

SISTEMA DE CONTROL REMOTO

GALILEO

LA SUITE DE HACKEO PARA INTERCEPTACIÓN GUBERNAMENTAL

Descripción de la solución

]lacking**Team**[

Índice

1	La empresa	1-4
2	Descripción general de la solución	2-5
3	Arquitectura.....	3-6
3.1	Front-end	3-6
3.1.1	Recopilador.....	3-6
3.1.2	Anonimizadores	3-7
3.2	Back-end.....	3-7
3.2.1	Nodo principal.....	3-7
3.2.2	Fracciones	3-7
3.3	Consola.....	3-7
3.3.1	Punto único de control	3-7
3.3.2	Soporte para el Analista.....	3-8
3.4	Módulos opcionales.....	3-8
3.4.1	Conector	3-8
3.4.2	Traducción	3-8
4	El Agente	4-9
	Compatibilidad de plataformas.....	4-9
4.1	Implementación de agentes.....	4-9
4.1.1	Infección de computadoras de escritorio y portátiles	4-10
4.1.2	Infección de smartphones.....	4-10
4.1.3	Infección en redes WiFi.....	4-11
	Vulneración de WiFi.....	4-11
	Infección de objetivos	4-11
4.1.4	Infección en líneas ADSL.....	4-12
4.1.5	Desinstalación remota.....	4-12
4.2	Evidencia recopilable	4-13

4.2.1	Escritorio	4-13
4.2.2	Móvil	4-13
4.2.3	Fuera de línea.....	4-14
4.3	Transmisión de evidencia	4-14
4.4	Comunicación fuera de canal	4-14
4.5	Paradigma de evento/acción	4-16
5	Inteligencia.....	5-17
5.1	Perfiles	5-17
5.2	Correlación	5-18
6	Cumplimiento.....	6-19
7	Mantenimiento	7-20
7.1	Soporte	7-20
7.2	Mantenimiento y control de calidad.....	7-20
8	Capacitación	8-21
Apéndice A	8-22

1 La empresa

David Vincenzetti y Valeriano Bedeschi fundaron HackingTeam en 2003, con el objetivo de concentrarse exclusivamente en la seguridad ofensiva. En el año 2004, fuimos los primeros en proponer una solución ofensiva para las investigaciones cibernéticas.

El personal técnico de HackingTeam consta de más de 50 profesionales de alto perfil, con muchos años de experiencia en todos los campos de la seguridad y el hackeo; muchos de los desarrolladores del RCS son conocidos en el área de la seguridad de TI y el ambiente clandestino.

Desarrollamos tecnología ofensiva y fácil de usar para agencias de inteligencia y orden público.

Nos motiva una gran pasión y somos líderes en este campo. Marcamos tendencias en el área de las soluciones de seguridad ofensiva que se utilizan todos los días para combatir los delitos en todos los continentes.

Luchar contra el crimen es más fácil con nuestra ayuda.

2 Descripción general de la solución

En las comunicaciones digitales de la actualidad, se utiliza mucho el cifrado para proteger a los usuarios de las escuchas no autorizadas.

Lamentablemente, el cifrado también evita que las agencias de inteligencia y orden público monitoreen y prevengan delitos y amenazas a la seguridad de la nación.

El Sistema de Control Remoto es la solución de interceptación activa y encubierta para las "Agencias Gubernamentales" que cumplan con ciertos requisitos (el "Usuario Final", de ahora en adelante "Usuario Final" o "usted"): una herramienta de investigación encubierta que se oculta dentro de los dispositivos objetivo y permite un control de procesos y monitoreo de datos activos. El Sistema de Control Remoto está diseñado para satisfacer las expectativas más altas de la comunidad de inteligencia global.

Los datos delicados se intercambian utilizando canales cifrados o no se intercambian; o en ocasiones se intercambian mediante redes que están fuera del alcance de su agencia. El Sistema de Control Remoto le da la posibilidad de recopilar esta información.

El Sistema de Control Remoto le permite rodear el cifrado y recopilar información de sus actividades objetivo. El Agente está diseñado para ser polimórfico y evadir el software antivirus común. La recopilación de evidencia se lleva a cabo de forma encubierta y la transmisión de datos al servidor del RCS se cifra con algoritmos de cifrado sólidos. El protocolo de comunicación es ligero y está diseñado para evitar la identificación. La identidad y ubicación de sus instalaciones se mantienen anónimas.

Todos los componentes del Sistema de Control Remoto se desarrollan en Milán, Italia, por un equipo de más de 50 profesionales. Desarrollamos cada línea de nuestro software: esto nos permite solucionar los errores rápidamente y personalizar el producto de acuerdo con sus necesidades.

El Sistema de Control Remoto se implementa en su sitio para permitirle controlar completamente las operaciones y la seguridad. Algunas de las características clave de la solución son:

- Alta escalabilidad y equilibrio de carga automático, para administrar fácilmente miles de objetivos simultáneamente.
- Componentes de front-end y back-end separados, con la posibilidad de realizar instalaciones geográficamente distribuidas.
- Punto único de control para todas las operaciones, con actualización y reconfiguración de los agentes implementados con un solo clic.
- Roles y privilegios de usuario con alta granularidad
- Sistema de auditoría integrada para proteger contra las amenazas internas
- Informes personalizados en HTML para verlos fuera de línea
- Integración con sistemas de terceros (p.ej., centros de monitoreo y equipos de procesamiento de audio)
- La función de OCR integrada adquiere texto de imágenes, documentos y metadatos
- Búsqueda de texto completo en toda la evidencia
- Minería de datos integrada para la creación de perfiles objetivo y la correlación de entidades
- Respaldos automáticos; configúrelos y olvídense
- Traducción automática de la evidencia a idiomas extranjeros, para comprender inmediatamente el nivel de la amenaza
- Etiquetado y anotación en la evidencia recopilada

3 Arquitectura

La infraestructura del Sistema de Control Remoto está desarrollada con distintos componentes distribuidos en la red del Usuario Remoto, en los dispositivos objetivo y en Internet.



