Pay attention to that man behind the curtain:
Discovering aliens on CNE infrastructure

CSEC Counter-CNE

Target Analytics thread
SIGDEV Conference
NSA – June 2010
The need for Counter-CNE...

- Foreign and friendly actors often encountered
- CNE operators do not pursue them beyond their targets
- Reporting groups need to be made aware
- OPSEC evaluation is needed
- Active pursuit of CNE actors: a different ballgame
Outline

- Introduction CCNE at CSEC
- CCNE tools and methods
- SNOWGLOBE
- De-confliction
CCNE Group at CSEC

- Part of CSEC CNE operations (K0)
- Recently formed matrix team
- Analysts and operators from CNE Operations, IO Reporting Lines and Global Network Detection
- Mandate:
  - Provide situational awareness to CNE operators
  - Discover unknown actors on existing CNE targets
  - Detect known actors on covert infrastructure
  - Pursue known actors through CNE
  - Review OPSEC of CNE operations
CCNE team

Reverse engineering

Target development

Active collection

CNE Operations

Foreign CNE actors

GND

Develop Collection signatures

Passive collection

TOP SECRET // COMINT
CNE Toolkit: WARRIORPRIDE

• **WARRIORPRIDE (WP):**
  – Scalable, Flexible, Portable CNE platform
  – Unified framework within CSEC and across the 5 eyes
  – Do more with less effort
    • Common framework for sharing code/plugins across the 5 eyes
    • WARRIORPRIDE is an implementation of the “WZOWSKI” 5-eyes API
  – WARRIORPRIDE@CSE/etc. == DAREDEVIL@GCHQ

• **WARRIORPRIDE**
  – xml command output to operators
  – Several plugins used for machine recon / OPSEC assessment
WARRIORPRIDE

Command Prompt - U_Base

Output

Transaction Id: 138546
Core storage files for implant 127.0.0.1
==================================
Plugin Store: c:\Temp\DP3BE9.tmp
Config Store: c:\Temp\configFileSys.sys
Note that this command does not list plugi
WARRIORPRIDE plug-ins and output

• Several WP plugins are useful for CCNE:
  – Slipstream: machine reconnaissance
  – ImplantDetector: implant detection
  – RootkitDetector: rootkit detection
  – Chordflier/U_ftp: file identification / retrieval
  – NameDropper: DNS
  – WormWood: network sniffing and characterization

