Come già descritto, nel ticket della scorsa settimana stiamo ottenendo ottimi riscontri con installazioni offline su dispositivi smartphone con OS Android.

Nella settimana in corso, le nostre esigenze operative richiedevano la rapida sostituzione dello smartphone precedente menzionato in quanto risultava essere oggetto di momentanea sostituzione con un device mobile di ultima generazione nel particolare, smartphone modello SAMSUNG S4-Mini GT-I9195 Build/JDQ39 OS Android 4.2.2;. In elenco le fasi delle due operazioni.

a) Installazione nr.1

Problematiche riscontrate e contestuali risoluzioni (l'installazione è ancora in produzione).

Smartphone modello SAMSUNG GT-I9001 OS Android 2.3.6 (GINGERBREAD), al momento della prima installazione la BACKDDOR si installava rapidamente, ma al successivo reboot del device non riusciva ad acquisire i permessi di ROOT al fine di catturare altri moduli all'interno del device quali chat WhatsApp, screenshot, mail gmail etc. Vista l'urgenza dell'operazione nonostante la perseverante collaborazione del vostro STAFF nell'intento di risolvere la problematica appena citata, abbiamo deciso di dare comunque inizio all'operazione con la cattura da parte dell'agente dei soli moduli MIC e POSITION che in ogni caso risultano di *fondamentale importanza* per la nostra attività.
La configurazione in corso di operazione prevede:

1. Modulo MIC sempre accesso;
2. Modulo POSITION ogni 10 minuti in rilevazione posizione GSM;
3. Sincronizzazioni ogni 30 minuti via cella 3G/UMTS;
4. Sincronizzazioni legate all'evento ricarica del device ogni 10 minuti per 2 volte;
5. Evento batteria con range 0-10%, modulo crisis abilitato con (sincronizzazioni disabilitate di default);
6. Attraverso i silent sms abbiamo inserito solo i comandi di "*emergenza*" per ottenere sincronizzazioni immediate o disinstallare la backdoor, tuttavia come da voi consigliato ne abbiamo sempre evitato l'uso.

Con la configurazione appena descritta abbiamo effettuato dei rapidi test ed abbiamo riscontrato i seguenti problemi:

1. **Non** potevano essere effettuate le sincronizzazioni attraverso le connessioni Wi-Fi in quanto se pur spenta (perché non utilizzata) la connessione Wi-Fi sullo smartphone all'evento sincronizzazione l'icona Wi-Fi risultava accesa;
2. **Non** potevano essere collegate le sincronizzazioni "via" Wi-Fi" all'evento Standby la problematica di cui al punto precedente si riproponevano;
3. **Non** potevamo utilizzare il modulo position GPS e Wi-Fi in quanto avveniva la contestuale accensione delle icone sul device, tuttavia la problematica del modulo GPS era già nota difatti di default è sempre disabilitata in fase di configurazione;

Purtroppo non avendo altro tempo a disposizione riguardo le attività di test abbiamo consegnato il device al target, abbiamo subito riscontrato attraverso i log del sistema funzionalità per altro molto

apprezzata, un eccessivo consumo della batteria, quindi coadiuvati dai preziosi consigli dello STAFF abbiamo proceduto alla modifica della configurazione:

1. sincronizzazioni ad ogni ora;
2. modulo position disabilitato;
3. Sincronizzazioni legate all'evento ricarica del device ogni 10 minuti per 2 volte;
4. Modulo MIC sempre acceso;
5. Evento batteria con range 0-10%, modulo crisis abilitato con (sincronizzazioni disabilitate di default)

- **Imprevisti durante l'operazione e risoluzioni annesse**:

  Nella giornata di domenica u.s. il target lamentava problematiche riguardo l'utilizzo dell'applicativo SHAZAM in quanto il software appena citato risultava inutilizzabile a causa della risorsa MIC (ovviamente) occupata, siamo intervenuti con una nuova configurazione associando all'evento processo ***com.shazam.android*** il modulo CRISIS con MIC OFF, abbiamo subito avuto riscontri positivi in merito, questo soprattutto grazie alla modularità e del prodotto per quanto concerne la configurazione ed i sempre costanti indirizzi e consigli da parte dello STAFF.

- Considerazioni e proposte:

  Ribadiamo che i risultati sono ottimi considerando l'obsoleto device, tuttavia bisogna considerare i seguenti aspetti:

  1. Possiamo effettuare sincronizzazioni solo attraverso il modulo dati GSM/UMTS/LTE, questo comporta un notevole carico di traffico dati annesso alle sincronizzazioni soprattutto nel caso specifico con modulo MIC sempre accesso, comunque al momento non risulta essere un problema rilevante, poiché il target nel caso specifico utilizza un profilo tariffario dati di tipo business aziendale, ma per altre future prossime realtà operative potrà rilevarsi un problema rilevante, il quale appunto, potrà essere risolto con il corretto "*silente*" l'utilizzo delle connessioni Wi-Fi, qualora non fosse possibile inibire lo spegnimento dell'icona legata alle connessione Wi-Fi si potrebbe pensare di permettere all'agente di effettuare sincronizzazioni immediate nel momento in cui riconosce connessioni Wi-Fi attive ed autenticate sul device, al fine di bilanciare il traffico dati esperito dalle connessioni 3G ed inoltre legare all'appena detta condizione (connessioni Wi-Fi attive ed autenticate) una banda dati più ampia durante la trasmissione delle evidence.
  2. Per quanto concerne l'accensione dei moduli Wi-Fi e GPS proponiamo inoltre una **suddivisione del modulo position in: Position Wi-Fi, Position 3G e Position GPS**, in quanto *se pur consapevoli* che alla loro abilitazione otteniamo una loro contestuale accensione per alcune tipiche esigenze operative "vale la pena" effettuarne l'accensione, ovviamente l'accensione dei moduli così suddivisi potrà avvenire attraverso eventi specifici come ad esempio sms silenti, che ne giustificano il contestuale utilizzo vista la condizione operativa ritenuta dalle nostre condizioni operative di "emergenza".
  3. **Modulo MIC**, valutare la possibilità di utilizzare impostazioni autosense / vox al fine di ottimizzarne l'utilizzo legato alla batteria e la riduzione di rumori e conversazioni inutili.