Figura 1 - Esquema de la arquitectura de RCS

3.1 Front-end

3.1.1 Recopilador

Los recopiladores son el punto de presencia del RCS en Internet. Los agentes que se ejecutan en los dispositivos objetivo se conectan a los Recopiladores para transmitir datos y recibir comandos.

La comunicación entre los Agentes y los Recopiladores utiliza un canal cifrado y autenticado: ningún otro componente es capaz de comunicarse con los Agentes, y la seguridad está garantizada por el cifrado de doble capa.

Los Agentes utilizan Internet para comunicarse con el Recopilador; por lo tanto, usted controla sus objetivos independientemente de dónde estén ubicados.

3.1.2 Anonimizadores

Los anonimizadores protegen al Recopilador, evitando la exposición de la dirección IP real del Recopilador y, con ella, cualquier información sobre su identidad.

Los Anonimizadores dirigen la evidencia recopilada y se implementan libremente en Internet. La seguridad de la comunicación está garantizada por el sólido cifrado del canal de comunicación.

3.2 Back-end

3.2.1 Nodo Principal

El Nodo Principal es el núcleo de la infraestructura: junto con las Fracciones, almacena todos los datos de los objetivos y lleva a cabo toda la lógica de negocios.

El Sistema de Control Remoto proporciona capacidades de escalamiento sin precedentes, obtenidas agregando servidores y haciéndolos trabajar en paralelo. También ofrece equilibrio de carga automático y la posibilidad de actualizar a una versión superior, para gestionar miles de objetivos simultáneamente.

El Nodo Principal almacena los datos recopilados, gestiona la configuración de los Agentes y el desarrollo de los Vectores de Infección. Además, coordina toda la infraestructura, equilibrando el almacenamiento y calculando las necesidades entre todos los nodos disponibles.

Los respaldos automáticos ("configurelos y olvídense") están integrados: elija qué desea incluir en los respaldos y cuándo, y el sistema se encargará. Puede crear una copia de respaldo de toda la base de datos, generar respaldos selectivos de un único elemento de Operación, Objetivo o Agente, o generar un respaldo de los datos esenciales para restaurar rápidamente una copia operativa de su sistema.

3.2.2 Fracciones

Las Fracciones se utilizan para incrementar la capacidad del sistema. Son fáciles de instalar y se integran automáticamente con la infraestructura.

Al agregar Fracciones, se monitorean más Objetivos y se incrementan significativamente los tiempos de respuesta y la capacidad de almacenamiento de su sistema: navegar por la Evidencia es más rápido y usted retiene la información, siempre disponible, durante más tiempo.

Cuando se agrega una Fracción, la base de datos se equilibra automáticamente, distribuyendo los datos de acuerdo a los nuevos recursos disponibles. No es necesario llevar a cabo mantenimiento complicado.

3.3 Consola

3.3.1 Punto único de control

La Consola es el punto único de control para todo el sistema y permite llevar a cabo todas las operaciones de acuerdo a los privilegios del usuario actual.

Utilizando la Consola, se configura un Agente de dos formas:

- **Básica:** una configuración rápida y completa basada en interruptores de ENCENDIDO-APAGADO, que lo lleva de cero a listo con unos pocos clics; su Agente está listo para implementarse en apenas minutos.

- **Avanzada:** proporciona un nivel más detallado sobre la configuración, mostrándole todas las opciones para permitirle poner a punto la configuración para que se adapte perfectamente a su situación. Su interfaz gráfica que permite arrastrar y soltar es muy eficiente y le permite especificar los comportamientos articulados.

El control de acceso basado en roles (RBAC, por sus siglas en inglés) aplica el nivel de acceso correspondiente a cada usuario:

- **Administrador:** administra usuarios y grupos, otorga privilegios, crea investigaciones y realiza auditorías en el sistema para evitar los abusos.
- **Técnico:** prepara los vectores para la infección de Dispositivos y configura el comportamiento de Agentes.
- **Analista:** explora la Evidencia proveniente de los objetivos, la etiqueta y la exporta para archivarla o analizarla en más detalle.
- **Administrador del Sistema:** administra los componentes del sistema a nivel de hardware y software. Pueden especificarse más privilegios para cada rol, para controlar en más detalle las capacidades del usuario.

3.3.2 Soporte para el Analista

La **búsqueda** está disponible en toda la Consola y permite filtrar la información y llegar a las secciones interesantes. Puede efectuar búsquedas con cualquier criterio, como el nombre o una palabra clave en la descripción. Asimismo, la función de Búsqueda permite buscar texto en los datos recopilados.

Una herramienta de OCR integrada analiza las imágenes, documentos y metaetiquetas del archivo para **extraer texto en el que se pueda buscar**.

