

CONFICKER WORM INFECTION
16TH SECURITY NIGHT, 12TH OF MARCH 2009



PRESENTED BY : GILDAS DEGRAT, CISSP
GILDAS@XECUREIT.COM



- Infection
- Propagation Techniques
- Features
- How to fight?

- September of 2008
 - Exploit used by Conficker for USD 37.8
- Since October 2008
 - Conficker.A 4.7 million
 - Conficker.B 6.7 million
 - Conficker.C 16 February 2009
- 15 October 2008: Patch MSo8-067
- Conficker.A avoids Ukraine's host infection by detecting keyboard layout
- Checks for the presence of a firewall
 - If a firewall exists, the agent sends a UPNP message to open a local random high-order port

- UK Ministry of Defense (Jan 2009)
 - Administrative offices
 - 24 Royal Air Force (RAF) bases
 - 75 per cent of the Royal Navy fleet including
 - Warships
 - Submarines
 - The aircraft carrier Ark Royal
- French Military (Jan 2009)
 - Fighter jets were unable to download their flight plans
- Bundeswehr - German Military (Feb 2009)
 - Hundreds of computers

- Exploiting the Windows Server Service Vulnerability (MS08-067)
- Dropping a copy of itself into network and removable drives
- Dropping a copy of itself in network shares with weak passwords

Exploiting the Windows Server Service Vulnerability (MS08-067)

- Scanning for target machines in the network
- Generating IP addresses
- On a successful exploitation
 - The target machine will download a copy of the malicious code
 - from the affected machine
 - via its built-in HTTP server functionality

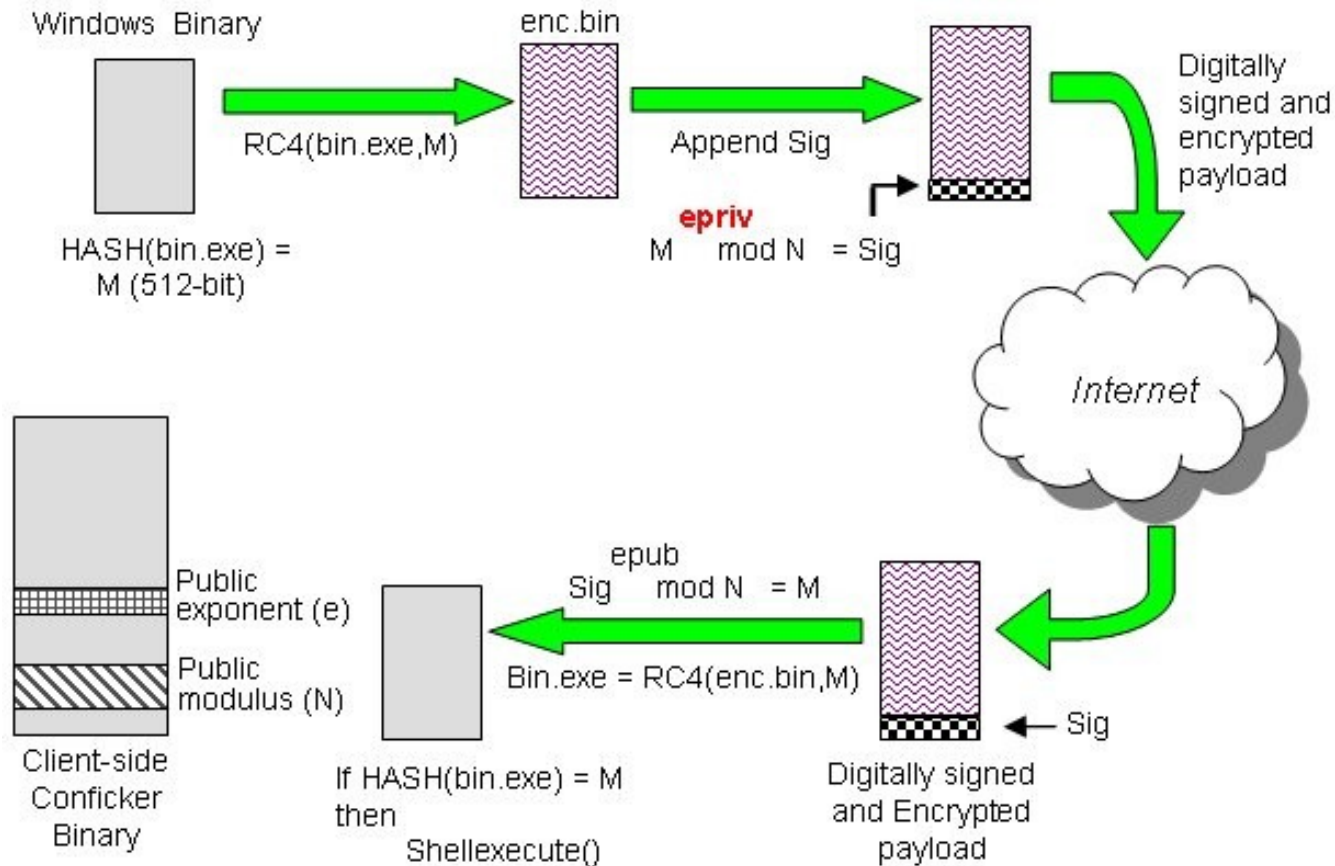
Dropping a copy of itself in network shares with weak passwords

