent saranno accodati in attesa che si liberi una licenza o che se ne acquistino di nuove.***

| *Dato* | *Descrizione* |
|---|---|
| **Tipo di licenza** | Tipo di licenza attualmente in uso per gli agent.<br>**reusable**: è possibile riutilizzare la licenza di un agent dopo la sua disinstallazione.<br>**oneshot**: la licenza di un agent ha validità solo per una installazione.<br>  NOTA: è possibile aggiornare la licenza solo se si è in possesso dell'autorizzazione **Modifica licenza**. |
| **Utenti** | Quantità di utenti attualmente usati dal sistema e quantità massima ammessa. |
| **Agent** | Quantità di agent attualmente usati dal sistema e quantità massima ammessa. |
| **Desktop**<br>**Mobile** | Rispettivamente quantità di agent desktop e di agent mobile attualmente usati dal sistema e quantità massima ammessa. |
| **Server distribuiti** | Quantità di database attualmente usati dal sistema e quantità massima ammessa. |
| **Collectors** | Quantità di Collector attualmente usati dal sistema e quantità massima ammessa. |
| **Anonymizers** | Quantità di Anonymizer attualmente usati dal sistema e quantità massima ammessa. |

# 10

# Appendice: azioni

## Presentazione

### Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencate le singole azioni con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

### Contenuti

Questa sezione include i seguenti argomenti:


**Elenco delle sotto-azioni** ..... **116**
**Azione Destroy** ..... **116**
**Azione Execute** ..... **117**
**Azione Log** ..... **117**
**Azione SMS** ..... **118**
**Azione Synchronyze** ..... **118**
**Azione Uninstall** ..... **120**

# Elenco delle sotto-azioni

## Descrizione dati sotto-azioni

Di seguito la descrizione delle sotto-azioni:

| *Dato* | *Descrizione* |
|---|---|
| **Nome** | Nome arbitrario assegnato all'azione. |
| **Sottoazioni** | Elenco dei tipi di sotto-azioni. |

## Descrizione tipi di sotto-azioni

NOTA: alcune sotto-azioni possono mancare perché non supportate da alcuni sistemi operativi.

Di seguito la descrizione dei tipi di sotto-azioni:

| *Azione* | *Dispositivo* | *Descrizione* |
|---|---|---|
| **Destroy** | desktop, mobile | Rende il dispositivo target inutilizzabile. |
| **Execute** | desktop, mobile | Esegue un comando arbitrario sulla macchina target. |
| **Log** | desktop, mobile | Crea messaggio informativo personalizzato. |
| **SMS** | mobile | Invia un SMS nascosto dal dispositivo del target. |
| **Synchronize** | desktop, mobile | Avvia una sincronizzazione con il Collector. |
| **Uninstall** | desktop, mobile | Rimuove l'agent dal dispositivo. |

# Azione Destroy

## Scopo

L'azione **Destroy** rende il dispositivo target temporaneamente o permanentemente inutilizzabile.

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Permanente** | Il dispositivo è reso inutilizzabile in modo permanente.<br>**AVVERTENZA: potrebbe essere necessario portare il dispositivo in assistenza.** |

# Azione Execute

## Scopo

L'azione **Execute** esegue un comando arbitrario sulla macchina target. Se richiesto, possono essere specificate impostazioni del comando e variabili di ambiente. Il programma sarà eseguito con i privilegi dell'utente che in quel momento è registrato nel sistema.

L'eventuale output del comando è visibile nella pagina **Comandi**. *Vedi "Pagina dei comandi" a pagina 41*.

**AVVERTENZA: anche se tutti i comandi sono eseguiti utilizzando il sistema di occultamento dell'agent e risultano quindi invisibili, qualsiasi modifica al file system (es.: un file creato sul desktop) sarà visibile dall'utente. Fare attenzione.**

**ATTENZIONE: evitare programmi che richiedono interazione da parte dell'utente o che aprono interfacce grafiche.**

Suggerimento: utilizzare applicazioni lanciate da linea di comando e file batch perché i loro processi (e la corrispondente finestra per la linea di comando) saranno nascosti dall'agent.

## Riferimento a cartella dell'agent

Alla stringa di comando si può aggiungere la variabile di ambiente virtuale $dir$ che si riferisce alla cartella di installazione (nascosta) dell'agent.

## Dati significativi

| *Campo* | *Descrizione* |
|---|---|
| **Comando** | Comando da eseguire.<br>Suggerimento: utilizzare un percorso assoluto. |

# Azione Log

## Scopo

L'azione **Log** crea messaggio informativo personalizzato.

NOTA: i messaggi personalizzati e i log provenienti da un agent sono visualizzati nella sezione **Info.** *Vedi "Pagina dell'agent" a pagina 38*

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Testo** | Testo del messaggio che comparirà nella sezione **Info**. |

# Azione SMS

### Scopo

L'azione **SMS** invia un SMS nascosto dal dispositivo del target, con i dati della posizione del dispositivo e della SIM.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Numero** | Telefono destinatario del messaggio. |
| **Posizione** | Inserisce nel messaggio la posizione della cella GPS o GSM del target. |
| **Sim** | Inserisce nel messaggio le informazioni relative alla SIM del telefono. |
| **Testo** | Testo del messaggio. |

# Azione Synchronyze

### Scopo

L'azione **Synchronize** sincronizza l'agent e il server RCS.
Il processo di sincronizzazione si divide nei seguenti passi:

| *Passo* | *Descrizione* |
|---|---|
| **1** | Autenticazione reciproca agent/server RCS. |
| **2** | Sincronizzazione temporale agent/server RCS. |
| **3** | Eventuale rimozione dell'agent in caso di chiusura dell'attività relativa. |
| **4** | Aggiornamento configurazione dell'agent. |
| **5** | Caricamento di tutti i file nella coda "upload". |
| **6** | Scaricamento di tutti i file nella coda "download". |
| **7** | Scaricamento di tutte le evidence raccolte dall'agent, con contestuale rimozione sicura. |
| **8** | Rimozione sicura nell'agent di tutte le evidence scaricate. |

## Parametri desktop

| *Nome* | *Descrizione* |
|---|---|
| **Host** | Nome dell'Anonymizer da connettere per la sincronizzazione. Nella casella combinata selezionare il nome del server oppure inserire l'FQDN (nome DNS) oppure l'indirizzo IP. |
| **Banda** | Massima ampiezza di banda da utilizzare durante la sincronizzazione. |
| **Ritardo minimo** | Minimo ritardo in secondi tra l'invio di una evidence e di quella successiva. |
| **Ritardo massimo** | Massimo ritardo in secondi tra l'invio di una evidence e di quella successiva. |
| **Stop se riuscito** | Se abilitato, la catena di sotto-azioni viene interrotta al corretto completamento della sincronizzazione. Le rimanenti sotto-azioni nella coda non sono eseguite. |

## Parametri mobile

| *Nome* | *Descrizione* |
|---|---|
| **Host** | Nome o indirizzo IP dell'Anonymizer cui connettersi per la sincronizzazione. Nella casella combinata selezionare il nome del server oppure inserire l'FQDN (nome DNS) oppure l'indirizzo IP. |
| **Stop se riuscito** | La catena di sotto-azioni viene interrotta al corretto completamento della sincronizzazione. Le rimanenti sotto-azioni nella coda non sono eseguite. |
| **Tipo** | **Internet**: sincronizzazione tramite connessione Internet.<br>• **Forza WiFi**: sincronizzazione via rete WiFi. Forza una connessione dati WiFi con una qualsiasi rete WiFi aperta o preconfigurata disponibile, prima di avviare la sincronizzazione.<br>• **Forza Cella**: sincronizzazione via rete GPRS/UMTS/3G . Forza una connessione dati GPRS/UMTS/3G verso il fornitore di telefonia prima di iniziare la sincronizzazione.<br><br>**APN**: specifica le credenziali per l'accesso a un APN che il telefono può usare per raccogliere i dati.<br>Utile per non addebitare al target i costi del traffico generato dall'agent. |

## Criteri di selezione del tipo di connessione (Windows Phone)

Per Windows Phone il sistema definisce internamente il tipo di connessione da utilizzare, indipendentemente dai parametri impostati.

Se il dispositivo è configurato per supportare sia WiFi che 3G/4G ed è presente una connessione WiFi configurata e attiva, allora il sistema utilizza la rete 3G/4G quando il dispositivo ha lo schermo spento e non è in ricarica, oppure la rete WiFI negli altri casi.

# Azione Uninstall

## Scopo

L'azione **Uninstall** rimuove completamente l'agent dal sistema del target. Tutti i file vengono eliminati.

NOTA: per BlackBerry rimuovere l'agent comporta un riavvio automatico.

NOTA: per Android, se il dispositivo non ha i privilegi di root l'utente dovrà autorizzare la disinstallazione. Per sapere come verificare di avere i privilegi di root, *vedi "Cose da sapere su Android" a pagina 144*.

NOTA: per Windows Phone rimuovere l'agent comporta l'eliminazione di tutti i file generati dall'agent, ma l'icona dell'applicazione rimane nella lista dei programmi.

# 11

# Appendice: eventi

## Presentazione

### Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli eventi con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

### Contenuti

Questa sezione include i seguenti argomenti:


**Elenco degli eventi** ..... **122**
**Evento AC** ..... **123**
**Evento Battery** ..... **123**
**Evento Call** ..... **123**
**Evento Connection** ..... **124**
**Evento Idle** ..... **124**
**Evento Position** ..... **125**
**Evento Process** ..... **125**
**Evento Quota** ..... **126**
**Evento Screensaver** ..... **126**
**Evento SimChange** ..... **126**
**Evento SMS** ..... **126**
**Evento Standby** ..... **127**
**Evento Timer** ..... **127**
**Evento Window** ..... **128**
**Evento WinEvent** ..... **128**

# Elenco degli eventi

## Descrizione dati eventi

Di seguito la descrizione degli eventi:

| *Dato* | *Descrizione* |
|---|---|
| **Abilitato** | Abilita o disabilita l'evento. |
| **Nome** | Nome assegnato all'evento. |
| **Tipo** | Elenco dei tipi di evento. Vedi tabella sottostante. |

## Descrizione tipi eventi

NOTA: alcuni eventi possono mancare perché non supportati da alcuni sistemi operativi.