Con la función de **Alerta** recibe advertencias en tiempo real, por correo electrónico o mediante notificaciones de la consola cuando llegue evidencia interesante: si lo desea, puede configurar automáticamente la relevancia de la evidencia, para facilitar las búsquedas en el futuro.

Con la Consola puede explorar capturas de pantalla, escuchar archivos de audio, visualizar su forma de onda y navegar por mapas de las ubicaciones.

El **Generador de informes** integrado crea informes personalizados para compartir los datos recopilados con terceros, que pueden consultarlos desde cualquier navegador.

Por último, puede **monitorear** todos los componentes del sistema y recibir alertas instantáneas en caso de fallas.

3.4 Módulos opcionales

3.4.1 Conector

El Conector integra el Sistema de Control Remoto con software de terceros, como los centros de monitoreo y los equipos de procesamiento de audio.

El Conector exporta evidencia en formato JSON, y HackingTeam brinda asistencia al Usuario Final durante el proceso de integración.

3.4.2 Traducción

El módulo de Traducción traduce cualquier evidencia en forma de texto. El idioma de origen se identifica automáticamente y puede elegir el idioma de destino entre muchas posibilidades. La traducción se lleva a cabo en tiempo real, y con un clic puede pasar de la versión original a la traducción.

4 El agente

El Agente es el software que extrae información del dispositivo y monitorea la actividad del usuario. Puede recopilar muchos tipos de información, desde aplicaciones sociales hasta un registro de teclas clásico.

Generalmente el Agente envía los datos recopilados al Recopilador, pero cuando no hay una conexión a Internet disponible, la recopilación continúa mientras el agente espera la próxima oportunidad de enviarla.

Los datos recopilados se almacenan cifrados y ocultos en el dispositivo. Solo es posible llevar a cabo el descifrado en el back-end, reforzando la confidencialidad de los datos recopilados.

El Agente puede reconfigurarse en cualquier momento: un potente paradigma de evento/acción le permite definir el comportamiento, para que reaccione de acuerdo al estado del dispositivo y el entorno externo. Por ejemplo, tal vez desee recopilar el audio del micrófono únicamente cuando el dispositivo se encuentre en un radio de 50 metros de un lugar de reunión, o tal vez desee que el Agente quede silenciado si se está llevando a cabo un análisis del dispositivo.

Todos los Agentes son autónomos en su operación, incluso cuando estén aislados de Internet: no se requiere intervención de los operadores para las actividades cotidianas. Todas las conexiones tienen autenticación mutua y cifrado con potentes algoritmos, evitando así el riesgo de escuchas no autorizadas o filtraciones de datos. Asimismo, el Agente está construido para que no resulte posible atribuirlo a su creador, protegiendo así la seguridad de sus operaciones en caso de divulgación y análisis del Agente.

El Agente está oculto del usuario y es resistente a la mayoría de los antivirus y las suites de seguridad disponibles en el mercado.

Compatibilidad de plataformas

Los Agentes pueden instalarse en los siguientes Sistemas Operativos:

- Windows
- OS X
- Linux

Para smartphones, RCS es compatible con las siguientes plataformas:

- iOS
- Android
- BlackBerryWindows Phone

Investigamos constantemente las nuevas plataformas antes o inmediatamente después de su lanzamiento, para proporcionar compatibilidad lo antes posible.

Consulte el Apéndice A para ver la compatibilidad con versiones específicas.

4.1 Implementación de Agentes

Según la situación, el objetivo y las necesidades que tenga, se ofrece una gran selección de vectores de instalación para ayudarle a implementar sus Agentes.

4.1.1 Infección de computadoras de escritorio y portátiles

- **Servicio de ataque remoto:** un equipo de servicio dedicado a ayudarle a implementar sus Agentes remotamente. Proporcionamos asesoría sobre situaciones para determinar la mejor estrategia de ataque y servicio dedicado para implementarla de forma efectiva y segura.
- **Aplicación Integrada:** combine el Agente con las aplicaciones más comunes. Al ejecutarla, se presenta la aplicación original al usuario mientras se instala el Agente silenciosamente. Esta estrategia presenta muchas ventajas:
 - Se disfraza al agente como una aplicación común
 - La aplicación integrada puede entregarse de forma remota
 - Idea para ataques de ingeniería social
- **Desde la red:** el Inyector Táctico de Red (TNI) y la Aplicación de Inyectores de redes (NIA) le permiten infectar a los objetivos mediante sus conexiones WiFi y ADSL; consulte las secciones correspondientes para ver más detalles:
- **Acceso físico:** cuando el acceso físico al dispositivo no está disponible se lleva a cabo la infección independientemente de que la computadora esté ejecutándose o apagada:
 - No se requiere la contraseña del usuario
 - Por lo general demora pocos segundos
 - Desbloquea la computadora si es necesario
 - Compatibilidad con sistemas hibernados
 - Fácil de usar
 - Recupere documentos, imágenes y archivos sin infectarlos

