Unravellling Stuxnet

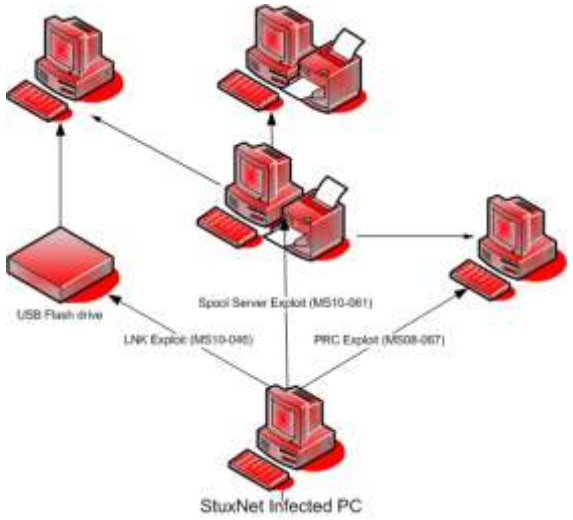
Aleks Gostev, Costin G. Raiu

Global Research and Analysis Team (GReAT)
Kaspersky Lab

September 29th, 2010. Virus Bulletin 2010 Conference

Stuxnet

- **Discovery**
- **Nemesis**
- **Analy(sz)ing Stuxnet**
- **Shared printers**
- **Analysis of network replication**
- **Spreading via MS10-061**
- **Elevation of privilege vulnerabilities**
- **Conclusions**