Di seguito la descrizione tipi di evento:

| *Evento* | *Dispositivo* | *Innesca un'azione quando...* |
|---|---|---|
| **AC** | mobile | il cellulare viene collegato all'alimentazione. |
| **Battery** | mobile | il livello di carica della batteria è entro il range specificato. |
| **Call** | mobile | viene effettuata o ricevuta una chiamata. |
| **Connection** | desktop, mobile | l'agent rileva una connessione alla rete attiva. |
| **Idle** | desktop | l'utente non interagisce col computer per un determinato periodo di tempo. |
| **Position** | mobile | il dispositivo raggiunge o lascia una posizione specifica. |
| **Process** | desktop, mobile | sul dispositivo viene lanciato un'applicazione o se c'è una finestra aperta. |
| **Quota** | desktop | l'occupazione disco delle evidence sul dispositivo supera il limite impostato. |
| **Screensaver** | desktop | sul dispositivo target si avvia il salva schermo. |
| **SimChange** | mobile | viene sostituita la scheda SIM. |
| **SMS** | mobile | viene ricevuto un messaggio SMS dal numero indicato. |
| **Standby** | mobile | il dispositivo è in modalità stand-by. |

| *Evento* | *Dispositivo* | *Innesca un'azione quando...* |
|---|---|---|
| **Timer** | desktop, mobile | scadono intervalli specificati. |
| **Window** | desktop | si apre una finestra. |
| **WinEvent** | desktop | il sistema operativo registra un evento Windows. |

# Evento AC

## Scopo

L'evento **AC** innesca un'azione quando il cellulare viene collegato all'alimentazione.

# Evento Battery

## Scopo

L'evento **Battery** innesca un'azione quando il livello di carica della batteria è entro il range specificato.

Suggerimento: se si vuole ridurre l'impatto sull'uso della batteria, è sensato associare all'evento **Battery**, impostato su valori 0%-30%, le azioni **Start** e **Stop Crisis**. In questo modo, se il livello di carica della batteria scende sotto il valore prefissato, sono sospese le attività più dispendiose dell'agent.

**ATTENZIONE: il modulo Crisis può essere configurato in modo da inibire la sincronizzazione.**

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Min** | Minima percentuale di batteria richiesta. Percentuali superiori a questo limite innescano l'evento. |
| **Max** | Massima percentuale di batteria richiesta. Percentuali inferiori a questo limite innescano l'evento. |

# Evento Call

## Scopo

L'evento **Call** innesca un'azione quando viene effettuata o ricevuta una chiamata.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Numero** | numero telefonico (o parte di esso) da cui viene effettuata/o ricevuta la chiamata.<br>Suggerimento: lasciare vuoto per innescare l'evento con qualsiasi numero. |

# Evento Connection

### Scopo

L'evento **Connection** innesca un'azione quando l'agent rileva una connessione alla rete attiva.

Nel caso di dispositivo desktop indicare l'indirizzo del destinatario della connessione.

Nel caso di dispositivo mobile innesca un'azione non appena il dispositivo disporrà di un indirizzo IP valido su una qualsiasi delle interfacce di rete (es.: WiFi, Activesync, GPRS/3G+), e disinnescherà l'azione quando tutte le connessioni sono terminate.

### Parametri desktop

| *Nome* | *Descrizione* |
|---|---|
| **Indirizzo IP** | Indirizzo IP di destinazione per la connessione<br>NOTA: Inserire 0.0.0.0 per indicare un qualsiasi indirizzo.<br>NOTA: le connessioni a indirizzi locali nella stessa sottorete del target non vengono considerate. |
| **Netmask** | Netmask applicata all'indirizzo IP. |
| **Porta** | Porta utilizzata per identificare la connessione. |

# Evento Idle

### Scopo

L'evento **Idle** innesca un'azione quando l'utente non interagisce con il computer per un determinato periodo di tempo.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Ora** | Secondi di inattività allo scadere dei quali viene innescato l'evento. |

# Evento Position

### Scopo

L'evento **Position** innesca un'azione quando il target raggiunge o lascia una posizione specifica.

La posizione può essere identificata dalle coordinate GPS e da un raggio d'azione oppure dall'ID di una cella GSM.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Tipo** | Tipo di posizione da utilizzare.<br>**GPS**<br>• **Latitudine, Longitudine**: coordinate<br>• **Distanza**: raggio a partire dalle coordinate.<br>**GSM Cell (tutti i sistemi operativi tranne Windows Phone)**<br>• **Country, Network, Area,ID:** dati della cella GSM. Inserire '*' per ignorare un campo. Per esempio, se si mantiene il valore di **Country** e si mette il simbolo '*' negli altri tre campi, l'evento è innescato quando il dispositivo entra o esce dalla nazione specificata. |

# Evento Process

### Scopo

L'evento **Process** innesca un'azione quando sul dispositivo viene lanciata un'applicazione o viene aperta una finestra.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Tipo** | **Nome del processo**: l'evento innesca un'azione all'avvio del processo specificato.<br>**Titolo finestra**: l'evento innesca un'azione quando il focus viene dato alla finestra specificata. |

| *Nome* | *Descrizione* |
|---|---|
| **Stringa** | Nome o parte del nome del programma o del titolo della finestra.<br>Suggerimento: utilizzare caratteri jolly per specificare un programma (es.: "*Calculator*") |
| **Focus** | (solo desktop) Se selezionato, l'evento innesca l'azione solo quando il processo o la finestra sono in primo piano. |

# Evento Quota

## Scopo

L'evento **Quota** innesca un'azione quando l'occupazione disco delle evidence sul dispositivo supera il limite impostato.

Quando lo spazio disco torna al di sotto del limite, alla successiva sincronizzazione l'azione sarà terminata.

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Quota** | Spazio disco da usare per salvare le evidence raccolte. |

# Evento Screensaver

## Scopo

L'evento **Screensaver** innesca un'azione quando sul dispositivo target si avvia il salva schermo.

# Evento SimChange

## Scopo

L'evento **SimChange** innesca un'azione quando viene sostituita la scheda SIM.

# Evento SMS

## Scopo

L'evento **SMS** innesca un'azione quando viene ricevuto uno specifico messaggio SMS dal numero indicato. Il messaggio non comparirà tra i messaggi ricevuti dal telefono.

**ATTENZIONE: i messaggi in arrivo vengono cancellati soltanto su BlackBerry OS 5.x.**

NOTA: il messaggio ricevuto non viene visualizzato sul dispositivo del target.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Numero** | Numero telefonico del mittente del messaggio SMS. Qualsiasi SMS proveniente da questo numero verrà nascosto. |
| **Testo** | Parte del testo che deve corrispondere.<br>**IMPORTANTE: nella stringa non si fa distinzione fra maiuscole e minuscole.** |

# Evento Standby

L'evento **Standby** innesca un'azione quando il dispositivo entra in modalità stand- by (retroilluminazione spenta).

# Evento Timer

### Scopo

L'evento **Timer** innesca un'azione agli intervalli indicati.

Quando l'evento si verifica, viene eseguita l'azione connessa all'azione **Start**.

Durante il periodo di tempo che intercorre tra l'innesco e il disinnesco dell'evento, viene ripetuta l'azione **Repeat**, con il periodo specificato dal connettore relativo.

Quando l'evento viene disinnescato, viene eseguita l'azione **Stop**.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Tipo** | Tipo di intervallo:<br>• **Loop**: innesca un'azione ripetendola indefinitivamente ogni periodo di tempo specificato dall'azione **Repeat**.<br>• **Daily**: innesca un'azione quotidiana all'interno degli orari indicati da **Da** e **A**<br>• **Date**: innesca un'azione nel periodo indicato da **Da** e **A**.<br>  NOTA: selezionare **Per sempre** affinché l'azione continui nel tempo.<br>• **AfterInst**: innesca un'azione dopo un certo numero di giorni (**Giorni**) dall'installazione dell'agent. |

# Evento Window

### Scopo

L'evento **Window** innesca un'azione all'apertura di ogni finestra.

# Evento WinEvent

### Scopo

L'evento **WinEvent** innesca un'azione quando il sistema operativo registra un evento Windows.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **ID Evento** | ID dell'evento Windows. |
| **Sorgente** | Sorgente dell'evento Windows (es.: sistema, applicazione) |

# 12

# Appendice: moduli

## Presentazione

### Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli moduli con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

### Contenuti

Questa sezione include i seguenti argomenti:


**Elenco dei moduli** ..... **130**
**Modulo Addressbook** ..... **132**
**Modulo Application** ..... **132**
**Modulo Calendar** ..... **132**
**Modulo Call** ..... **132**
**Modulo Camera** ..... **133**
**Modulo Chat** ..... **133**
**Modulo Clipboard** ..... **133**
**Modulo Conference** ..... **133**
**Modulo Crisis** ..... **134**
**Modulo Device** ..... **135**
**Modulo File** ..... **136**
**Modulo Keylog** ..... **137**
**Modulo Livemic** ..... **137**
**Modulo Messages** ..... **137**
**Modulo Mic** ..... **138**
**Modulo Money** ..... **139**
**Modulo Mouse** ..... **139**
**Modulo Password** ..... **140**
**Modulo Photo** ..... **140**
**Modulo Position** ..... **140**
**Modulo Screenshot** ..... **141**
**Modulo Url** ..... **141**

# Elenco dei moduli

## Descrizione tipi moduli

NOTA: alcuni moduli possono mancare perché non supportati da alcuni sistemi operativi.