4.1.2 Infección de smartphones

- **Servicio de Ataque Remoto:** un equipo de servicio dedicado a ayudarle a implementar sus Agentes remotamente. Proporcionamos asesoría sobre situaciones para determinar la mejor estrategia de ataque y servicio dedicado para implementarla de forma efectiva y segura.
- **Enviar un enlace web:**
 - Enviar por correo electrónico
 - Ideal para ataques de ingeniería social
 - Se puede entregar remotamente
- **Enviar un mensaje de texto con un enlace**
 - Aparece como cualquier aplicación (por ejemplo, una actualización del sistema operativo)
 - Se carga el enlace y, según la configuración del teléfono, se le solicita confirmación al usuario
 - Puede personalizar el texto para que resulte atractivo para su objetivo
- **Aplicación Integrada:** combine el Agente con las aplicaciones más comunes. Al ejecutarla, se presenta la aplicación original al usuario mientras se instala el Agente silenciosamente. Esta estrategia presenta muchas ventajas:
 - Se disfraza al agente como una aplicación común
 - Ideal para ataques de ingeniería social
 - La aplicación integrada puede entregarse de forma remota
- **Acceso físico:** cuando el acceso físico al dispositivo está disponible, se lleva a cabo la instalación local:
 - ...

4.1.3 Infección en redes WiFi

El Inyector Táctico de Red (TNI, por sus siglas en inglés) de HackingTeam es una solución portátil para infectar objetivos mediante conexiones WiFi y LAN. El TNI incrusta una tecnología patentada que permite operar sin estar en línea y ofrece vulneración de WiFi, identificación de objetivo y capacidades de infección.

Vulneración de WiFi

- Privacidad Equivalente a Cableado (WEP de 64 y 128 bits): explotando vulnerabilidades de protocolo, se puede descubrir la contraseña de WEP en apenas 3 minutos;
- Acceso Protegido a WiFi (WPA/WPA2): utilizando ataques basados en diccionario, el TNI intenta automáticamente descifrar la contraseña de WiFi;
- Configuración WiFi Protegida: un ataque especial contra el protocolo WPS intenta descifrar la contraseña de WiFi.

Infección de objetivo

El operador de TNI identificó el objetivo deseado mediante la siguiente información:

- Dirección MAC
- Dirección IP
- Nombre de host
- Sistema operativo
- Navegador en uso
- Lista de todos los sitios web visitados
- Ataques realizados contra el Objetivo

Después de identificar el objetivo, el operador lo infecta aprovechando los siguientes eventos, comunes durante el uso de Internet:

- descargar un archivo ejecutable (.exe);
- visitar un sitio web;
- ver un video en YouTube;
- visitar un recurso web (por ej., pdf, doc).

Hay funciones adicionales disponibles para facilitar el proceso de infección, como por ejemplo:

- emular un Punto de Acceso No Autorizado, para proporcionar acceso a Internet gratuito en cualquier computadora;
- reemplazar una página web legítima con una personalizada, por ejemplo, para obtener credenciales de inicio de sesión o información personal;

Por último, se proporciona el TNI con baterías adicionales para extender su autonomía a hasta 35 horas de operación continua. También se proporcionan tarjetas de red y antenas adicionales, para extender su rango operativo.

4.1.4 Infección en líneas ADSL

El Dispositivo Inyector de Red (NIA, por sus siglas en inglés) de HackingTeam es una solución diseñada para infectar a objetivos conectados a líneas de Internet ADSL. Las funciones clave son:

- implementación en el Proveedor de Servicios de Internet
- no es necesario instalar en línea, gracias a la tecnología patentada de HackingTeam
- el objetivo se identifica mediante distintos criterios:
 - Dirección IP o rango de IP
 - Dirección MAC
 - Parámetros de DHCP
 - Parámetros de radio
 - Contenido de paquetes a través de DPI
- se aplican distintas técnicas de infección a distintas actividades de objetivo:
 - descargar cualquier equipo ejecutable (.exe) de Internet;
 - navegar por la web;
 - ver videos en YouTube;
 - tener acceso a recursos web (por ejemplo, archivos pdf o doc).
- Disponible para enlaces de 1 GB y 10 GB, con conectores de fibra y cobre (SPF+)
- Administración fácil de múltiples NIA
- Soporte dedicado para la implementación de proyecto en el ISP.

4.1.5 Desinstalación remota

El Agente se desinstala de forma remota con un simple clic. Después de eliminarlo, el Agente y todos sus datos se eliminan permanentemente del dispositivo objetivo. Puede configurar el Agente para que elimine de forma segura todos los archivos, y esta eliminación resistirá un análisis forense.

4.2 Evidencia recopilable

Los agentes recopilan distintos tipos de evidencia, según el dispositivo específico y la plataforma objetivo. Se recopilan distintos tipos de datos de dispositivos de escritorio y smartphones.

4.2.1 Escritorio

En los dispositivos de escritorio, el Agente recopila:

- Grabaciones de Skype y llamadas en aplicaciones de voz
- Chats y mensajes de redes sociales (por ejemplo, Facebook, Twitter, etc.)
- Correo de clientes e interfaces web (por ejemplo, Outlook, Windows Mail, Gmail, etc.)
- Archivos abiertos, aunque estén cifrados y residan en volúmenes externos o de red
- Capturas de pantalla
- Sitios web visitados
- Contraseñas de navegadores, clientes de correo, etc.
- Registro de teclas, incluidos los teclados en pantalla
- Texto del bloc de notas (copiado y pegado)
- Posición, aunque no haya GPS
- Grabaciones del micrófono
- Información sobre el hardware y el software
- Fotos de la cámara web
- Contactos
- Y mucho más

4.2.2 Dispositivos móviles

En los dispositivos móviles, el Agente recopila la siguiente Evidencia:

- BBM, WhatsApp y otras aplicaciones de chat
- Información sobre el hardware y el software
- Información de la red celular
- Historial de llamadas
- Contactos
- Citas de calendario
- Correo electrónico y SMS
- Capturas de pantalla
- Registro de teclas
- Contraseñas almacenadas

- Posición de la señal celular, WiFi o GPS
- Grabaciones del micrófono
- Fotos de la cámara web
- Sitios web visitados
- Descarga y carga de archivos
- Y mucho más

4.2.3 Fuera de línea

Algunos dispositivos objetivo no se conectan a Internet durante períodos prolongados. En ese caso, todavía es posible recopilar evidencia para evitar pérdidas debido a que se agote el espacio en disco.

