

RCS-DEMOKIT

- Studio –

**SCOPO DI QUESTO DOCUMENTO**

Questo documento contiene una proposta dettagliata per l’impiego dei nuovi RCS-demokit quale strumento, tra gli altri, di dimostrazione delle funzionalità di RCS DaVinci ed è stato scritto con l’intento di selezionare dei punti di discussione sui vari temi aperti, soprattutto in termini di sicurezza.

**DESCRIZIONE GENERALE**

RCS demokit è uno strumento consegnato da Hacking Team a una lista di partner selezionati che permette loro di effettuare alcune dimostrazioni del prodotto senza la presenza o l’interazione diretta dei tecnici di Hacking Team. E’ stato ideato sulla base delle nuove policy di sicurezza che, tra le altre cose, vietano tassativamente alle persone estranee a Hacking Team o estranee ai diretti clienti di HackingTeam di venire in contatto con i sample degli installer di RCS DaVinci.

**CONTENUTO DEL DEMOKIT**

Per questo motivo un demokit consta fondamentalmente di uno o più device preinfettati con agenti che che si connettono a [www.demotime.org](http://www.demotime.org) (tramite anonimyzer chain) , raccogliendo informazioni che i partner possono mostrare dal vivo ai prospect semplicemente accedendo in console con i loro account Analyst.

Ogni demokit si presenta come una borsa/zaino contenente :

* Un laptop Windows 7
  + Modello: DELL XPS 13.3" SSD128 4GB layout USA Windows 7
  + Un adattatore usb->ethernet
* Un Android phone -> opzionale
  + Modello: Samsung Galaxy SII
* Un Blackberry -> opzionale
  + Modello: Bold 9780
* Una penna usb (non brandizzata e cifrata con Truecrypt) contenente:
  + L’installer della console
  + L’installer di Adobe AIR
  + Un documento “demokit-HowTo” che contiene parte dei contenuti di questo documento in più ne spiega il funzionamento dal punto di vista dell’utente, descrive le best practice e cosa evitare e altro
  + Note sulle credenziali di accesso (non incluse nella penna usb ma mandate via mail):
    - Truecrypt pwd
    - Password accesso dei telefoni
    - Account RCS (comprensivo di password di accesso e link del server www.demotime.org)

A meno della documentazione, in cui ci sono riferimenti al software “RCS”, la composizione del demokit è fatta in modo da non riportare alcuna informazione legata ad Hacking Team o a RCS DaVinci. Questo nasce dall’esigenza di mantenere nascosta l’identità di HT nel caso in cui il demokit venga perduto/rubato o utilizzato per scopi diversi.

In Hacking Team, conserviamo 1 documento in cui, per ogni Demokit, sono presenti:

* Dati dei device demokit (product number, model number, truecrypt password, system password, Machine name,phone password, etc.)
  + Dati del la persona a cui è stato spedito il demokit + dati del suo account utente su demotime.org
* Backup delle configurazioni degli agenti

**LICENZA di RCS-demo e BUILD AGENTI**

La licenza del server rcs-demo, verso cui si connettono i demokit-device, sarà una licenza di sviluppo. Solo Fulvio Daniele e Marco V hanno la password di accesso al server. I build degli agenti saranno tutti senza self disclosure (o demo feature), ovvero sui device infettati non compare alcun status log, nè gli agenti emettono suoni o lasciano intuire la loro presenza: ciò migliora l’impatto della dimostrazione e, soprattutto, evita che un device incustodito rilevi la presenza di RCS a persone non autorizzate.

**CONFIGURAZIONE DEI DEMOKITDEVICE**

I device demokit, sia desktop che mobile, sono configurati in modo da permettere all’agente installato di prelevare tutti i dati necessari a dimostrare efficacemente le funzionalità di RCS. Per ogni piattaforma, le configurazioni degli agenti sono identiche su tutti i demokit device. Per ogni Partner si creerà una Fake Identity (da ora “FI”, contenente nome, cognome, num telefono), in modo da simulare l’appartenenza dei device a una persona con nome e cognome . Nel server, i dati collezionati, così come le factory, apparterranno ad un Target corrispondente alla Fake Identity, similmente a quanto avviene già con le catene demo (Fake Identity Leonard Miller, John Netwood etc). Avendo gia a disposizione delle FI, provvederemo a creare una rete di contatti per ogni demokit.