Di seguito la descrizione dei moduli di registrazione:

| *Modulo* | *Configurazione* | *Dispositivo* | *Registrazione di...* |
|---|---|---|---|
| **Addressbook** | avanzata | desktop, mobile | contatti. |
| **Application** | avanzata | desktop, mobile | applicazioni utilizzate. |
| **Calendar** | avanzata | desktop, mobile | calendario. |
| **Call** | avanzata | desktop, mobile | chiamate (es.: GSM e VoIP). |
| **Calls** | base | desktop, mobile | chiamate (es.: telefono, Skype, MSN). |
| **Camera** | base, avanzata | desktop, mobile | immagini della webcam. |
| **Chat** | avanzata | desktop, mobile | chat (es.: Skype, BlackBerry Messenger). |
| **Clipboard** | avanzata | desktop, mobile | informazioni copiate nella clipboard. |
| **Contacts and Calendar** | base | desktop, mobile | contatti e calendario. |
| **Device** | avanzata | desktop, mobile | informazioni del sistema. |
| **File** | avanzata | desktop | file aperti dal target. |
| **Files and photos** | base | desktop, mobile | documenti o immagini aperti dal target e foto scattate con il dispositivo o presenti nella libreria di foto. |
| **Keylog** | avanzata | desktop, mobile | tasti premuti sulla tastiera. |
| **Keylog, Mouse and Password** | base | desktop | tasti premuti sulla tastiera, clic del mouse, password salvate. |

| *Modulo* | *Configurazione* | *Dispositivo* | *Registrazione di...* |
|---|---|---|---|
| **Messages** | avanzata | desktop, mobile | e-mail, SMS, MMS. |
| **Messages** | base | desktop, mobile | e-mail, SMS e chat. |
| **Mic** | avanzata | desktop, mobile | audio proveniente dal microfono. |
| **Money** | avanzata | desktop | informazioni del portafoglio digitale di cryptocurrency (es. Bitcoin) |
| **Mouse** | avanzata | desktop | clic del mouse. |
| **Password** | avanzata | desktop, mobile | password salvate. |
| **Photo** | avanzata | desktop, mobile | foto scattate con il dispositivo o presenti nella libreria di foto. |
| **Position** | base, avanzata | desktop, mobile | posizione geografica del target. |
| **Screenshots** | base, avanzata | desktop, mobile | schermata attive sul display del target. |
| **URL** | avanzata | desktop, mobile | URL visitati. |
| **Visited websites** | base | desktop, mobile | URL visitati. |

Di seguito la descrizione dei moduli di altro tipo:

| *Modulo* | *Configurazione* | *Dispositivo* | *Azione* |
|---|---|---|---|
| **Conference** | avanzata | mobile | Crea una chiamata a tre. |
| **Crisis** | avanzata | desktop, mobile | Riconosce situazioni di pericolo (es.: esecuzione di uno sniffer). Può disabilitare temporaneamente la sincronizzazione e l'esecuzione di comandi. |
| **Infection** | avanzata | desktop | Deprecato a partire dalla versione RCS 8.4 |
| **Livemic** | avanzata | mobile | Ascolta in tempo reale conversazioni. |
| **Online Synchronization** | base | desktop, mobile | Sincronizza l'agent con RCS permettendo la ricezione delle evidence e la riconfigurazione dell'agent. |

# Modulo Addressbook

## Scopo

Il modulo **Addressbook** registra tutte le informazioni trovate nella rubrica del dispositivo. La versione per desktop recupera i contatti da Outlook, Skype ed altre fonti.

# Modulo Application

## Scopo

Il modulo **Application** registra il nome e le informazioni relative all'avvio e alla chiusura di un processo sul dispositivo del target.

Le evidence riporteranno tutte le applicazioni utilizzate dal target in ordine cronologico.

# Modulo Calendar

## Scopo

Il modulo **Calendar** registra tutte le informazioni trovate nel calendario del dispositivo del target. La versione per desktop recupera il calendario da Outlook, e altre fonti.

# Modulo Call

## Scopo

Il modulo **Call** cattura l'audio e le informazioni (ora di inizio, durata, numeri di origine e destinazione della chiamata) di tutte le telefonate effettuate e ricevute dal target.

Su un dispositivo desktop, il modulo **Call** intercetta le conversazioni voce effettuate da applicazioni supportate.

Su un dispositivo mobile, il modulo **Call** intercetta tutte le chiamate (GSM e VoIP).

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Abilita registrazione chiamate** | (solo mobile) Abilita la registrazione delle chiamate. Se disabilitato l'audio delle chiamate non viene registrato. |
| **Dimensione buffer** | Dimensioni del buffer di acquisizione utilizzato per i settori audio. |
| **Qualità** | Qualità audio (1=massima compressione, 10=migliore qualità). |

# Modulo Camera

## Scopo

Il modulo **Camera** cattura un'immagine dalla fotocamera integrata.

**ATTENZIONE: la cattura dell'immagine su un desktop provoca il lampeggio del led della fotocamera.**

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Qualità** | Qualità immagine (bassa, media, alta). |

# Modulo Chat

## Scopo

Il modulo **Chat** registra tutte le sessioni di chat del target, sia con contenuto testuale che multimediale (es.: video, immagini). Ogni messaggio viene catturato come una evidence distinta.

**IMPORTANTE: per Android, per catturare le chat è necessario ottenere i privilegi di root.** ***Vedi "Cose da sapere su Android" a pagina 144.***

**IMPORTANTE: per BlackBerry questo modulo, per attivarsi al riavvio del dispositivo, richiede che il telefono rimanga in standby (retroilluminazione spenta) per qualche minuto.**

# Modulo Clipboard

## Scopo

Il modulo **Clipboard** copia e registra il contenuto in formato testo della clipboard.

# Modulo Conference

## Scopo

Il modulo **Conference** chiama il numero indicato creando una teleconferenza ogni volta che il target effettua una chiamata. Il numero ricevente potrà ascoltare la conversazione in tempo reale.

**IMPORTANTE: il funzionamento del modulo dipende delle caratteristiche dell'operatore telefonico. Il target potrebbe accorgersi della teleconferenza se l'operatore telefonico inserisce un segnale acustico in attesa dell'inizio chiamata.**

### Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Numero** | numero telefonico ricevente |

# Modulo Crisis

### Comportamento su dispositivi desktop

Il modulo **Crisis** viene abilitato (automaticamente o su una specifica azione) e riconosce le situazioni di pericolo sul dispositivo che possono far scoprire la presenza dell'agent (es.: esecuzione di uno sniffer). Può disabilitare temporaneamente la sincronizzazione e l'esecuzione di comandi.

Questo modulo aumenta il livello di occultamento nei confronti dei software di protezione.

NOTA: **Crisis** può essere abilitato di default sul dispositivo desktop per permettere all'agent di rilevare automaticamente la condizione di pericolo e agire di conseguenza (es. : diventare invisibile).

### Comportamento su dispositivi mobile

Il modulo **Crisis** viene usato per sospendere il funzionamento di attività che fanno uso pesante della batteria. In base ai parametri impostati, questo modulo può disabilitare temporaneamente alcune funzioni.

Su un dispositivo mobile **Crisis** deve essere avviato manualmente da un'azione specifica (es.: avvio dell'agent con carica della batteria troppo bassa) e arrestato quando la situazione anomala termina.

NOTA: questo modulo non crea evidence.

### Dati significativi desktop

Sui dispositivi desktop non si dovrebbero modificare le impostazioni di default a meno di diversa indicazione da parte dei tecnici HackingTeam.

| *Campo* | *Descrizione* |
|---|---|
| **Inibire rete** | Abilita inibizione della sincronizzazione in presenza di processi potenzialmente pericolosi. |

| *Campo* | *Descrizione* |
|---|---|
| **Inibitori (rete)** | Elenco dei processi che, se in esecuzione, possono impedire la sincronizzazione. |
| **Inibire Hooking** | Abilita inibizione dell'hooking dei programmi in presenza di processi potenzialmente pericolosi. |
| **Inibitori (Hooking )** | Elenco dei processi che, se in esecuzione, possono impedire l'hooking. |
| **Process** | Processo da aggiungere all'elenco. |

### Dati significativi mobile

Nella versione mobile è possibile specificare le funzionalità da bloccare:

| *Campo* | *Descrizione* |
|---|---|
| **Microfono** | se selezionato, impedisce la registrazione audio Mic |
| **Chiamate** | se selezionato, impedisce la registrazione audio Call |
| **Camera** | se selezionato, impedisce l'istantanea Camera |
| **Posizione** | se selezionato, impedisce l'uso del GPS |
| **Sincronizzazione** | se selezionato, impedisce la sincronizzazione<br>  **AVVERTENZA: operazioni altamente rischiose! Prima di impedire la sincronizzazione contattare i tecnici HackingTeam! È possibile perdere l'agent in modo permanente.** |

# Modulo Device

## Scopo

Il modulo **Device** registra le informazioni del sistema (es.: tipo di processore, memoria in uso, sistema operativo installato, privilegi di root). Può essere utile per monitorare l'uso del disco fisso sul dispositivo e ricavare la lista della applicazioni installate.

NOTA: su Android, se il dispositivo ha i privilegi di root, nella evidence di tipo **Device** è riportato **root:yes.**

## Dati significativi mobile

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Recupera la lista delle applicazioni** | Oltre alle informazioni di sistema, registra l'elenco delle applicazioni installate. |

# Modulo File

## Scopo

Il modulo **File** registra tutti i file che vengono aperti sul computer del target. Può anche catturare il file nel momento in cui viene aperto.

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Filtro inclusioni** | Elenco delle estensioni dei file da registrare. Specificare opzionalmente il processo per registrare il file solo quando viene eseguito o aperto da quel processo. |
| **Filtro esclusioni** | Elenco delle estensioni dei file da non registrare. Specificare opzionalmente il processo per ignorare il file solo quando viene eseguito o aperto da quel processo. |
| **Maschera** | Stringa per filtrare il processo e il file da registrare o ignorare.<br>**Sintassi**<br>*Processo*\|*Filtro*<br>**Esempio caratteristiche per inclusione**<br>"skype.exe\|*.*"<br>"word.exe\|*John*.doc"<br>**Esempio caratteristiche per esclusione**<br>"skype.exe\|*.dat" |
| **Registra percorso e modo di accesso** | Registra il percorso del file e il tipo di accesso (es.: lettura, scrittura) |
| **Cattura contenuto file** | Se abilitato, il file viene copiato e scaricato al primo accesso. |
| **Dimensione minima/massima** | Minima e massima dimensione ammessa per il file da scaricare. |
| **Più recenti di** | Data minima di creazione del file da scaricare. |

# Modulo Keylog

## Scopo

Il modulo **Keylog** registra tutto quello che viene digitato dal target.

NOTA: supporta tutti i caratteri unicode via IME.

# Modulo Livemic

## Scopo

Il modulo **Livemic** permette di ascoltare in tempo reale eventuali conversazioni già in corso.