Puede elegir entre dos formas de recopilar la evidencia fuera de línea:

- **CD de arranque:** arranque desde un CD y operación mediante una interfaz gráfica sencilla. La evidencia se guarda en una unidad USB externa. Disponible para Windows y OS X.
- **USB de arranque:** arranque desde una unidad USB portátil. La misma interfaz gráfica que una unidad USB externa. Disponible para Windows.

La evidencia recopilada en línea puede importarse al RCS utilizando la Consola. Después de la importación, puede administrarla como cualquier otra evidencia recibida a través de los Recopiladores.

4.3 Transmisión de evidencia

La evidencia se transmite utilizando el mejor canal de comunicación disponible en cada oportunidad de sincronización. De otra forma, al cambiar la configuración del Agente puede **indicar un uso específico de los canales disponibles** (por ejemplo, utilizar solo WiFi o utilizar solo 3G).

En los Agentes de Windows, OS X y Linux, el Agente utiliza cualquier conexión a Internet por cable o inalámbrica disponible, y en caso de las redes WiFi, el agente utiliza automáticamente Puntos de Acceso abiertos o preconfigurados:

En los entornos empresariales, el Agente rodea los proxies y los cortafuegos para obtener acceso a Internet.

En BlackBerry, Android, iOS y Windows Phone, la transmisión utiliza GPRS/UMTS/3G/4G o WiFi. Si es necesario, el Agente puede encenderlos silenciosamente y luego apagarlos después de completar la transmisión.

Puede utilizarse un Nombre de Punto de Acceso (APN, por sus siglas en inglés) para evitar que el objetivo genere costos adicionales por las conexiones de datos del Agente; esto es útil cuando el objetivo no tiene un plan de tarifa fija para las conexiones de datos de su smartphone.

4.4 Comunicación fuera del canal

Los Agentes para smartphones pueden enviar mensajes SMS invisibles que contienen información valiosa, como detalles de la tarjeta SIM y la posición del GPS. Esto es especialmente útil cuando está en el campo y necesita detectar dónde está ubicado el dispositivo.

También puede enviar comandos al Agente mediante mensaje SMS; una vez que se lo reciba, el SMS no se muestra y se llevan a cabo las acciones configuradas. Por ejemplo, puede indicar al Agente que devuelva información sobre su posición.



Figura 2 - Flujo de evidencia del RCS

4.5 Paradigma de eventos/acciones

Se recomienda configurar todos los Agentes para que funcionen de acuerdo a criterios diseñados para adaptarse a la situación específica. Utilice la lógica de eventos/acciones incrustada para indicar al Agente que reaccione a un conjunto de eventos. Al mismo tiempo, le indica al Agente qué información debe recopilar.

En la siguiente tabla verá algunos ejemplos de las capacidades de la lógica de eventos/acciones:

Evento	Acción
Se inicia el protector de pantalla	Enviar la Evidencia recopilada al Recopilador
Se alcanza una posición del GPS	Comenzar a recopilar el audio del micrófono
La batería se está agotando	Dejar de recopilar el audio del micrófono, ya que esto drena la carga de las baterías
Cuando se recibe una llamada	Tomar una instantánea con la cámara frontal, ya que es posible que el Objetivo esté viendo quién llama, y que esté directamente frente a la Cámara
Después de 30 días	Desinstalar el Agente, ya que nuestra Operación ha finalizado

En las Figuras 3 y 4 puede ver la apariencia de la configuración avanzada. Los eventos se vinculan libremente a las acciones, y las Acciones, a su vez, se vinculan a los módulos de recopilación. Con este paradigma, puede diseñar fácilmente el comportamiento de cada uno de sus Agentes.

