DuQu the precursor to the next Stuxnet

Charalampos Mavroforakis
Why talk about it?

- Connection with Stuxnet (Feb 2010)
- Exploit used to get DuQu rolling
- P2P infection strategy
Goals of InfoStealer

- List of running processes
- Key presses
- File exploration, including removable drives
- Network information
- Open window names
Level-by-level

Internet
- True-type font exploit
- Kernel shellcode

Kernel
- Executes a driver to inject code in `services.exe` and runs the installer

Installer
- Decrypts the main DLL and the load point driver and creates a service. Also, writes a configuration file to the disk

Services
- Invokes the load point driver, which injects the main DLL to a process.
Level-by-level

DLL
- Reads the configuration file and injects the payload loader to the appropriate process

Loader
- Loads the payload into the memory and executes it

Payload
- Enables command-and-control (C&C) functionality

Info Stealer
- ...
Configuration file

Lifetime value

DNS Addresses

List of injected processes

<table>
<thead>
<tr>
<th>Product</th>
<th>Injection Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky Antivirus (versions 1-7)</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>Kaspersky Antivirus (versions 8-11)</td>
<td>Kaspersky process</td>
</tr>
<tr>
<td>McAfee</td>
<td>winlogon.exe</td>
</tr>
<tr>
<td>AntiVir</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>Bitdefender</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>Etrust v5 and v6</td>
<td>does not perform injection</td>
</tr>
<tr>
<td>Etrust (other versions)</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>Symantec</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>ESET NOD32</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>Trend</td>
<td>Trend process</td>
</tr>
<tr>
<td>Rising</td>
<td>Rising process</td>
</tr>
</tbody>
</table>
C&C communication protocol

HTTP & friends
- outbound requests to server
- results returned inside JPG files

SMB
- stands for Server Message Block
- is a client server, for sharing files, printers, etc.
- serves P2P cases
Peer-to-Peer C&C
Peer-to-Peer C&C

Insecure zone

Initial infected computer
Peer-to-Peer C&C

Insecure zone

Initial infected computer

Command bridge

Internet
Peer-to-Peer C&C

Insecure zone

Initial Infected computer

Command bridge

Internet

Command & Control Server
Peer-to-Peer C&C

- Insecure zone
  - Initial infected computer
  - Command bridge

- Secure zone
  - Infected server

- Internet
  - Command & Control Server
  - Command bridge
C&C functionality

Download executables

Steganography: Hiding messages, so that no one suspects their existence

Upload results

Run

Hubble image
References

- W32.Duqu – The precursor to the next Stuxnet (Symantec, Nov 2011)
- Duqu: A Stuxnet-like malware found in the wild (CrySys, Oct 2011)
- Duqu – Threat Research and Analysis (McAfee Labs)