***PRUDENZA: questo modulo è fornito "as is" e il suo utilizzo può risultare pericoloso. Ogni apparecchio si comporta diversamente. Si consiglia di fare test approfonditi prima di utilizzarlo sul campo.***

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Numero** | Numero del telefono usato per l'ascolto. Deve comprendere il prefisso internazionale, es.: "+341234567890".<br>**ATTENZIONE: non nascondere l'ID del chiamante e disabilitare il microfono mentre si ascolta la conversazione.** |

# Modulo Messages

## Scopo

Il modulo **Messages** registra tutti i messaggi ricevuti o inviati dal target. Questo modulo cattura:

- e-mail
- SMS (solo Mobile)
- MMS (solo Mobile)

**IMPORTANTE: per Android è necessario ottenere i privilegi di root.** ***Vedi "Cose da sapere su Android" a pagina 144.***

### Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Abilitato** | Abilita la registrazione. |
| **Da** | Registra i messaggi a partire dalla data indicata. |
| **A** | Registra i messaggi fino alla data indicata. |
| **Dimensione massima** | Dimensione massima del messaggio da registrare. |

# Modulo Mic

### Scopo

Il modulo **Mic** registra i suoni circostanti utilizzando il microfono del dispositivo.

**IMPORTANTE: non attivare il microfono per registrare chiamate dati (es.: Skype, Viber) senza aver fatto test approfonditi sullo stesso modello di telefono con la stessa versione di sistema operativo. Si rischia di disabilitare l'audio sul client, rendendo la relativa applicazione inutilizzabile.**

**IMPORTANTE: per alcuni sistemi operativi mobile, il modulo non è abilitato durante le chiamate.**

NOTA: per Windows Phone, su alcuni modelli di dispositivi l'inizio e il termine della registrazione potrebbero essere accompagnati da un segnale acustico.

### Dati significativi desktop

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Silenzio tra le voci** | Numero massimo di secondi di silenzio ammessi nella registrazione. Superato il periodo impostato, l'agent sospende la registrazione e si riavvia alla ricezione di nuovi suoni.<br>**AVVERTENZA: se il valore è troppo basso la registrazione escluderà tutti i silenzi e si otterrà una conversazione continua senza pause. Se il valore è troppo alto la registrazione includerà tutti i silenzi e si otterrà una conversazione molto lunga.** |

| *Campo* | *Descrizione* |
|---|---|
| **Riconoscimento vocale** | NOTA: non supportata da iOS, BlackBerry, Android e Symbian, Windows Phone.<br><br>Valore per identificare la voce umana ed escludere dalla registrazione eventuali rumori di fondo.<br><br>**AVVERTENZA: 0.2-0.28 è l'intervallo suggerito per identificare la voce umana. Valori più alti si adattano meglio alle voci femminili ma causano la registrazione di maggiori rumori di fondo.** |
| **Autosense** | Se abilitato, l'agent cerca di modificare le impostazioni del mixer audio (attiva/disattiva microfono, selezione linea e volume) per ottimizzare la qualità della registrazione audio, evitando volumi troppo bassi e o interruzioni nella registrazione. |

# Modulo Money

## Scopo

Il modulo **Money** registra le informazioni presenti nel portafoglio digitale di cryptocurrency (es.: Bitcoin) del target. In particolare registra:

- l'indirizzo/gli indirizzi del target
- l'elenco delle transazioni effettuate
- la rubrica con gli indirizzi dei destinatari delle transazioni effettuate
- il saldo

# Modulo Mouse

## Scopo

Il modulo **Mouse** cattura a ogni clic l'immagine di una piccola area dello schermo attorno al puntatore.

Utile per intercettare tastiere virtuali utilizzate per evitare le intercettazioni dei tasti della tastiera. *Vedi "Modulo Keylog" a pagina 137.*

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Larghezza** | dimensioni immagine catturata |
| **Altezza** | |

# Modulo Password

## Scopo

Il modulo **Password** registra tutte le password salvate nei vari account degli utenti. Vengono raccolte le password salvate dai browser, dagli Instant Messenger, e dai client web-mail.

# Modulo Photo

## Scopo

Il modulo **Photo** cattura fotografie del target, in particolare:

- sui dispositivi mobile: cattura le foto scattate con il dispositivo.
- sui dispositivi desktop: cattura le foto presenti nella libreria di foto (comprese le foto pubblicate su Facebook con eventuali informazioni di posizione e/o persone taggate).

# Modulo Position

## Scopo

Il modulo **Position** registra la posizione del dispositivo, utilizzando:

- sui dispositivi mobile: il sistema GPS, la cella GSM o le informazioni Wi-Fi
- sui dispositivi desktop: informazioni Wi-Fi o chek-in di Facebook

## Dati significativi mobile

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **GPS** | Ricava la posizione dalle informazioni GPS. |
| **Cell** | Ricava la posizione dalle informazioni della cella GSM o CDMA. |
| **Wifi** | Ricava la posizione dal BSSID delle stazioni Wi-Fi. |

NOTA: per Windows Phone il sistema definisce internamente come è più efficace ricavare la posizione del dispositivo in un dato momento, indipendentemente dai parametri impostati.

# Modulo Screenshot

## Scopo

Il modulo **Screenshot** cattura un'immagine dello schermo del dispositivo del target.

**IMPORTANTE: per Android, per catturare gli screenshot è necessario ottenere i privilegi di root.** ***Vedi "Cose da sapere su Android" a pagina 144.***

## Dati significativi

Di seguito la descrizione dei dati:

| *Campo* | *Descrizione* |
|---|---|
| **Qualità** | Qualità finale dell'immagine catturata.<br>**Bassa**: immagini di qualità peggiore, con massima compressione<br>**Alta**: immagini di qualità migliore, con minima compressione<br>Suggerimento: lasciare il valore di default. |
| **Solo finestra in primo piano** | (solo Desktop) Cattura un'istantanea della finestra in primo piano. |

# Modulo Url

## Scopo

Il modulo **Url** registra i nome delle pagine visitate dal browser target.

**IMPORTANTE: per BlackBerry questo modulo, per attivarsi al riavvio del dispositivo, richiede che il telefono rimanga in standby (retroilluminazione spenta) per qualche minuto.**

# 13

# Appendice: vettori di installazione

## Presentazione

### Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli vettori di installazione con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

### Contenuti


**Elenco dei vettori di installazione** ..... **143**
**Cose da sapere su Android** ..... **144**
**Ottenere un certificato per il Code Signing** ..... **145**
**Vettore Exploit** ..... **145**
**Vettore Installation Package** ..... **146**
**Preparazione Installation Package per Windows Phone** ..... **150**
**Vettore Local Installation** ..... **154**
**Vettore Melted Application** ..... **155**
**Vettore Network Injection** ..... **156**
**Vettore Offline Installation** ..... **156**
**Vettore Persistent Installation (desktop)** ..... **157**
**Vettore Persistent Installation (mobile)** ..... **159**
**Vettore QR Code/Web link** ..... **160**
**Vettore Silent Installer** ..... **161**
**Vettore U3 Installation** ..... **161**
**Vettore WAP Push Message** ..... **162**

# Elenco dei vettori di installazione

## Descrizione tipi vettori di installazione

Di seguito l'elenco dei vettori con il tipo di dispositivo e il sistema operativo supportati:

| *Installation Vector* | *Dispositivo* | *Sistema operativo* | *Descrizione* |
|---|---|---|---|
| **Exploit** | Desktop, | OS X, Windows | Inserisce l'agent in un qualsiasi documento (il formato del documento può dipendere dagli exploit disponibili). |
| | Mobile | iOS | |
| **Installation Package** | Mobile | Android, BlackBerry, iOS, Symbian, Windows Phone, WinMobile | Crea un file autoinstallante con l'agent. |
| **Local Installation** | Mobile | BlackBerry, iOS, WinMobile | Installa l'agent sul dispositivo del target o tramite USB o tramite memory card SD/MMC. |
| **Melted Application** | Desktop | Linux, OS X, Windows | Inserisce l'agent in un qualsiasi file eseguibile. |
| | Mobile | Android, Symbian, WinMobile | |
| **Network Injection** | Desktop | Linux, OS X, Windows | Rimanda alla pagina di creazione delle regole di infezione. *Vedi "**Gestione dei Network Injector**" a pagina 62*. |
| | Mobile | - | |
| **Offline Installation** | Desktop | Multipiattaforma | Crea un file ISO per la generazione di un CD/DVD/USB di avvio da utilizzare su un computer spento o ibernato. |
| **Persistent Installation** | Desktop | Windows | Inserisce l'agent nel firmware del computer del target. |
| **QR Code/Web Link** | Mobile | Multipiattaforma, Android, BlackBerry, Symbian, WinMobile | Genera un codice QR per siti o stampati, che installerà l'agent se il targetli fotografa . |

| *Installation Vector* | *Dispositivo* | *Sistema operativo* | *Descrizione* |
|---|---|---|---|
| **Silent Installer** | Desktop | Linux, OS X, Windows | Crea un file eseguibile vuoto che, quando eseguito sul dispositivo del target, installa l'agent. |
| **U3 Installation** | Desktop | Windows | Crea un pacchetto da installare su chiave U3. La chiave U3 installa l'agent automaticamente al suo inserimento sul dispositivo del target. |
| **Wap Push Message** | Mobile | Multipiattaforma, Android, BlackBerry, Symbian, WinMobile | Invia un messaggio WAP che installa l'agent se l'agent accetta il messaggio. |

# Cose da sapere su Android

## Privilegi di root

Il sistema operativo Android richiede di ottenere i privilegi di root per effettuare alcune operazioni sui suoi dispositivi.

Un agent per dispositivi Android richiede di ottenere i privilegi di root per esempio per:

- catturare le chat, *vedi "**Modulo Chat**" a pagina 133*
- catturare le e-mail, *vedi "**Modulo Messages**" a pagina 137*
- catturare gli screenshot, *vedi "**Modulo Screenshot**" a pagina 141*
- essere aggiornato, *vedi "**Pagina dell'agent**" a pagina 38*, *"**Pagina del target**" a pagina 25*

## Ottenere i privilegi di root

I privilegi di root possono essere ottenuti automaticamente, senza alcuna interazione sul dispositivo.