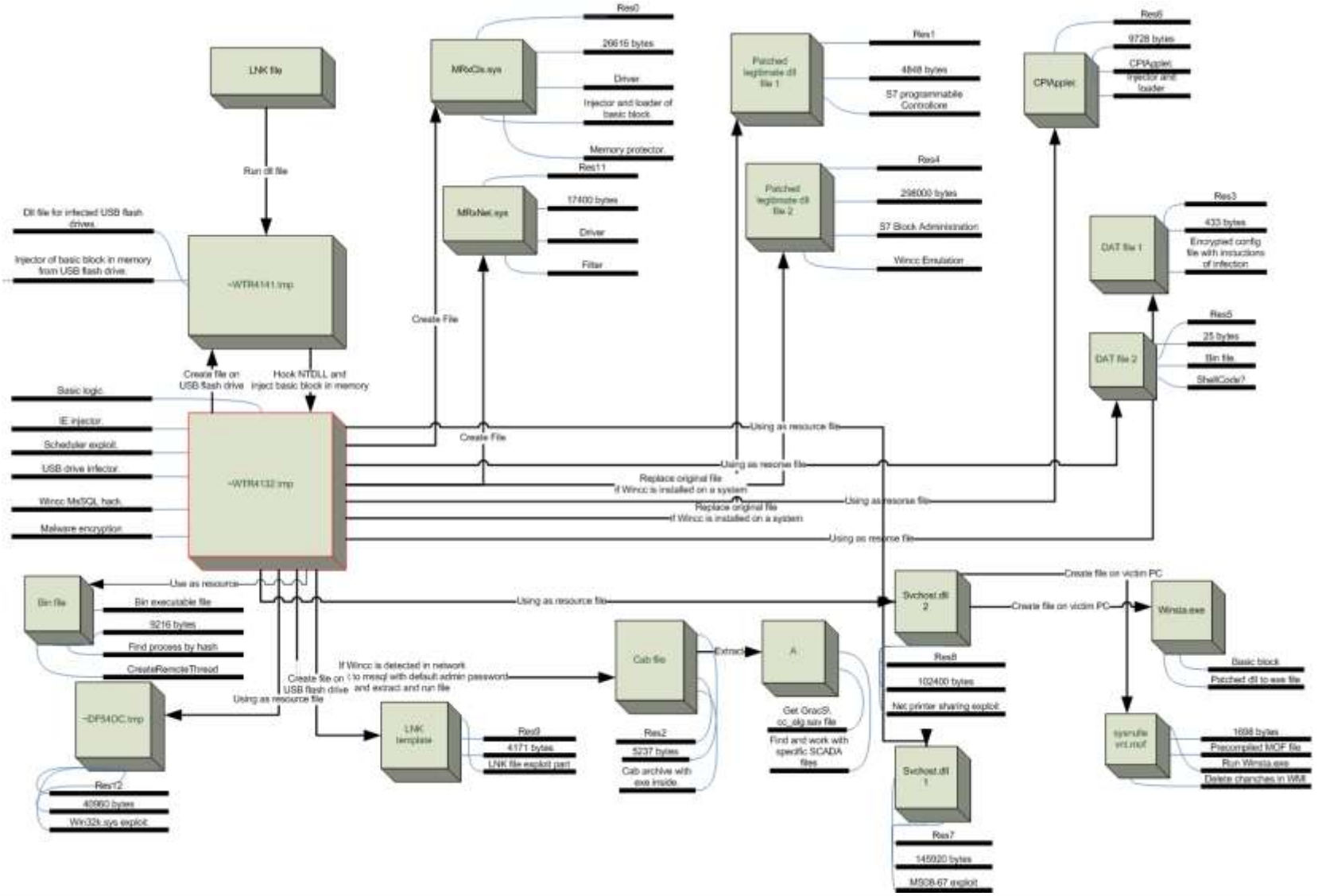
Discovery

- Early July – fellow researchers at VBA
  - Main point was stolen digital certificates
  - VBA discovered the LNK vulnerability and reported to MS
  - First focus on signed RealTek drivers
  - This was just the beginning
- Questions:
  - What was the purpose of the worm?
  - Full functionality?
  - Show me the money!!!

Nemesis

- Incident response team at KL
- Stuxnet clearly required cross departmental investigation – eventually cross-vendor
- **Results:**
  - **Huge** amount of code
  - Parallel investigation with multiple people/teams
  - In the end took 2 months
  - MS08-067 – but different exploit code from Conficker
  - Fully patched computers got infected
  - Created virtual test environments
  - Used 2 networks – only one remotely infected