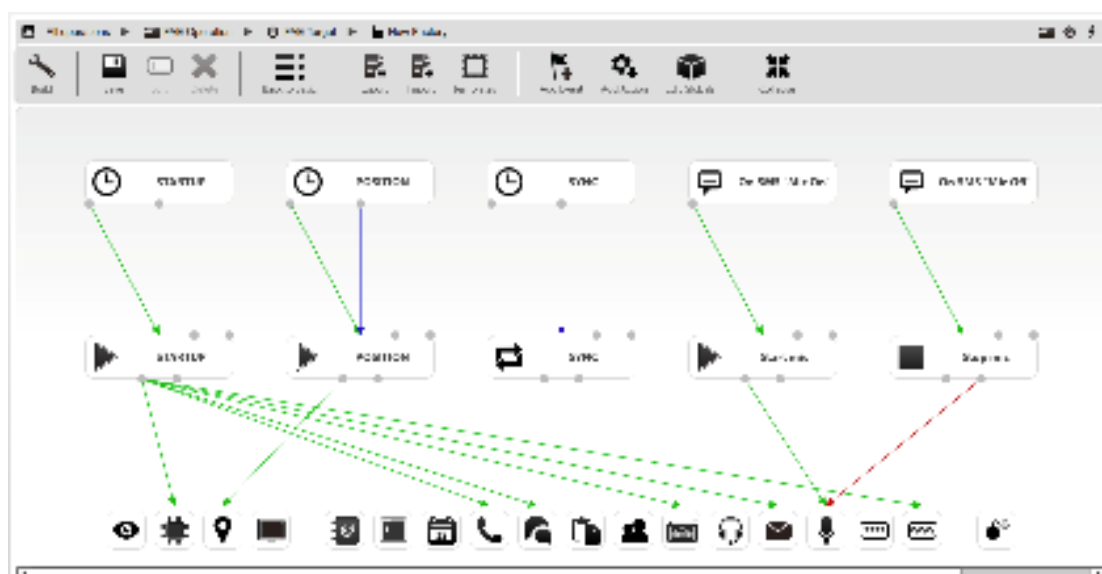


Figura 3 – Ejemplo de configuración avanzada

5 Inteligencia

El acceso a la información esencial de alto nivel de forma oportuna es fundamental y con frecuencia es decisivo para una investigación exitosa.

El Sistema de Control Remoto proporciona un motor de correlación que destaca toda la información de alto nivel relevante sobre sus objetivos y operaciones. Con el módulo de Inteligencia, puede acelerar de forma significativa su investigación y descubrir inmediatamente relaciones entre objetivos, lugares y comunicaciones.

El módulo de Inteligencia está dividido en dos funcionalidades principales:

- La opción **Perfiles** genera el perfil; combinando la identidad digital y la identidad real;
- La opción **Correlación** sintetiza la información de las interacciones (por ejemplo, las comunicaciones, las reuniones, etc.) entre distintos objetivos y operaciones.

También puede cargar manualmente información adicional (por ejemplo, fotos de objetivos, números telefónicos, cuentas, etc.) para que la correlación sea aún más completa y potente.

5.1 Generación de perfiles

La generación de perfiles concentra información útil sobre cada objetivo, como una lista de todas sus cuentas digitales (por ejemplo, Facebook, Twitter, Gmail, Skype, etc.), las personas con las que más se contacta (por correo electrónico, mensajes o llamadas telefónicas), sus sitios web más visitados y su última posición conocida.

La información de perfil se filtra por fecha, para ver cómo evoluciona el perfil a lo largo del tiempo.

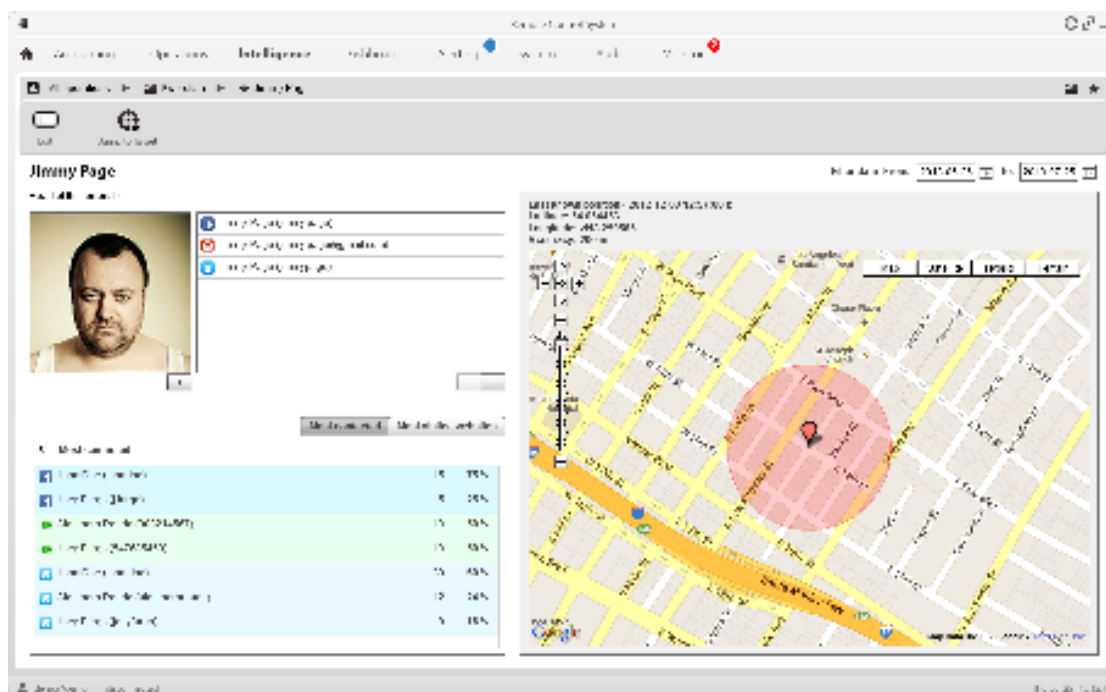


Figura 4 – Creación del perfil de un objetivo

5.2 Correlación

La correlación le proporciona una perspectiva de las relaciones e interacciones entre los objetivos y las operaciones. Gracias a esta función, puede obtener información agrupada sobre los movimientos de sus objetivos y sus hábitos de comunicación.