L'acquisizione automatica però non è sempre garantita. Se l'acquisizione automatica non riesce, se in fase di compilazione dell'agent si è selezionato **Richiesta l'interazione dell'utente** e se il sistema operativo lo consente, l'agent richiede all'utente di ottenere i privilegi manualmente dal dispositivo.

## Verificare di avere i privilegi di root

Per verificare di avere i privilegi di root sul dispositivo del target, abilitare il modulo **Device**.

Nelle evidence di tipo **Device** è indicato lo stato dei root: se i privilegi di root sono ottenuti è riportato **root:yes**.

# Ottenere un certificato per il Code Signing

## Introduzione

Per poter utilizzare la funzione di firma del codice disponibile in fase di compilazione di alcuni vettori è necessario acquistare un certificato per Code Signing emesso da una Certification Authority riconosciuta.

La maggior parte delle Certification Authority offre certificati per Code Signing, fra cui le seguenti:

- Verisign (http://www.verisign.com)
- Thawte (http://www.thawte.com)
- GoDaddy (http://www.godaddy.com)

## Installazione del certificato Code Signing

Sul sistema Backend, dalla cartella C:\RCS\DB\bin digitare il seguente comando:

**> rcs-db-config --sign-cert *FileCertificato* --sign-pass *PasswordCertificato***

**Risultato**: il certificato viene installato nel sistema e da questo momento è possibile utilizzare la funzione di firma.

# Vettore Exploit

## Scopo

La compilazione crea un installer che, una volta aperto sul dispositivo del target, sfrutta la vulnerabilità di un programma specifico. In base al tipo di Exploit possono anche esserci comportamenti diversi (es.: il programma in esecuzione s'interrompe).

## Installazione per dispositivi desktop

L'installer viene creato e automaticamente viene salvato nella cartella C:\RCS\Collector\public il pacchetto di file utili. Questi file possono essere usati in molti tipi di attacchi (es.: tramite collegamento da un sito web).

## Installazione per dispositivi mobile

L'installer deve essere copiato manualmente sul dispositivo e occorre eseguire install.sh dalla cartella copiata.

**IMPORTANTE: il dispositivo deve essere sbloccato.**

Il pacchetto di file utili viene copiato automaticamente nella cartella C:\RCS\Collector\public. Questi file possono essere usati in molti tipi di attacchi (es.: tramite collegamento da un sito web).

## Esempio di comandi per copiare un installer nel dispositivo iOS

```
mymac>scp -r ./RCS_IPHONE root@myiphone.local.net:/tmp
mymac>ssh root@myiphone.local.net
```

```
myiphone>cd /tmp/RCS_IPHONE
myiphone>sh install.sh
```

### Eliminazione di file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, nella sezione **System, Frontend**.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Tipo di file** | Tipo di file che verrà infettato (es.: .PDF). |
| **Scegli un Exploit** | Nome per esteso dell'applicativo usato dal target per aprire il file (es.: Adobe Acrobat Reader 10). |
| **URL** | Parametri che identificano il file da infettare. |
| **Document** | **URL**: collegamento a un Anonymizer dove l'installer è stato salvato. |
| **...** | **Document**: per la selezione del file da infettare. |

# Vettore Installation Package

### Scopo

La compilazione crea un eseguibile che installa l'agent in modo silente. L'eseguibile può essere caricato sul dispositivo con uno qualsiasi di questi metodi:

- download da URL
- link tramite SMS, MMS o e-mail
- direttamente da computer via cavo USB
- (solo Windows Mobile) copia diretta sulla scheda SD
- (solo Windows Phone) allegato via e-mail

### Note per sistemi operativi Android (preparazione del vettore)

La compilazione genera due vettori APK (Android Application Package File):

- *ApplicationName*.v2.apk: vettore per Android 2.x
- *ApplicationName*.default.apk: vettore per Android 3.x e 4.x

### Note per sistemi operativi Android (installazione)

Di seguito la procedura per l'installazione:

| Passo | Azione |
|---|---|
| 1 | Sul dispositivo abilitare l'opzione **Origini sconosciute** nelle impostazioni del dispositivo (tipicamente sotto **Impostazioni** , **Applicazioni** ). Terminata l'installazione è possibile disabilitare nuovamente l'opzione.<br>NOTA: se non si abilita questa opzione, durante l'installazione compare una richiesta di autorizzazione a installare un'applicazione che non appartiene all'Android Market. |
| 2 | Se il vettore contiene i moduli Screenshot, Chat e Messages è necessario ottenere i privilegi di root del dispositivo. *Vedi "Cose da sapere su Android" a pagina 144* |
| 3 | Sul dispositivo selezionare ed eseguire il vettore APK appropriato. |
| 4 | Durante l'installazione del vettore APK, accettare i permessi richiesti dall'agent. |
| 5 | Per Android 3.x e 4.x, fare clic sul pulsante **Apri** per avviare il vettore, altrimenti il vettore non sarà installato**.**<br>**IMPORTANTE: il vettore APK di default per Android 3.x e 4.x si mostra come una normale applicazione denominata DeviceInfo, che mostra le informazioni del dispositivo.** |
| 6 | Durante l'esecuzione del vettore, se è stata abilitata l'opzione **Require Administrative Privilege**, potrebbe comparire una richiesta per ottenere i privilegi di root. |

## Note per sistemi operativi Windows Phone (preparazione del vettore)

La compilazione della factory con il vettore Installation Package per il sistema operativo Windows Phone crea nella cartella RCS Download il file .zip `NomeFactory_winphone_silent.zip` che contiene due file:

- `NomeApplicazione.xap`: pacchetto con le applicazioni da installare sul dispositivo target
- `NomeApplicazione.aetx`: certificato aziendale per installare l'applicazione

**IMPORTANTE: affinché la compilazione vada a buon fine seguire la procedura per caricare in RCS i file necessari. *Vedi "Preparazione Installation Package per Windows Phone" a pagina 150***

## Note per sistemi operativi Windows Phone (installazione)

Nel pacchetto con le applicazioni `.xap` è contenuta l'applicazione MyPhoneInfo tramite la quale viene installato l'agent. L'installazione non richiede lo sblocco del cellulare.

I file.xap e .aetx possono essere inviati sul dispositivo del target:

- come allegati di una email
- come link inviati tramite email, sms o presenti su una pagina web

Nel caso di installazione via web, il server web deve correttamente supportare i tipi MIME per i file .xap e .aetx; nel file `mime.types` devono essere presenti le istruzioni:

- `application/x-silverlight-app xap`
- `application/x-aetx aetx`

Per entrambe le modalità eseguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Aprire il file *`NomeApplicazione`*`.aetx`.<br>**IMPORTANTE: questo è il certificato e deve essere sempre aperto per primo.** |
| **2** | Alle domande visualizzate rispondere facendo clic su **Add.** |
| **3** | Aprire il file *`NomeApplicazione`*`.xap`. |
| **4** | Alle domande visualizzate rispondere facendo clic su **Install**: sul telefono viene installata l'applicazione MyPhoneInfo**.** |
| **5** | Aprire almeno una volta l'applicazione MyPhoneInfo dall'elenco delle applicazioni. |
| **6** | Chiudere MyPhoneInfo: l'agent è pronto.<br>**IMPORTANTE: se si esce dall'applicazione senza chiuderla, l'applicazione e quindi l'agent, vengono sospesi. L'agent si avvia solo alla chiusura effettiva dell'applicazione o alla riaccensione del cellulare.** |

L'agent comunica con il server RCS se e finché l'applicazione MyPhoneInfo resta installata sul dispositivo e il dispositivo è acceso. Se non è disponibile una connessione dati mobile, l'agent può comunicare con il server RCS solo quando l'utente usa il telefono o il telefono è collegato a un computer o a un caricabatteria.

NOTA: all'accensione del dispositivo, l'agent impiega 30 minuti per riattivare la comunicazione con il server RCS. I 30 minuti sono garantiti se sul dispositivo sono presenti una connessione dati mobile e delle reti Wi-Fi attive, altrimenti il tempo richiesto potrebbe essere più lungo.

## Note per sistemi operativi Windows Mobile

È possibile specificare un installer CAB esistente per aggiungervi l'agent.

Se non viene specificato un CAB, il sistema utilizzerà un CAB di default che non installa nulla.

## Note per sistemi operativi BlackBerry

Per permettere il download dell'agent da parte di un BlackBerry estrarre i contenuti del file zip creato su un server Web cui il dispositivo possa accedere.

NOTA: il server Web deve correttamente supportare i tipi MIME per i file .jad e .cod, `.text/vnd.sun.j2me.app-descriptor` e `application/vnd.rim.cod`. rispettivamente. La cartella public del Collector già esegue questa funzione.

Una volta che l'installer viene eseguito sul dispositivo, accettare i permessi richiesti dall'agent.

## Note per sistemi operativi Symbian

**IMPORTANTE: per Symbian è necessario aver già ottenuto il certificato.**

## Parametri Android, WinMobile, Windows Phone

| *Nome* | *Descrizione* |
|---|---|
| **Nome applicazione** | Nome dell'applicazione (visibile al target). |
| **Richiesta l'interazione dell'utente** | (solo Android) Se l'acquisizione automatica non riesce, questa opzione abilita la richiesta all'utente di ottenere manualmente i privilegi di root dal dispositivo.<br>**ATTENZIONE: la richiesta è visualizzata sul dispositivo del target.** |

## Parametri BlackBerry

| *Nome* | *Descrizione* |
|---|---|
| **Nome applicazione** | Nome dell'installer (visibile al target). |
| **Nome**<br>**Descrizione**<br>**Vendor**<br>**Versione** | (solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent. |

### Parametri Symbian

| *Nome* | *Descrizione* |
|---|---|
| **Nome applicazione** | Nome dell'applicazione (visibile al target). |
| **Certificato legato all'IMEI** | Certificato per il dispositivo. |
| **Chiave legata al certificato** | Chiave del certificato. |
| **S60 Edition** | Versione sistema operativo. |
| **Symbian configuration** | Parametri:<br>• **UID 1-6**: elenco degli UID legati al certificato.<br>• **Key**: file di chiave. |

# Preparazione Installation Package per Windows Phone

## Introduzione

Per i dispositivi Windows Phone l'agent viene installato sul dispositivo del target attraverso un'applicazione Windows Phone. Per portare a termine l'esecuzione e l'installazione dell'agent è necessario che sul server RCS siano caricati i seguenti file:

- un file .pfx per firmare il pacchetto di installazione .xap Windows Phone
- un file .aetx come certificato per l'applicazione Windows Phone

## Sequenza consigliata

Completare i seguenti passi per generare i file .pfx e .aetx e caricarli sul server RCS:

| *Passo* | *Azione* |
|---|---|
| **1** | Ottenere un codice identificativo Symantec da usare per acquistare il certificato necessario a distribuire l'applicazione Windows Phone. |
| **2** | Ottenere il certificato Symantec necessario a distribuire applicazioni Windows Phone. |
| **3** | Installare il certificato Symantec necessario a distribuire applicazioni Windows Phone. |
| **4** | Generare il file .pfx e il file .aetx |
| **5** | Caricare il file .pfx e il file .aetx sul server RCS |

## Come leggere queste istruzioni

NOTA: i link alle pagine web inseriti nelle procedure risultano attivi al momento della scrittura del manuale. Se il link risulta inattivo, ricercare la pagina web adeguata..