• Already used for CNE OPSEC

• Used for precise identification and heuristics
<?xml version="1.0" encoding="UTF-8"?>
<response xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="U_FileCollectorLp/U_FileCollectorLp_2.15.xsd">
   <implantId>51.1.2.160</implantId><transaction><transactionSource>50.0.0.101</transactionSource><transactionId>320453</transactionId></transaction><timestamp><TLT>2010-02-23T15:53:06.366</TLT><UTC>2010-02-23T15:47:43.448</UTC></timestamp><errors><errorPlugin>0</errorPlugin><errorOs>0</errorOs></errors><commandInfo>fcstart</commandInfo><responseDetails><fcstart><status>Success</status><standbyMode>FALSE</standbyMode></fcstart></responseDetails></response>
<table>
<thead>
<tr>
<th>PID</th>
<th>Service Name</th>
<th>Status</th>
<th>Startup Type</th>
<th>Service Process Type</th>
<th>Display Name</th>
<th>Binary Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Alerter</td>
<td>STOPPED</td>
<td>DISABLED</td>
<td>SHARED</td>
<td>Alerters</td>
<td>C:\WINDOWS\system32\svchost.exe -k</td>
</tr>
<tr>
<td>3184</td>
<td>Alg</td>
<td>RUNNING</td>
<td>MANUAL</td>
<td>OWN PROCESS</td>
<td>Application Layer Gateway Service</td>
<td>C:\WINDOWS\System32\alg.exe</td>
</tr>
<tr>
<td>924</td>
<td>AppMgmt</td>
<td>STOPPED</td>
<td>MANUAL</td>
<td>SHARED</td>
<td>Application Management</td>
<td>C:\WINDOWS\system32\svchost.exe -k</td>
</tr>
<tr>
<td>924</td>
<td>AudioSrv</td>
<td>RUNNING</td>
<td>AUTOMATIC</td>
<td>SHARED</td>
<td>Windows Audio</td>
<td>C:\WINDOWS\System32\svchost.exe</td>
</tr>
<tr>
<td>0</td>
<td>B itching</td>
<td>STOPPED</td>
<td>MANUAL</td>
<td>SHARED</td>
<td>Background Intelligent Transfer Service</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Browser</td>
<td>STOPPED</td>
<td>AUTOMATIC</td>
<td>SHARED</td>
<td>Computer Browser</td>
<td>C:\WINDOWS\system32\svchost.exe -k</td>
</tr>
<tr>
<td>1028</td>
<td>ccEvntMgr</td>
<td>RUNNING</td>
<td>AUTOMATIC</td>
<td>SHARED</td>
<td>Symantec Event Manager</td>
<td>&quot;C:\Program Files\Common</td>
</tr>
<tr>
<td>1028</td>
<td>ccSetMgr</td>
<td>RUNNING</td>
<td>AUTOMATIC</td>
<td>SHARED</td>
<td>Symantec Settings Manager</td>
<td>&quot;C:\Program Files\Common</td>
</tr>
<tr>
<td>1708</td>
<td>Cissannerservice</td>
<td>RUNNING</td>
<td>AUTOMATIC</td>
<td>OWN PROCESS</td>
<td>HP Smart Array SAS/SATA Event Notification Service</td>
<td>&quot;C:\Program</td>
</tr>
<tr>
<td>0</td>
<td>CiSvc</td>
<td>STOPPED</td>
<td>DISABLED</td>
<td>SHARED</td>
<td>Indexing Service</td>
<td>C:\WINDOWS\system32\cisvc.exe</td>
</tr>
<tr>
<td>0</td>
<td>ClipSrv</td>
<td>STOPPED</td>
<td>DISABLED</td>
<td>OWN PROCESS</td>
<td>ClipBook</td>
<td></td>
</tr>
</tbody>
</table>
WP SLIPSTREAM output... drivers (parsed)

<table>
<thead>
<tr>
<th>Driver Name</th>
<th>Status</th>
<th>Startup Type</th>
<th>Driver Type</th>
<th>Display Name</th>
<th>Binary Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntoskrnl.exe</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\ntoskrnl.exe</td>
</tr>
<tr>
<td>hal.dll</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\hal.dll</td>
</tr>
<tr>
<td>KDCOM.DLL</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\KDCOM.DLL</td>
</tr>
<tr>
<td>BOOTVID.dll</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\BOOTVID.dll</td>
</tr>
<tr>
<td>ACPI.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\ACPI.sys</td>
</tr>
<tr>
<td>WMLIB.SYS</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\WMLIB.SYS</td>
</tr>
<tr>
<td>pci.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\pci.sys</td>
</tr>
<tr>
<td>sapnp.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\sapnp.sys</td>
</tr>
<tr>
<td>pcide.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\pcide.sys</td>
</tr>
<tr>
<td>PCLI.EXED.SYS</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\PCLI.EXED.SYS</td>
</tr>
<tr>
<td>MountMgr.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\MountMgr.sys</td>
</tr>
<tr>
<td>ftdisk.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\ftdisk.sys</td>
</tr>
<tr>
<td>dmload.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\dmload.sys</td>
</tr>
<tr>
<td>dmio.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\dmio.sys</td>
</tr>
<tr>
<td>volsnap.sys</td>
<td>RUNNING</td>
<td></td>
<td></td>
<td></td>
<td>C:\WINDOWS\system32\DRIVERS\WMI\volsnap.sys</td>
</tr>
</tbody>
</table>
REPLICANTFARM

• Extend WP output to a signature based system: REPLICANTFARM

• Module based parser/alert system running on real-time CNE operational data

• Custom/module based analysis:
  – Actors
  – Implant technology
  – Host based signatures
  – Network based signatures
CCNE/Opsec WPID Alerts

Note that the search is done with the fields as perl regular expressions...