Abra niveles más profundos de información para ver los detalles que componen cada relación. Es fácil identificar los lugares donde su objetivo trabaja, vive o se reúne con sus cómplices y analizar el flujo de comunicaciones entre ellos.

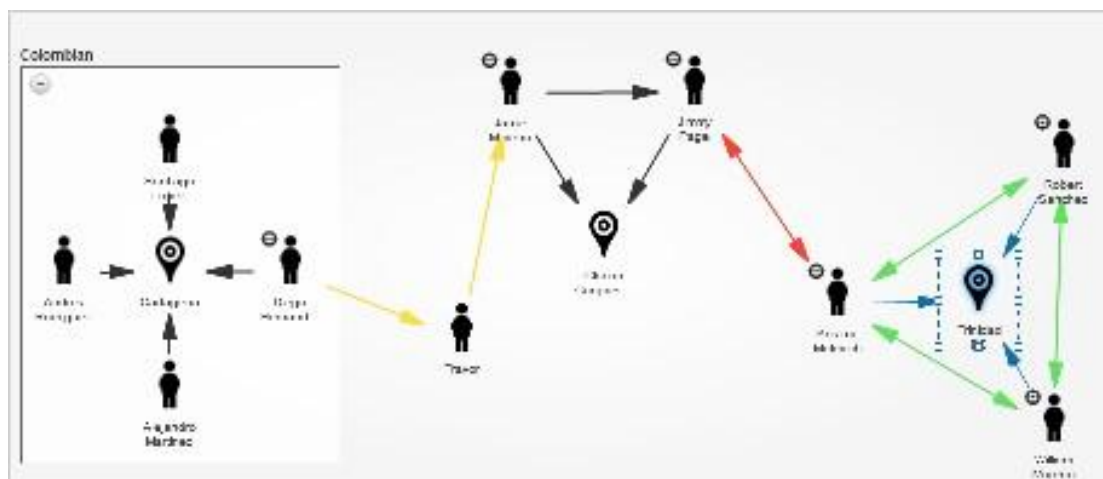


Figura 5 - Ejemplo de relaciones complejas

Con la vista de correlación también es posible ver dónde se mueve su objetivo durante el día, mediante animaciones que le permiten identificar inmediatamente cuándo y cómo se reúnen los sospechosos.

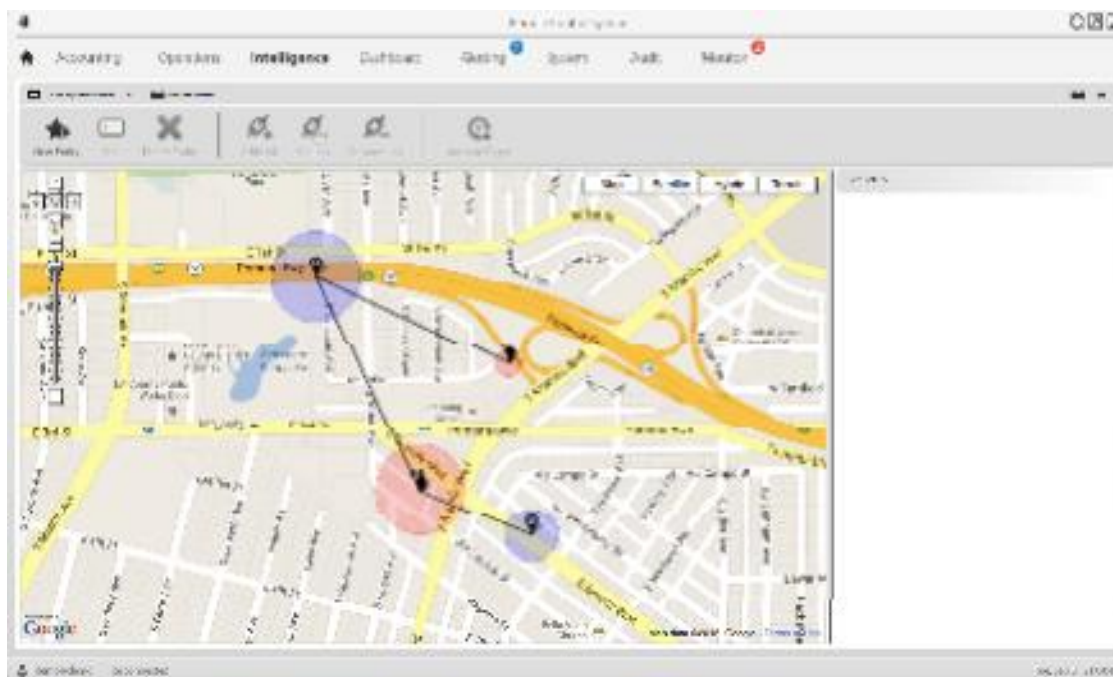


Figura 6 - Ejemplo del análisis de múltiples objetivos

6 Cumplimiento

El sistema RCS está diseñado para asegurar el uso legítimo del Sistema y la integridad de los datos recopilados. Esto se logra principalmente de la siguiente forma:

- **Administración de usuarios y privilegios:** la definición de cuatro roles estándar distintos y la posibilidad de asignar privilegios de forma granular a cada usuario garantizan que cada usuario pueda hacer solo lo que tiene permitido.
- **Administración de grupos:** la posibilidad de asignar usuarios a uno o más Grupos hace que sea posible limitar la evidencia que puede ver cada usuario, para que resulte muy sencillo definir distintos equipos para distintas operaciones.
- **Auditoría:** en la sección Auditoría se enumeran todas las operaciones ejecutadas por cada usuario; esta sección no puede modificarse ni eliminarse, y nunca vence: en cualquier momento, un usuario con la autorización correspondiente podrá ver todas las operaciones llevadas a cabo en el sistema desde el primer día.
- **Integridad de la evidencia:** la evidencia recopilada de los dispositivos monitoreados se cifra inmediatamente y se crea una suma de comprobación; el Recopilador del RCS acepta únicamente la evidencia que mantenga su integridad, de modo que solo se considere válida y se almacene la información generada en el dispositivo del sospechoso.