In caso di contraddizione tra quanto riportato nel manuale e le istruzioni ricevute direttamente dagli enti coinvolti, seguire le istruzioni ricevute direttamente.

## Ottenere un codice identificativo Symantec

Per ottenerlo seguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Registrare un account Microsoft in https://signup.live.com/signup.aspx?lic=1. |
| **2** | Registrare un account in Windows Phone Dev Center entrando con il proprio account Microsoft in https://dev.windowsphone.com/en-us/join/ |
| **3** | • Fare clic su **Join Now**: compare la pagina per la registrazione dell'account Windows Phone Dev Center.<br>• Selezionare **Company** come **Account Type**.<br>• Fare clic su **Next.**<br>• Nella sezione **Account Info** inserire i propri dati e contatti.<br>• Nella sezione **Publisher Info** inserire come **Publisher Name** il nome che si vuole venga visualizzato come distributore dell'applicazione in fase di installazione.<br><br>**ATTENZIONE: l'utente che installa il pacchetto** .xap **e il certificato** .aetx **sul proprio telefono vede questo nome.**<br><br>• Nella sezione **Approver Info** inserire i dati e i contatti di un responsabile in azienda che può approvare la richiesta di registrazione.<br>• Completare la registrazione seguendo le istruzioni fornite dalla pagina.<br><br>**IMPORTANTE: fornire un indirizzo e-mail e un numero di telefono corretti, poiché saranno utilizzati per validare la registrazione e per fornire il Publisher ID.** |
| **4** | A registrazione completata, si viene contattati via e-mail da Symantec, azienda partner di Microsoft che si occupa della validazione delle aziende registrate al Windows Phone Dev Center, per validare la registrazione. Una ulteriore comunicazione potrebbe avvenire tramite telefono.<br><br>**IMPORTANTE: sollecitare l'Approver a rispondere tempestivamente all'e-mail di Symantec.** |
| **5** | Al termine del processo di validazione, si riceve una e-mail con i dati dell'account:<br>• Publisher ID<br>• Publisher Name |

NOTA: per approfondimenti vedi http://msdn.microsoft.com/library/windowsphone/help/jj206719(v=vs.105).aspx.

## Ottenere il certificato Symantec

L'Enterprise Mobile Code Signing Certificate è il certificato necessario per distribuire applicazioni Windows Phone.

Per ottenerlo seguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Acquistare l'Enterprise Mobile Code Signing Certificate da Symanted da https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do. |
| **2** | • Inserire il **Publisher ID** ottenuto e l'indirizzo e-mail inserito nella sezione **Account Info** durante la registrazione al Windows Phone Dev Center.<br>• Completare l'acquisto seguendo le istruzioni fornite dalla pagina. |
| **3** | Ad acquisto concluso, si ricevono da Symantec alcune e-mail con:<br>• le conferma dell'ordine<br>• l'elenco delle funzioni abilitate grazie all'ordine effettuato<br>• il certificato e le istruzioni per importarlo sul proprio computer |

NOTA: per approfondimenti vedi https://knowledge.verisign.com/support/code-signing-support/index?page=content&id=SO20770&actp=search&viewlocale=en_US.

## Installare il certificato Symantec

Per potare a buon fine l'installazione dell'Enterprise Mobile Code Signing Certificate, è necessario installare prima:

- l'Enterprise Mobile Root
- l'Enterprise Mobile CA certificate

**IMPORTANTE: utilizzare sempre lo stesso browser per scaricare i certificati. Nella procedura descritta si fa riferimento al browser Firefox.**

Seguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Aprire Firefox. |
| **2** | Copiare e incollare nella barra degli indirizzi l'URL ricevuto nell'e-mail per installare l'Enterprise Mobile Root Certificate di Microsoft. |
| **3** | Nella finestra di dialogo **Download certificato** selezionare tutte e tre le caselle di controllo e fare clic su **OK.** |

| *Passo* | *Azione* |
|---|---|
| **4** | Copiare e incollare nella barra degli indirizzi l'URL ricevuto nell'e-mail per installare l'Enterprise Mobile CA Certificate di Microsoft. |
| **4** | Nella finestra di dialogo **Download certificato** selezionare tutte e tre le caselle di controllo e fare clic su **OK.**<br><br>NOTA: per verificare l'avvenuta installazione dei certificati, selezionarela voce **Opzioni** nel menu **Firefox**, quindi selezionare la sezione **Avanzate**, e poi la scheda **Certificati,** e fare clic su **Mostra Certificati:**nell'elenco di certificati della scheda **Autorità** ci sono i nomi dei certificati installati**.** |
| **5** | Installare l'Enterprise Mobile Code Signing Certificate dal link nella e-mail ricevuta e fare clic su **Continue**. |

## Generare il file .pfx e il file .aetx

Con l'Enterprise Mobile Code Signing Certificate è possibile generare un file .pfx e un file .aetx necessari per firmare e distribuire applicazioni Windows Phone.

**IMPORTANTE: la procedura prevede che sul computer sia installato il Software Developer Kit 8.0 di Windows Phone, scaricabile da http://www.microsoft.com/it-it/download/windows.aspx. L'AET Generator tool fornito in questo Kit permette di creare il file .aetx.**

**IMPORTANTE: eseguire la procedura con lo stesso browser utilizzato per installare i certificati. Nella procedura descritta si fa riferimento al browser Firefox.**

Seguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Aprire Firefox. |
| **2** | Nel menu **Firefox** selezionare la voce **Opzioni**, quindi selezionare la sezione **Avanzate** e poi la scheda **Certificati.** |
| **3** | Fare clic su **Mostracertificati**. |
| **4** | • Nella scheda **Certificati personali** selezionare il certificato *`Publisher name`* e fare clic su **Esporta.**<br>• Salvare il file con estensione .p12.<br>• Inserire come password di esportazione del certificato: "password".<br><br>**IMPORTANTE: inserire questa e non altre password.** |
| **5** | Rinominare il file con estensione .pfx. |

| *Passo* | *Azione* |
|---|---|
| **6** | Dal prompt dei comandi di Windows entrare nella cartella dove si è salvato il file .pfx ed eseguire il seguente comando:<br>**"%ProgramFiles (x86)%\Microsoft SDKs\Windows Phone\v8.0\Tools\AETGenerator\AETGenerator.exe" *NomeFile*.pfx password**<br>dove *NomeFile* è il nome del file .pfx.<br>**Risultato**: nella cartella dove si è salvato il file .pfx vengono generati tre file:<br>• AET.aetx<br>• AET.aet<br>• AET.xml |

NOTA: per approfondimenti vedi http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj206943%28v=vs.105%29.aspx.

### Caricare il file .pfx e il file .aetx sul server database RCS

Seguire la seguente procedura:

| *Passo* | *Azione* |
|---|---|
| **1** | Copiare i file sul server database RCS. |
| **2** | Dal prompt dei comandi di Windows eseguire il seguente comando per utilizzare il file .pfx per firmare le applicazioni Windows Phone:<br>`rcs-db-config --sign-pfx-winphone PercorsoFile\NomeFile.pfx`<br>dove *PercorsoFile* è il percorso del file .pfx sul server RCS. |
| **3** | Dal prompt dei comandi di Windows eseguire il seguente comando per utilizzare il file .aetx come certificato per le applicazioni Windows Phone:<br>`rcs-db-config --sign-aetx-winphone PercorsoFile\NomeFile.aetx`<br>dove *PercorsoFile* è il percorso del file .aetx sul server RCS. |

# Vettore Local Installation

## Scopo

La compilazione installa l'agent direttamente sul dispositivo del target oppure crea una cartella sulla scheda SD da inserire nel dispositivo.

**IMPORTANTE: per completare con successo l'installazione su dispositivo BlackBerry, su un computer Windows deve essere installata l'applicazione Blackberry Desktop Software. La console produrrà un file .zip contenente tutti i file necessari a infettare il BlackBerry collegato. Copiare il file .zip sul computer Windows (se necessario) e poi decomprimerlo. Collegare il BlackBerry al PC usando un cavo USB, poi eseguire il file install.bat. Se il BlackBerry è protetto da PIN, inserire il PIN richiesto.**

**IMPORTANTE: per completare con successo l'installazione su dispositivo iOS, sul computer deve essere installata l'applicazione iTunes.**

# Vettore Melted Application

## Scopo

In compilazione modifica un eseguibile esistente inserendovi un agent.
I componenti dall'agent sono criptati per evitare eventuali attacchi di reverse engineering.

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Applicazione da usare come dropper** | File eseguibile in cui inserire l'agent.<br>Il tipo di file è diverso in base al sistema operativo:<br>**Dispositivi desktop**<br>• **OS X**: file MacOs compresso .app. È quindi necessario comprimere l'applicazione (è una cartella) con il comando zip dalla console Terminal.app.<br>**IMPORTANTE: non utilizzare la voce di menu** Compress **dall'applicazione Finder.**<br>• **Windows**: file EXE<br>• **Linux**: file DEB<br>**Dispositivi mobile**<br>• **Android**: applicazione APK di terze parti.<br>**IMPORTANTE: fare un test dell'applicazione finale. Infatti alcune applicazioni eseguono dei controlli di sicurezza addizionali a runtime.**<br>• **Symbian**: file .sisx<br>• **WinMobile**: file .cab |

| *Nome* | *Descrizione* |
|---|---|
| **Richiesta l'interazione dell'utente** | (solo Android, WinMobile, OS X) Se l'acquisizione automatica non riesce, questa opzione abilita la richiesta all'utente di ottenere manualmente i privilegi di root dal dispositivo.<br>  **ATTENZIONE: la richiesta è visualizzata sul dispositivo del target.** |

# Vettore Network Injection

## Scopo

La pagina conduce direttamente alla funzione Network Injector della sezione System.