4. Abbiamo riscontrato un difetto di configurazione nelle sincronizzazioni Fall Back, nello specifico facendo la prima sincronizzazione sul VPS 1 e selezionando “stop se riuscito” non dovrebbero essere eseguite eventuali azioni successive tra le quali ad esempio un log che indichi invece se eseguito lo stato del VPS1 down, tuttavia nei log riscontriamo sempre dei “falsi negativi” in quanto i nostri VPS sono quasi sempre on line questo particolare problema (non di particolare rilevanza) è stato riscontrato anche nelle configurazioni degli agenti di tipo Desktop.

b) Istallazione nr.2

Problematiche riscontrate e le contestuali risoluzioni (al momento l’installazione è *prossima* alla produzione).

Nella settima in corso abbiamo provveduto all’installazione offline sul precedentemente descritto dispositivo SAMSUNG S4-Mini GT-I9195 Build/JDQ39 OS Android 4.2.2. Nel momento in cui abbiamo provveduto all’installazione dell’agente questa è avvenuta rapidamente, ma al successivo reboot del device la BACKDOOR non ha ottenuto i permessi di root al fine di catturare altri moduli quali: chat, screenshot, mail gmail e password, avendo più tempo a disposizione per i test e la sempre instancabile disponibilità dello STAFF siamo riusciti nel root del device ed alle successive operazioni di root della sola BACKDOOR, in modo tale da nascondere il reale “modding” del device, l’operazione è stata tutta interamente svolta dallo STAFF HT la sola collaborazione che abbiamo fornito è stata nel processo di root del device seguendo le normali procedure che si trovano in rete utilizzando i software ODIN e rootkit.zip. **Durante le operazioni su citate oltre che ad apprezzare l’alta professionalità degli sviluppatori HT**, **questi sono riusciti ad utilizzare la stessa tecnica che in precedenza funzionava con firmware antecedenti anche con il firmware presente nello smartphone S4 mini che risultava essere di ultima release**, **non ci resta che “inchinarci” a così tanta competenza!** Quindi appena l’operazione di root ha dato esito positivo anche ai successivi reboot del device abbiamo potuto apprezzare le funzionalità relative alla cattura di tutti moduli. La configurazione utilizzata sul nuovo device è la stessa descritta nei punti precedenti con la ***notevole*** differenza della cattura dei moduli aggiuntivi, ovviamente con device nuovo e performance superiori abbiamo ottenuto nei test durata di batteria superiore di seguito la nuova configurazione:

1. sincronizzazioni ad ogni ora;
2. modulo position disabilitato;
3. Sincronizzazioni legate all’evento ricarica del device ogni 20 minuti per sempre;
4. Modulo MIC sempre acceso;
5. Controllo livello batteria con range da 90% a 20% con log associati;
6. Evento batteria con range 0-10%, modulo crisis abilitato con (sincronizzazioni disabilitate di default)
7. Modulo screenshot abilitato con timer loop ogni 10 secondi;
8. Moduli chat, message. e password abilitati.
9. Evento process SHAZAM crisis on

- **Considerazioni e proposte:**

Nei test effettuati abbiamo notato che, utilizzando l'APP. WhatsApp se si utilizzava la funzionalità di invio messaggi vocali, quest'ultima operazione non poteva essere svolta in quanto la risorsa MIC era (evidentemente) occupata, abbiamo utilizzato quindi la stessa tecnica per l'APP. SHAZAM ma poiché l'APP. WhatsAPP risulta essere sempre in esecuzione o in modalità BACKGROUND ed inoltre in avvio automatico sullo SNARTPHONE il device MIC risulterebbe essere sempre disabilitato, quindi non si sarebbero più più catturare evidence di tipo MIC. Abbiamo prontamente segnalato la problematica allo STAFF il quale al momento ha già prospettato soluzioni ***plausibili*** ovviamente con tempi più lunghi vista la complessità della problematica, in ogni caso abbiamo comunque deciso di perseverare con l'operazione e qualora il target dovesse lamentare lo "strano" funzionamento del device legato l'APP. WhatsAPP riguardo l'invio di messaggi vocali, eventualità tuttavia molto rara ma comunque non sottovalutabile, potremmo in ogni caso disabilitare il modulo MIC attraverso l'invio di una nuova configurazione già pronta nella sezione modelli per l'eventuale emergenza, infine al momento dell'attività presupponiamo che siano più utili le catture inerenti le chat piuttosto che le evidence di tipo MIC. Infine essendo il device in condizioni di **root:yes** qualora lo staff risolvesse la problematica potremmo operare un rapido upgrade della release, **inoltre siamo disposti ad effettuare qualsiasi tipo test avendo anche un masternode di laboratorio presso la nostra infrastruttura, nonché uno smartphone SAMSUNG S4 mini**.

Vi ringraziamo per l'assidua, cordiale e professionale collaborazione.

Roma lì 22/05/2014