Stuxnet

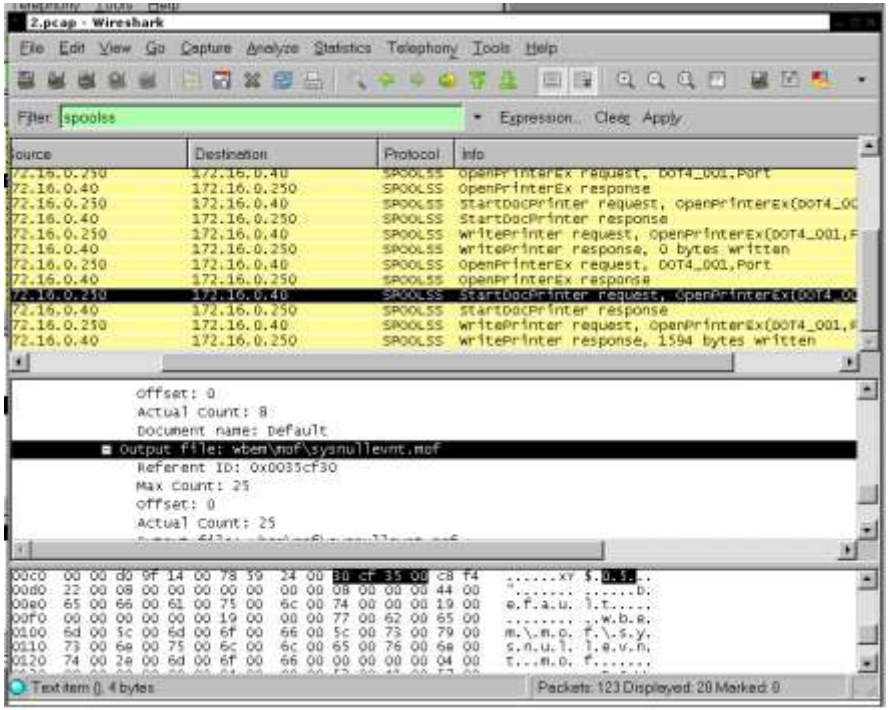

LNK file
Run dll file
Dll file for infected USB flash drives
Injector of basic block in memory from USB flash drive
~WTR4141.tmp
Create file on USB flash drive
Hook NTDLL and inject basic block in memory
Basic logic
IE injector
Scheduler exploit
USB drive infector
Wincc MsSQL hack
Malware encryption
~WTR4132.tmp
Create File
Res0
26616 bytes
Driver
Injector and loader of basic block
Memory protector
MRxCls.sys
Res11
17400 bytes
Driver
Filter
MRxNet.sys
Patched legitimate dll file 1
Res1
4848 bytes
S7 programmable Controllore
Patched legitimate dll file 2
Res4
298000 bytes
S7 Block Administration
Wincc Emulation
Res6
9728 bytes
CPVApplet
Injector and loader
CPVApplet
DAT file 1
Res3
433 bytes
Encrypted config file with insuctions of infection
DAT file 2
Res5
25 bytes
Bin file
ShellCode?
Using as resorse file
Replace original file if Wincc is installed on a system
Bin file
Use as resource
Bin executable file
9216 bytes
Find process by hash