# Vettore Offline Installation

## Scopo

La compilazione crea un autoinstallante ISO da copiare su un CD o su una USB Thumbdrive.

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Bootable CD/DVD** | Crea un autoinstallante ISO per CD o DVD. |
| **Bootable USB drive** | Crea un autoinstallante ISO per chiave USB. |
| **Dump Mask** | Estrae automaticamente i documenti appartenenti a un determinato utente. I documenti potranno essere salvati su una periferica USB per poi essere importati nel database di RCS in un secondo tempo.<br>Sono disponibili tre opzioni per la cattura dei documenti:<br>• **Documenti**: documenti MS Office, PDF e file di testo<br>• **Immagini**: foto e immagini<br>• **Personalizzato**: seleziona le estensioni dei file da catturare, separate dal carattere pipe (“\|”) |

## Installare o disinstallare l'agent

Di seguito la procedura per installare o disinstallare l'agent sul computer del target:

| *Passo* | *Azione* |
|---|---|
| **1** | Inserire il CD o la chiave USB e quindi accendere il computer del target. |

| *Passo* | *Azione* |
|---|---|
| **2** | Fare il boot dal supporto inserito e attendere la comparsa di una schermata. |
| **3** | Selezionare il sistema operativo su cui installare l'agent. |
| **4** | Selezionare dall'elenco degli utenti disponibili del sistema quelli sui quali installare l'agent. |
| **5** | Fare clic su **Install** per avviare l'installazione oppure su **Uninstall** per avviare la disinstallazione dell'agent precedentemente installato. |
| **6** | Fare clic su **Halt** per spegnere il computer oppure su **Reboot** per riavviarlo. |

### Esportare le evidence

Di seguito la procedura per esportare le evidence dal computer del target precedentemente infettato:

| *Passo* | *Azione* |
|---|---|
| **1** | Inserire il CD o la chiave USB con cui si è effettuata l'installazione e una chiave USB dove salvare le evidence. |
| **2** | Accendere il computer del target. |
| **3** | Fare il boot dal CD o dalla chiave USB di installazione e attendere la comparsa di una schermata. |
| **4** | Selezionare il sistema operativo dove è installato l'agent. |
| **5** | Selezionare dall'elenco degli utenti infettati disponibili del sistema quelli di interesse. |
| **6** | Fare clic su **Export logs** per esportare le evidence: le evidence raccolte dall'agent vengono salvate sulla chiave USB inserita appositamente. |
| **7** | Fare clic su **Halt** per spegnere il computer oppure su **Reboot** per riavviarlo. |

# Vettore Persistent Installation (desktop)

### Scopo

Il vettore **Persistent Installation** inserisce l'agent nel firmware del computer del target.
Questo tipo di infezione ha due grandi vantaggi:

- resiste alla formattazione e alla sostituzione del disco
- può essere eseguita su un computer nuovo, prima ancora della configurazione degli utenti

### Preparazione del vettore

La compilazione della factory con il vettore Persistent Installation crea nella cartella RCS Download il file .zip *NomeFactory*_windows_persistent.zip.

## Installare l'agent

*Richiede assistenza: la procedura può danneggiare irrimediabilmente il dispositivo. Prima di effettuare l'installazione contattare l'assistenza tecnica Hacking Team.*

Di seguito la procedura per installare l'agent:

| *Passo* | *Azione* |
|---|---|
| **1** | Decomprimere il file *NomeFactory*_windows_persistent.zip. |
| **2** | Copiare tutto il contenuto del file .zip decompresso su una chiavetta vuota formattata in FAT32.<br>  **IMPORTANTE: la chiavetta deve contenere solo il contenuto del file *NomeFactory*_windows_persistent.zip** |
| **3** | Spegnere il computer del target e inserire la chiavetta nella porta USB del computer. |
| **4** | Accendere il computer e fare il boot dalla chiavetta inserita: comparirà una finestra. |
| **5** | Proseguire la procedura seguendo le istruzioni presentate a video. |

## Condizioni per l'attivazione dell'infezione

Se l'installazione dell'agent è andata a buon fine, l'infezione si attiva al successivo riavvio del computer solo se è stato configurato almeno un utente. L'infezione coinvolge tutti e solo gli utenti esistenti all'attivazione dell'infezione.

Se l'installazione è avvenuta su un computer spento in modo non corretto o ibernato, occorre spegnere completamente il computer e riavviarlo, per attivare l'infezione.

## Verificare l'installazione

Poiché il computer del target non mostra alcun segnale dell'avvenuta installazione dell'agent, è necessario procedere con una verifica sulla RCS Console, prima di allontanarsi dal computer del target.

Di seguito la procedura per verificare l'installazione:

| *Se...* | *Allora...* |
|---|---|
| il computer è nuovo e non sono ancora configurati degli utenti | 1. riavviare il computer<br>2. installare Windows e configurare almeno un utente<br>3. riavviare il computer<br>4. verificare su RCS Console che l'agent sincronizzi e invii evidence<br>5. ripristinare il computer |

| *Se...* | *Allora...* |
|---|---|
| il computer ha già degli utenti configurati | 1. riavviare il computer<br>2. verificare che l'agent sincronizzi con RCS Console e invii evidence |

# Vettore Persistent Installation (mobile)

## Scopo

Il vettore **Persistent Installation** inserisce l'agent nel firmware del telefono del target. Questo tipo di infezione resiste anche al ripristino delle impostazioni di fabbrica.

## Preparazione del vettore

La compilazione genera due vettori APK (Android Application Package File):

- *ApplicationName*.v2.apk: vettore per Android 2.x
- *ApplicationName*.default.apk: vettore per Android 3.x e 4.x

Suggerimento: poichè durante l'installazione è necessario ottenere i privilegi di root del dispositivo, durante la compilazione del vettore abilitare l'opzione **Richiesta l'interazione del cliente** per assicurarsi che i privilegi vengano ottenuti.

## Installare l'agent

Di seguito la procedura per installare l'agent:

| *Passo* | *Azione* |
|---|---|
| 1 | Sul dispositivo abilitare l'opzione **Origini sconosciute** nelle impostazioni del dispositivo (tipicamente sotto **Impostazioni** , **Applicazioni** ). Terminata l'installazione è possibile disabilitare nuovamente l'opzione.<br>  NOTA: se non si abilita questa opzione, durante l'installazione compare una richiesta di autorizzazione a installare un'applicazione che non appartiene all'Android Market. |
| 2 | Ottenere i privilegi di root del dispositivo. *Vedi "Cose da sapere su Android" a pagina 144*<br>  **IMPORTANTE: sul dispositivo del target potrebbe comparire una richiesta per ottenere i privilegi.** |
| 3 | Sul dispositivo selezionare ed eseguire il vettore APK appropriato. |
| 4 | Durante l'installazione del vettore APK, accettare i permessi richiesti dall'agent. |

| *Passo* | *Azione* |
|---|---|
| 5 | Per Android 3.x e 4.x, fare clic sul pulsante **Apri** per avviare il vettore, altrimenti il vettore non sarà installato**.**<br>  **IMPORTANTE: il vettore APK di default per Android 3.x e 4.x si mostra come una normale applicazione denominata DeviceInfo, che mostra le informazioni del dispositivo.** |

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Richiesta l'interazione dell'utente** | Se l'acquisizione automatica non riesce, questa opzione abilita la richiesta all'utente di ottenere manualmente i privilegi di root dal dispositivo.<br>  **ATTENZIONE: la richiesta è visualizzata sul dispositivo del target.** |

# Vettore QR Code/Web link

### Scopo

La compilazione crea un QR Code da inserire in un qualsiasi sito web o documento cartaceo. Non appena il target cattura il codice QR, l'agent viene installato nel suo dispositivo.

### Funzionamento

Non appena il target si connette all'Anonymizer chiedendo l'installer, il Collector scarica l'installer adatto al sistema operativo del dispositivo del target dalla cartella C:\RCS\Collector\public.

 NOTA: se il sistema operativo del target è sconosciuto, usare la versione Multipiattaforma.

### Eliminazione file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, nella sezione **System**, **Frontend**.

### Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Nome applicazione** | Nome dell'installer (visibile al target). |
| **URL** | Collegamento a un Anonymizer dove l'installer è stato salvato. |

| *Nome* | *Descrizione* |
|---|---|
| **Richiesta l'interazione dell'utente** | (solo Android) Se l'acquisizione automatica non riesce, questa opzione abilita la richiesta all'utente di ottenere manualmente i privilegi di root dal dispositivo.<br>  **ATTENZIONE: la richiesta è visualizzata sul dispositivo del target.** |
| **Applicazione da usare come dropper** | (solo Android) Applicazione APK di terze parti in cui inserire l'agent.<br>  **IMPORTANTE: fare un test dell'applicazione finale. Infatti alcune applicazioni eseguono dei controlli di sicurezza addizionali a runtime.** |
| **Nome**<br>**Descrizione**<br>**Vendor**<br>**Versione** | (solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent. |
| **Certificato legato all'IMEI** | (solo Symbian) Certificato per il dispositivo. |
| **Chiave legata al certificato** | (solo Symbian) Chiave del certificato. |
| **S60 Edition** | (solo Symbian) Versione sistema operativo. |

# Vettore Silent Installer

## Scopo

La compilazione crea un eseguibile che installa l'agent in modo silente. Nessun output è visibile sul dispositivo.

# Vettore U3 Installation

## Scopo

La compilazione crea un autoinstallante ISO da scrivere su una chiave U3 (SanDisk) tramite il programma **U3 customizer** (il software può essere scaricato da Internet).

Quando la chiave è inserita nel dispositivo compare direttamente un menu (nessun disco USB viene visto automaticamente) per l'installazione degli agent.