7 Mantenimiento

7.1 Asistencia

Puede tener acceso a la asistencia para su Sistema de Control Remoto mediante un portal de asistencia en línea, con los siguientes beneficios:

- Respuestas puntuales y competentes
- Revisión rápida de todo su historial de casos
- Descarga inmediata de nuevas versiones y actualizaciones
- Protegido mediante una conexión segura autenticada

Además, HackingTeam ofrece un **Servicio de Análisis Personalizado de Situaciones**. Si aprovecha este servicio, podrá compartir sus requisitos específicos con los expertos de HT y obtener soluciones personalizadas. La solución puede incluir el desarrollo de código personalizado o ingeniería de dispositivos ad hoc, u otras formas de ayudarlo a alcanzar su objetivo.

7.2 Mantenimiento y control de calidad

Como parte del procedimiento de mantenimiento y control de calidad del Sistema de Control Remoto, HackingTeam desarrolló un sistema de pruebas internas, denominado RiTe, que simula un conjunto de objetivos reales con diversas configuraciones de software. Todas las noches se llevan a cabo más de 500 unidades de prueba únicas en esos entornos, para evaluar un conjunto de requisitos de calidad:

- Invisibilidad contra más de 50 suites de seguridad y productos antivirus;
- Recopilación de datos de aplicaciones sociales;
- Vida útil del Agente (es decir, instalación, ejecución, actualización, desinstalación);
- Vida útil de la explotación (es decir, envío, explotación, instalación del Agente e invisibilidad).

Estas pruebas nos permiten mejorar nuestro nivel de asistencia en muchas áreas:

- Tiempos de reacción más breves en caso de anomalías o cambios repentinos en el entorno;
- Comunicaciones oportunas para mitigar el impacto en sus operaciones;
- Procedimientos de asistencia mejorados.

Por último, como parte del proceso de Mantenimiento, HT ofrece pruebas personalizadas en caso de situaciones particulares o entornos de objetivos poco comunes (por ejemplo, software antivirus menos conocido o local, versiones poco comunes de sistemas operativos, etc.).

8

Capacitación

Cuando adquiere el Sistema de Control Remoto, la capacitación sobre el producto se incluye con la entrega: se hace presente un ingeniero experto en sus instalaciones para explicarle cómo operar el sistema de forma eficiente, cómo entrenar a su personal y cómo probar su nivel de preparación. En caso de mayores necesidades, por ejemplo, para estudiar ciertos temas en profundidad, estamos disponibles para proporcionar capacitaciones de seguimiento personalizadas. Para obtener más información sobre la capacitación sobre el producto, consulte el documento anexo "HT_Galileo_ProductTraining".

Además, HackingTeam ofrece un conjunto de cursos de capacitación comprobados que ya han ayudado a muchas agencias gubernamentales a fortalecer sus habilidades de seguridad de TI. Consulte el documento anexo "HT_ITTraining".

Si desea un curso o un conjunto personalizado, comuníquese con su representante de ventas.

Apéndice A

Plataformas

Escritorio

OSX	Linux	Windows
Yosemite (10.10)	Debian	10*
Mavericks (10.9)	Fedora	8.1
Mountain Lion (10.8)	Mageia	8
Lion (10.7)	Mint	7
Snow Leopard (10.6)	Ubuntu	Vista
		XP SP3




Móvil

Android	BlackBerry	iOS	Symbian	Win Phone
5.0*	7.1	8.1	Symbian3	8.1*
4.4	7.0	7.0.2	9.4 (5ª ed.)	8.0.10327.77
4.3	6.0	6.1.2	9.3 (2ª ed. FP2)	8.0.10211.204
4.2	5.0	6.1.1	9.2 (3ª ed. FP1)	8.0.9903.10
4.1	4.6	6.0	9.1 (3ª ed. MR)	
4.0	4.5	5.1		
3.x		5.0		
2.3		4.x		
2.2		3.x		






*Experimental

Agentes

Escritorio

			
Explotación	✓		✓
Aplicación integrada	✓	✓	✓
Inyección de red	✓	✓	✓
Instalación fuera de línea	✓	✓	✓
Instalación persistente			✓
Instalación silenciosa	✓	✓	✓
Instalación U3	✓	✓	✓

Móvil

					
Explotación	✓		✓		
Paquete de instalación	✓	✓	✓	✓	✓
Instalación local		✓	✓		
Instalación integrada	✓			✓	
Instalación persistente	✓				
Código QR/enlace web	✓	✓		✓	
Mensaje push WAP	✓	✓		✓	

No todos los agentes son relevantes para todas las versiones de las plataformas; las capacidades detalladas se describirán durante la capacitación.

Sujeto a cambios in previo aviso.