CreateRemoteThread
~DF54DC.tmp
Res12
40960 bytes
Win32k.sys exploit
Using as resource file
Create file on USB flash drive
If Wincc is detected in network and extract and run file
LNK template
Res0
4171 bytes
LNK file exploit part
Cab file
Res2
5237 bytes
Cab archive with exe inside
Extract
A
Get GracS\ cc_dlg.scx file
Find and work with specific SCADA files
Svchost.dll 2
Create file on victim PC
Res8
102400 bytes
Net printer sharing exploit
Svchost.dll 1
Res7
145920 bytes
MS08-67 exploit
Winsta.exe
Basic block
Patched dll to exe file
1698 bytes
Precompiled MOF file
Run Winsta.exe
Delete chanches in WMI

Hands up please

How many of you have shared printers in the test networks you use for malware analysis?

New 0-day

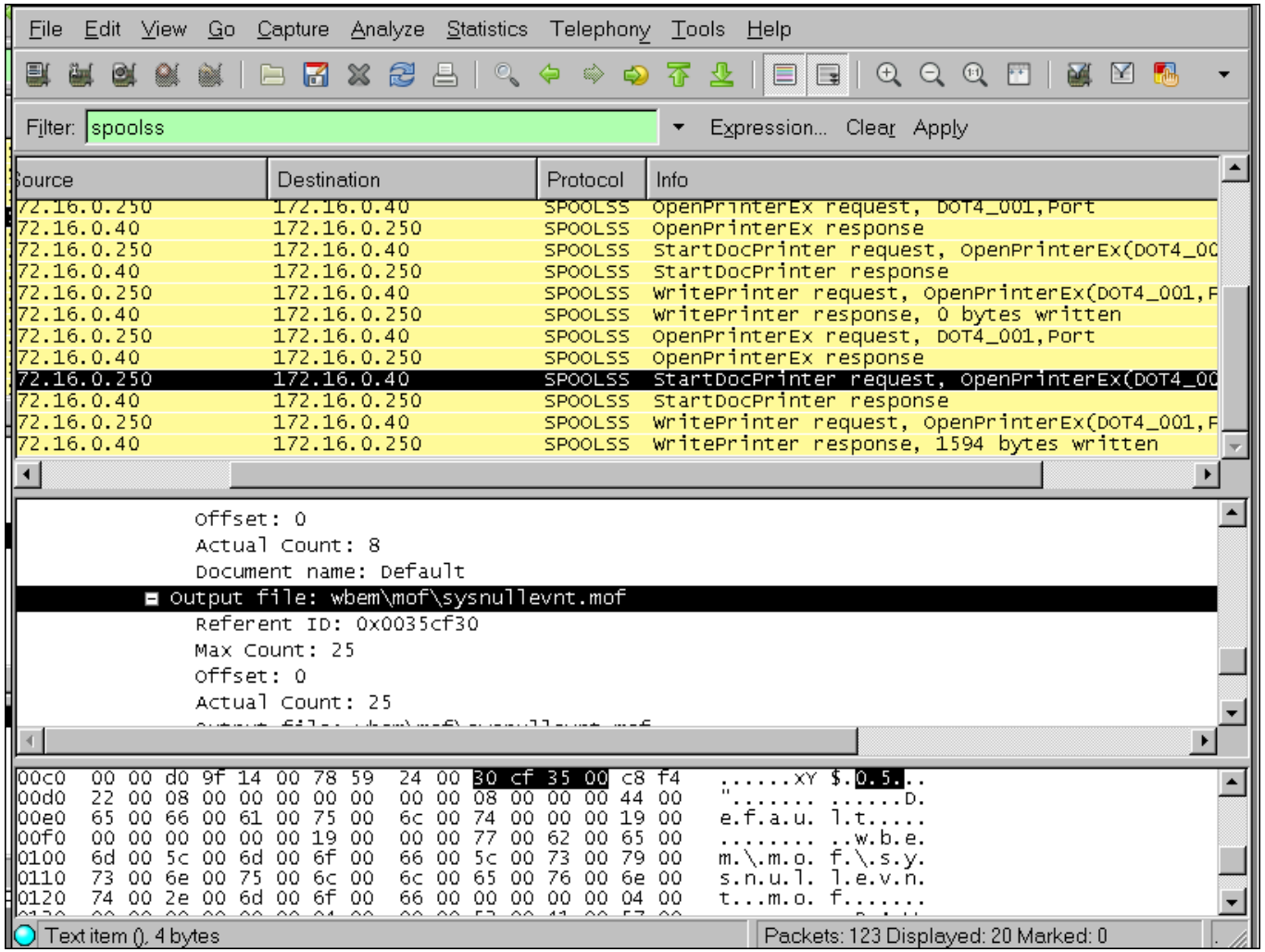
- Allowed Stuxnet to remotely infect computers with shared printers
- Already researching another vulnerability exploited by Stuxnet – an EoP
- *Finding two 0-day vulnerabilities in two days was a **big surprise** for us*