**Desktop:**

* FACEBOOK/GMAIL/SKYPE: ogni laptop avrà alcuni account preconfigurati contenenti dati e contatti relativi alla Fake Identity creata per quel demokit*.*
* TRUECRYPT: ogni laptop ha il drive protetto con Truecrypt, le password sono conservate nel file DEMOKIT.xls. La stessa password apre un file posizionato sul desktop che contiene un file .txt che Viene collezionato dall’agente. Il file viene collezionato di nuovo tutte le volte che viene cancellata la evidence corrispondente sul server. Per questo si doteranno gli account Analyst della possibilità di cancellare selettivamente le evidence.
* ANTIVIRUS: i demokit Laptop verranno dotati dell’antivirus Kaspersky, precedentemente installato e configurato da Hacking Team.

**Mobile:**

* RUBRICA: ogni mobile avrà alcuni falsi contatti in rubrica, possibilmente relativi alla rete di contatti della Fake Identity dello specifico demokit.
* NO SIM: i telefoni NON conterranno alcuna simcard, sarà cura del partner provvedere al reperimento di una simcard per ogni telefono in dotazione. Questa informazione verrà specificata accuratamente nel documento di HowTo, per permettere ai partner di aggiungere gli account che potrebbero essere legati al piano operatore/piano Blackberry
* ANDROID *[Android rooted per permettere di prelevare più dati? TBD, chiedere a QUE]*

**CONFIGURAZIONI DEGLI AGENTS**

TBD

Indipendentemente dalla configurazione degli agenti, è stato previsto di modificare il codice dell’agente demokit per permettere di ricevere alcuni dati (Chat e contatti Facebook e Gmail, Chat Skype etc.) appena vengono generati e non seguendo un algoritmo il cui tempo di esecuzione non è determinabile a priori (che invece caratterizza il normale funzionamento dell’agente).

**SPECIFICHE ACCOUNT su RCS-DEMO**

Ogni demokit sarà legato ad un Analyst account col quale i partner potranno accedere a [www.demotime.org](http://www.demotime.org) per visualizzare i dati raccolti dagli agenti del demokit. I dettagli di ciascun account sono conservati nel file DEMOKIT.xls e sono definiti come segue:

* Account name: nome società (ad es.: Nice)
  + Password definita da HT e comunicata tramite sms o email (vedi: ”Contenuto del Demokit”)
* Operation e Group hanno la forma [nome societa]-[operation/group] (ad es.: Nice-Operation, Nice-Group)
* Il Target ha la forma: [Nome società]-[Fake Identity] (ad es.: Nice-Guido La Vespa)
* Gli agenti hanno la forma: [Nome società]-[modello Hardware] (ad es.: Nice-Dell XPS, Nice-Samsung Galaxy S2)

**VERSION UPGRADE/REINSTALLAZIONE AGENTE**

Ogni volta che c’è la necessità di aggiornare la versione degli agenti installati (a discrezione di HT) si indice una confcall con il partner e si gestisce da remoto l’installazione di un nuovo agente aggiornato per il device in questione. L’aggiornamento della console avviene in maniera automatica ogni volta che viene effettuato l’accesso a www.demotime.org.

**AGGIORNAMENTO PIATTAFORMA**

Per supportare il cambio di versione di un sistema operativo (ad es. A breve Windows 8, gia supportato dai demokit laptop) i demokit sul campo dovranno essere ritirati e aggiornati . I demokit verranno rialsciati con Windows 7, al momento possiamo procrastinare di circa 6 mesi il da farsi in merito al supporto per Windows 8..

**LISTA PARTNER**

RCS-Demokit verrà consegnato ai seguenti partner di Hacking Team :

* RCS SPA (Windows)
* Fajar Indah (Windows + Blackberry)
* Miliserv (Windows + Blackberry)
* Intech (Windows)
* NICE Systems (Windows+ Blackerry + Android)

**RACCOMANDAZIONI per i PARTNER**

Di seguito alcune importanti raccomandazioni che verranno inoltrate ai partner riguardo l’uso dei demokit:

* Non installare software o hardware nè aggiornare software o driver se non concordato prima con HackingTeam
* Non installare alcun antivirus se non concordato con HT e comunque non installare AV diversi da quelli concordati con HackingTeam.
* Non inserire informazioni personali *[privacy?siamo coperti? Giancarlo]*
* Limitare quanto più possibile l’utilizzo dei device da parte del prospect, non permettere al prospect di effettuare qualsiasi analisi sui devices o di navigare le cartelle del file system
* Nel documento di How TO verrà specificato accuratamente che, nel caso il Partner lo ritenga necessario, è possibile cancellare selettivamente alcune evidence. Questa funzionalità è estremamente importante nel caso di due demo successive in cui si vuole tenere nascosta l’identità delle persone coinvolte, che può essere riconosciuta da indirizzi email o chat, peggio, da foto fatte dalla webcam.