Architecture réseaux

Rush SRS (Sébastien Bombal)
Analyse Forensic

Francillon Jérôme
Roissard Stéphane
Rofes-Vernis Pierre-Yves
Herbault Jérôme
Mohtacham Pouya

But du rush SRS, Analyse Forensic

- Nous avons à disposition une image d'un disque dur issu d'un système corrompu.
- Nous devons retracer les événements ayant conduit à l'altération/divulgation des données
- Découvrir qui a pu réaliser cette attaque
- Le tout en un temps limité et en concurrence avec les autres groupes de l'option SRS.

Processus lancées

- Nous avons d'abord vérifié les processus lancées sur la machine

- Nous n’avons trouvé que des processus standard tournant sur la machine

Logiciels Installées

- Configuration de windows standard
- Logiciel de chiffrage TruCrypt

Utilisateurs de la machine

- Tim Thomas (compte administrateur)
- Pas de mot de passe pour cet utilisateur.

Réseau

- Configuration réseau : DHCP
- Le bureau à distance est désactivé
- Partages réseaux (partages standards)
  - ADMIN$
  - c$
  - IPC$
- Lecteur réseau :
  my sur 192.168.127.1
  (Portable de Tim Thomas)
  => Accès vers le portable !

Encore plus loin

- cookies:
  - google: la personne a accédé a Google.

- logiciels:

  Winword: Fichiers ouverts récemment C:/rootkit/sound.wav

Fichiers suspects

- c:/WINDOWS/AppPatch/sound.wav
  - Log du Keylogger
- c:/WINDOWS/AppPatch/pslist.exe
  - Liste les processus lancés
- c:/WINDOWS/AppPatch/*.*
  - RootKit

Les commandes brutes du keylogger ayant été exécutées sur la machine de Tim:

Started logging: Thu Jul 06 18:24:47 2006
pslist.exe listage des processus
svi486.exe
svi486.exe -ph 508 cacher le processus 508 (keylogger?)
pslist.exe
svi486.exe
pslist.exe
cd c:\windows
cd appPatch
pslit erreur
pslist listage des processus
svi486.exe
svi486.exe -ph 412 cacher le processus 508 (keylogger?)
Started logging: Thu Jul 06 18:55:20 2006
pslist
pslist
svi486
svi486 -ph 1616 cacher le processus 1616 (keylogger?)
ps aux pslist exit regeditsvi386 modification de la base de registre

Déroulement des événements:

01/07/2006 15:13	Installation de la machine.
01/07/2006 15:39	Installation de Microsoft Office.
01/07/2006 15h34	Reboot après installation
01/07/2006 16h20	Installation de Trucrypt
01/07/2006 16h25	Execution de FU.EXE (Rootkit) => infection
01/07/2006 21h12	Execution de ROOTKIT.EXE (Rootkit) => infection
01/07/2006 21h19	Execution de PSLIST.EXE (Listage des processus)
01/07/2006 21h19	Execution de FU.EXE (Rootkit) => infection
02/07/2006 21:05	Exécution du rootkit.exe
	(journaux d'événements) (Echec)
...	
06/07/2006 17h54	Execution de ROOTKIT.EXE (Rootkit) => infection
06/07/2006 17h54	Execution de FU.EXE (Rootkit) => infection
06/07/2006 17h54	Execution de PSLIST.EXE (Listage des processus)
06/07/2006 18:18	Arrêt du journal des événements
06/07/2006 18:19	Reprise du journal des événements

Explications

Le premier Rootkit a été installe des l'installation du windows. (16h25, alors que Tim Thomas était devant l'ordinateur, comme l'a mentionne le DSI)

Le soir même, un second rootkit stocké dans le fichier z:/rootkit.exe a été installé. Il s'agit du rootkit FU renommé. Ce rootkit est particulièrement dangereux, il permet de cacher et d'élever les droits Windows des processus. Il a d'ailleurs été utilisé pour cacher 3 processus sur la machine de Tim Thomas. (Surement les rootkits et le keylogger)

Son origine provient du partage Réseau Z://rootkit.exe qui correspond à l'adresse IP 192.168.127.1 (Portable de Tim Thomas)
Il a été exécute pour la première fois le 2 Juillet a 21h05 depuis Z://rootkit.exe.

Une autre possibilité est qu'un employé du nettoyage est pu s'introduire dans le bureau et booter sur un portable qui lui appartient et simuler l'accès au portable de Tim.

Explications

Par la suite, un keylogger (Logiciel enregistrant n'importe quelle touche du clavier) a été lance le 06 Juillet vers 18h24 sur la machine de Tim Thomas, comme l'indiquent les logs génèrés par le keylogger.

Enfin, la personne connectée sur la machine de Tim Thomas a tenté de cacher la présence des processus (keyloguer, rootkit ..) en cachant leurs processus via la commande :

"c:/WINDOWS/AppPatch/svi486.exe -ph [numero du processus]"

Explications

Cette même personne a tenté de voir le résultat du keylogger en ouvrant le fichier de logs (c:/rootkit/sound.wav, fichier qui a été déplacé vers Z:/WINDOWS/AppPatch/)

Nous tentons donc de savoir qui a pu accéder au portable et au pc de Tim Thomas. D'âpres ce qu'il a rapporté au DSI, seul lui a pu accéder au portable qu'il garde avec lui.

Conclusion

Nous avons pu retracer l'installation des keyloggers et rootkits.

Trop peux de preuves et de moyens nous permettent de designer de manière sure le coupable.

Conclusion

Deux principaux suspects sont

-Tim Thomas

-Le personnel de nettoyage

Nous souhaiterions donc rencontrer les deux partis afin de les questionner

Questions ?