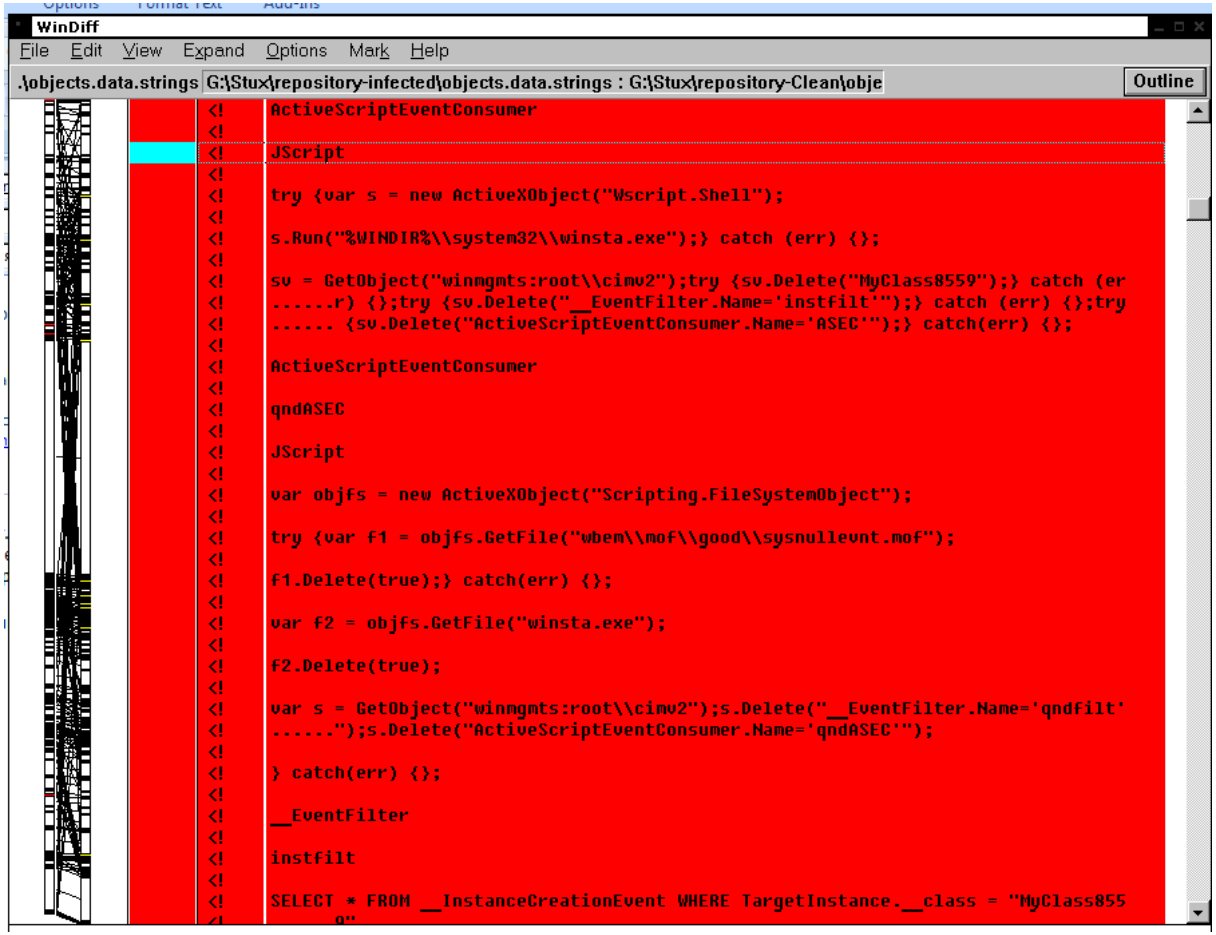
Remote infection

- Stuxnet copies two files via MS10-061 exploit:
  - the worm body “winsta.exe” in %system%
  - and “sysnullevent.mof” in %**system%\mof**
- Windows uses MOFCompiler functionality to automatically add contents of “.mof” file to the WMI repository
- Next, Windows attempts to act on the instruction from the repository
- Result - the body of the worm is executed

MOF-file (Managed Object Format)



Windiff of repositories



MOF file contains Visual Basic code which completes three actions

Was it really 0-day?

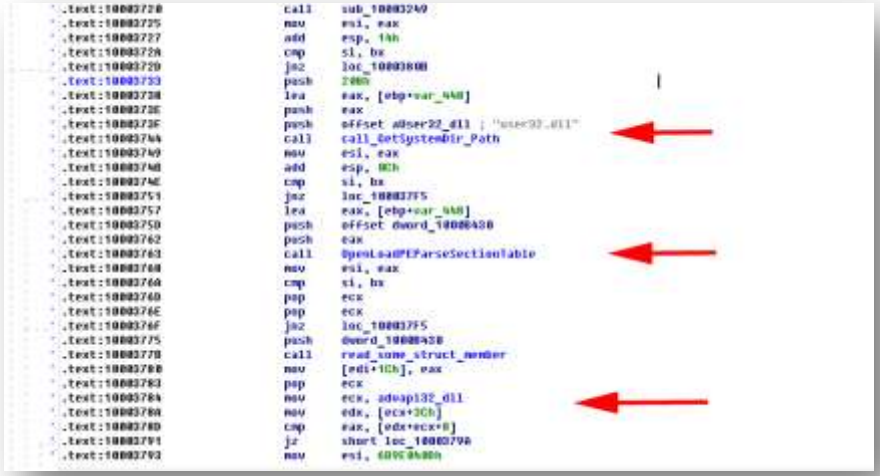
- Hakin9 magazine published an article in April 2009
- Carsten Kohler – “Print Your Shell”
- Describes a method to copy arbitrary data to remote systems
- Exactly what Stuxnet used
- Fixed via MS10-061

Use A Shared Printer to Copy Data to the Target System

Actually this part of the article is quite trivial: If a printer has been shared on a remote system and you have sufficient access to print documents on this printer, you can copy arbitrary data to this system.

An EoP vulnerability

- 0-day EoP, found by Maxim Golovkin
- Vulnerability in win32k.sys
- NtUserSendInput function
- Reported to MS via MAPP
- MSRC advisory issued, patch pending



Conclusions

- Elegant + dangerous techniques
- AV solutions don't scan CIM repositories
- CIM/MOF - not commonly used by malware… *YET*
- Shared printers => main targets were organizations
  - Extremely common in industrial networks
- Methods show attackers carefully analyzed target systems
- Next steps:
  - adding protection technologies in our products
  - Working together: security vendors, MS, Siemens, etc..

Thank you! Questions?

Aleks Gostev, Costin Raiu

GReAT
Kaspersky Lab

Virus Bulletin 2010 Conference

KASPERSKY lab