# Vettore WAP Push Message

## Scopo

Creare un messaggio WAP-Push che invita il target a visitare un collegamento.

## Funzionamento

Invia un messaggio WAP-Push contenente del testo o il link all'installer dell'agent. Se il messaggio è accettato sul dispositivo target, l'agent sarà installato.

**IMPORTANTE: per Symbian è necessario aver già ottenuto il certificato.**

NOTA: se il sistema operativo del target è sconosciuto, usare la versione Multipiattaforma. Questa crea più installer, uno per ogni piattaforma supportata e li salva nella cartella Public del Collector. Non appena il target si connette all'Anonymizer chiedendo l'installer, il Collector scarica l'installer adatto al sistema operativo del dispositivo del target.

## Installazione

La compilazione crea un installer e automaticamente salva il pacchetto dei file utili nella cartella C:\RCS\Collector\public.

## Eliminazione dei file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, nella sezione **System, Frontend**.

## Parametri

| *Nome* | *Descrizione* |
|---|---|
| **Nome applicazione** | Nome dell'installer (visibile al target). |
| **Numero di telefono** | Numero telefonico del target, comprensivo di prefisso internazionale. |
| **URL** | Collegamento a un Anonymizer dove l'installer è stato salvato. Se il pacchetto è stato salvato su un altro sito web, specificarne l'URL. |

| *Nome* | *Descrizione* |
|---|---|
| **Service Type** | Tipo di servizio richiesto:<br>• **Loading**: il telefono target è reindirizzato automaticamente alla risorsa indicata in **URL**. In base alle impostazioni di sicurezza del telefono, l'applicazione può essere installata automaticamente oppure può apparire un messaggio per l'utente su come procedere.<br>• **Indication**: sarà visualizzato un messaggio con un testo specifico, per richiedere all'utente come proseguire.<br>• **SMS**: manda il link preceduto dal testo specificato |
| **Testo** | (solo per **Indication** e **SMS**) Testo per l'utente target. |
| **Richiesta l'interazione dell'utente** | (solo Android) Se l'acquisizione automatica non riesce, questa opzione abilita la richiesta all'utente di ottenere manualmente i privilegi di root dal dispositivo.<br>  **ATTENZIONE: la richiesta è visualizzata sul dispositivo del target.** |
| **Applicazione da usare come dropper** | (solo Android) Applicazione APK di terze parti in cui inserire l'agent.<br>  **IMPORTANTE: fare un test dell'applicazione finale poiché alcune applicazioni eseguono dei controlli di sicurezza addizionali a runtime.** |
| **Nome** | (solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent. |
| **Descrizione** | |
| **Vendor** | |
| **Versione** | |
| **Certificato legato all'IMEI** | (solo Symbian) Certificato per il dispositivo. |
| **Chiave legata al certificato** | (solo Symbian) Chiave del certificato. |
| **S60 Edition** | (solo Symbian) Versione sistema operativo. |

# Glossario dei termini

Di seguito i termini utilizzati in questo manuale e loro definizione.

## A

**Accounting**
Sezione della console dedicata alla gestione degli accessi a RCS.

**Agent**
Sonde software installate sui dispositivi sotto monitoraggio. Progettate per raccogliere prove e comunicarle al Collector.

**Agent elite**
Agente installato su dispositivi sicuri. Permette di raccogliere tutti i tipi di evidence disponibili.

**Agent scout**
Sostituto dell'agent inviato sul dispositivo per verificarne il livello di sicurezza prima di installare gli agent veri e propri (elite o soldier).

**Agent soldier**
Agente installato su dispositivi non completamente sicuri. Permette di raccogliere solo alcuni tipi di evidence.

**Alerting**
Sezione della console dedicata alle segnalazioni di nuove prove.

**Amministratore**
Colui che abilita l'accesso al sistema agli utenti, crea i gruppi di lavoro e definisce le indagini in essere, gli obiettivi e il tipo di dati da raccogliere.

**Amministratore di sistema**
Colui che installa i server e le console, si occupa degli aggiornamenti software e del ripristino dei dati in caso di malfunzionamento.

**Analista**
Persona incaricata dell'analisi dei dati raccolti durante le indagini.

**Anonymizer**
(opzionale) Protegge il server da attacchi esterni e consente l'anonimato durante le operazioni di indagine. Trasferisce i dati degli agent ai Collector.

**Audit**
Sezione della console che riporta tutte le azioni degli utenti e del sistema. Utilizzata per controllare abusi di RCS.

**avvisi da evidence**
Avvisi, normalmente email, inviati agli analisti per avvisarli che una nuova evidence corrisponde alle regole impostate.

## B

**back end**
Ambiente destinato alla decodifica e salvataggio delle informazioni raccolte. Include il Master Node e i database Shard.

**BRAS**
(Broadband Remote Access Server) instrada il traffico da/a DSLAM verso la rete dell'ISP e fornisce l'autenticazione per gli iscritti dell'ISP.

**BSSID**
(Basic Service Set IDentifier) Identificativo dell'Access Point e dei suoi client.

## C

**Carrier**
Servizio del Collector: invia i dati ricevuti dagli Anonymizer agli shard o al Master Node.

**Collector**
Servizio del Collector: riceve i dati inviati dagli agent, tramite la catena di Anonymizer.

**console**
Computer su cui è installato RCS Console. Accede direttamente a RCS Server o al Master Node.

## D

**Dashboard**
Sezione della console dedicata all'Analista. Usata per avere una rapida panoramica dello stato delle investigazioni, dei target e degli agent più importanti.

**DSLAM**
(Digital Subscriber Line Access Multiplexer) apparato di rete, spesso collocato negli scambi telefonici dell'operatore telefonico. Connette più interfacce DSL a un canale di comunicazione digitale ad alta velocità usando le tecniche di multiplexing.

## E

**entità**
Insieme di informazioni di intelligence associate al target e a persone e luoghi coinvolti nell'indagine.

**ESSID**
(Extended Service Set IDentifier) Conosciuto anche come SSID, identifica la rete WiFi.

**evidence**
Dati delle prove raccolti. Il formato dipende dal tipo di evidence (es.: immagine).

**Exploit**
Codice che, sfruttando un bug o una vulnerabilità, porta all'esecuzione di codice non previsto. Utilizzato per infettare i dispositivi dei target.

## F

**factory**
Un modello per la configurazione e la compilazione di agent.

**front end**
Ambiente destinato a comunicare con gli agent per raccogliere informazioni e impostare la loro configurazione. Include i Collector.

## G

**Gruppo**
Entità di intelligence che raggruppa più entità.

**gruppo di alerting**
Raggruppa gli utenti che devono ricevere notifiche via mail ogni volta che si genera un allarme di sistema (per esempio, il database ha superato il limite di spazio libero disponibile). Normalmente, questo gruppo è associato a nessuna operation.

## M

**Monitor**
Sezione della console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

## N

**Network Controller**
Servizio del Collector: controlla lo stato dei Network Injector e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

**Network Injector**
Componente hardware che controlla il traffico di rete del target e inietta un agent nelle risorse Web selezionate. Fornito in due versioni, Appliance o Tactical: Appliance è per installazioni presso ISP, mentre Tactical è utilizzato sul campo.

**Network Injector Appliance**
Versione rack di Network Injector, per l'installazione presso l'ISP. Cfr.: Tactical Network Injector.

## O

**operation**
Investigazione verso uno o più target, i cui dispositivi saranno i destinatari degli agent.

## P

**Person**
Entità di intelligence che rappresenta una persona coinvolta in un'indagine.

**Position**
Entità di intelligence che rappresenta un luogo coinvolto in un'indagine.

## R

**RCS**
(Remote Control System) il prodotto oggetto di questo manuale.

**RCS Console**
Software dedicato all'interazione con RCS Server.

**RCS mittente**
Sistema RCS che riceve le evidence dagli agent e li trasferisce ad altri sistemi RCS riceventi (vedi) tramite le regole di connessione. È un sistema RCS completo.

**RCS ricevente**
Sistema RCS che riceve le evidence da un altro sistema RCS mittente (vedi) e non direttamente dagli agent. Rispetto a RCS nella sua forma completa, RCS ricevente offre solo le funzioni per elaborare le evidence.

**RCS Server**
Una o più macchine, in base all'architettura di installazione, dove sono installati i componenti alla base di RCS: i database Shard, i Network Controller e Collector.

**regole di alert**
Regole che creano alert quando una nuova evidence viene salvata o quando l'agent sincronizza per la prima volta.

**regole di injection**
Impostazioni che definiscono come identificare traffico HTTP, quale risorsa da infettare e quale metodo usare per l'infezione.

## S

**sequenze di acquisizione**
Insieme di eventi, azioni e moduli di acquisizione complessi che costituiscono la configurazione avanzata di un agent.

**SSH**
(Secure SHell) protocollo di rete per sessioni remote cifrate, servizi remoti o esecuzioni comandi.

**System**
Sezione della console dedicata alla gestione del sistema.

## T

**Tactical Network Injector**
Versione portatile di Network Injector, per utilizzo tattico. Cfr.: Network Injector Appliance.

**TAP**
(Test Access Port) dispositivo hardware inserito in reti informatiche che permette il monitoraggio passivo del flusso dati in transito.

**target**
La persona fisica sotto investigazione. Nella sezione intelligence è rappresentata dall'entità Target.

**Tecnico**
Colui che su mandato dell'Amministratore crea e gestisce gli agent.

## V

**Virtual**
Entità di intelligence che rappresenta un luogo virtuale (es. un sito web) coinvolto in un'indagine.

**VPS**
(Virtual Private Server) server remoto su cui installare l'Anonymizer. Normalmente disponibile a noleggio.

# W

**WPA**

(WiFi Protected Access) Protezione per le reti WiFi.

**WPA 2**

(WiFi Protected Access) Protezione per le reti WiFi.

]HackingTeam[

**HT S.r.l.**
via della Moscova, 13
20121 Milano (MI)
Italy
**tel.**: + 39 02 29 060 603
**fax**:+ 39 02 63 118 946
www.hackingteam.com
**e-mail:**info@hackingteam.com

RCS 9.6 Manuale del tecnico
Manuale del tecnico 2.0 MAR-2015

info@hackingteam.com