- The malware attempts to propagate
 - by dropping a copy of itself
 - into network shares with weak passwords
 - by enumerating machines in the network
 - then attempting to connect to them
 - using a pre-defined list of passwords
 - in addition to generating passwords
 - from the user names of accounts in the target machine
 - then dropping a copy of itself in the following folder:
 - ➔ `\\(target machine)\ADMIN$\System32\%random%.%random%`
- The malware schedules a job on the target machine so that its dropped copy will be executed.

Dropping a copy of itself into network and removable drives

- It drops a copy of itself
 - as “%drive%:\RECYCLER\S-%d-%d-%d-%d-%d-%d-%d\%random%.random%”
 - then creates the file “%drive%:\autorun.inf”
 - %drive% refers to the target drive and %d refers to a random number
- Its dropped copy will automatically be executed when the drive is accessed.

- Binary validation



- Hiding Feature
 - Created files and directories are set as hidden attribute
 - Sets the file time with the file time of “%System%\kernel32.dll”
 - The malcode also sets the following registry entry:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL
 - CheckedValue = 0
 - Resets System Restore points
 - Injects itself into the svchost.exe, explorer.exe, services.exe processes
- Auto Run
 - Creates a service to load the dropped DLL on restart
 - If failed as a service then it will create the autostart registry entries
- Stops and disables the some services

- It has the capability to download and execute an arbitrary file
- Before downloading the file, it will first generate a host name with the following form:
 - %name%.%TLD%
- Where %name% is generated by the malcode and %TLD% is selected from any the following:
 - .cc, .cn, .ws, .com, .net, .org, .info, .biz
- Next, it will generate a URL with the following form:
 - http://(Resolved IP address of generated host name)/search?q=%number%
- Then download a file from the generated URL and execute it afterwards.

- The malware creates a mutex with a random name
- It also creates another mutex
 - name "Global\%s-7"
 - %s refers to a machine ID generated based from the machine name

- The malware also attempts to detect if it is running a virtual machine, if it does, it will attempt delete itself or pause execution.

- The malware also connects to the following URL in order to retrieve the external IP address of the affected machine:
 - ➔ <http://checkip.dyndns.org>
 - ➔ <http://www.whatismyip.org>
 - ➔ <http://www.whatsmyipaddress.com>
 - ➔ <http://www.getmyip.org>

- Install Network-based Intrusion Detection Systems
- Create Honeypot
- Create isolated network for re-installation
- Update patch
- Update Anti Virus
- Work with user privileges

- <http://mtc.sri.com/Conficker/>
- <http://www.iss.net/threats/conficker.html>

THANK YOU

<http://think.securityfirst.web.id>