Examples:
- Dots (.) are single-character wildcards
- Dot-Star (*) means any number of characters
- Simple WPID: 518:1.1.3
- Class C WPID: 518:1
- Infrastructure (518)

Current Modules:
- mod_1000_VO_Implant.pl
- mod_1000_MM_SHEEPHERD.pl
- mod_101_MM_CARBON.pl
- mod_102_MM_REGBACKUP.pl
- mod_103_MM_DOGHOUSE.pl
- mod_104_MM_WALKER.pl
- mod_1100_VO_Implant.pl
- mod_11_cleocad.pl
- mod_12uracionepl.pl
- mod_13_rapmonitor.pl
- mod_14_strangedllextensions.pl
- mod_15ProcParents.pl
- mod_16_recyclerssec.pl
- mod_17_reggsec.pl
- mod_18_passwwordfilter.pl
- mod_19_formskelcoding.pl
- mod_20_planned.pl
- mod_21_scheduletest.pl
- mod_22_moduleinstaller.pl
- mod_23_hidden.pl
- mod_24_expectedArguments.pl
- mod_25_privileges.pl
- mod_26_STJURV32.pl
- mod_27_scheduledtask.pl
- mod_28_moduleinstaller.pl
- mod_29_UNK_CYDOLL.pl
- mod_304_UNK_WINPACP.pl
- mod_305_UNK_IASEX.pl
- mod_306_UNK_WINUPDATE.pl
- mod_307_UNK_WINVEROSQUAB.pl
- mod_308_UNK_WINDO.pl
- mod_309_UNK_DIELERATTLE.pl
- mod_310_UNK_WIDOWKEY.pl
- mod_311_UNK_CIVETCAT.pl
- mod_3客气假.pl
- mod_491_858LINN.pl
- mod_492_858TERNAL.pl

WPID Regexp: .................................................
Module Regexp: MM ...........................................
Types
Historic: ..........................
Live: ..........................

Submit Query:

ALERTS

WPID: ...
Module: mod_103_MM_DOGHOUSE.pl
Date: 2010-01-21T15:36:39.968
Tag: MM
File name: /datastore/archive/2010/01/21/15/TXID0000272485_18_Y201001D21_H15M28S59_MS642MU500NS0_RX1D050_000_0

Details:
Possible MM DOGHOUSE driver file: C:\WINNT\NtUninstallQ44598$.
Possible MM DOGHOUSE driver file: C:\WINNT\NtUninstallQ44598$\afcl.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\NtUninstallQ44598$\netbt.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\NtUninstallQ44598$\tcpip.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\NtUninstallQ44598$\hotfix.inf.

-----PULLEDPOK----
REPLICANTFARM generic modules

• Cloaked
• Recycler
• Rar password
• Tmp executable
• Packed
• Peb modification
• Privileges
• MS pretender
• System32 “variables”
• Strange DLL extensions

• Kernel cloaking
• Schedule at
• Ntuninstall execution
• hidden

Other ideas…. 
my @runningProcs = xml_isProcessRunning( $xml, 'svchost.{1,3}\.exe',
    'winlogon.{1,3}\.exe',
    'services.{1,3}\.exe',
    'lsass.{1,3}\.exe',
    'spoolsv.{1,3}\.exe',
    'autochk.{1,3}\.exe',
    'logon.{1,3}\.scr',
    'rundll32.{1,3}\.exe',
    'chkdsk.{1,3}\.exe',
    'chkntfs.{1,3}\.exe',
    'logonui.{1,3}\.exe',
    'ntoskrnl.{1,3}\.exe',
    'ntvdm.{1,3}\.exe',
    'rdpclip.{1,3}\.exe',
    'taskmgr.{1,3}\.exe',
    'userinit.{1,3}\.exe',
    'wsceiptf.{1,3}\.exe',
    'tcpmon.{1,3}\.dll' );

foreach my $runningProc (@runningProcs)
{
    $alertText .= "Suspicious process detected, legitimate exe named appended with string: ". $runningProc . ".\n";
}
RF specific signatures

• KNOWN actor filenames, processes, covert stores:
  – MAKERSMARK / FANNER
  – SEEDSPHERE / BYZANTINE
  – ALOOFNESS
  – SNOWGLOBE
  – VOYEUR
  – SUPERDRAKE
  – GOSSIPGIRL

• Infrastructure
  – Known IP addresses
  – Known DNS queries

• Other tools
Specific signatures : example

# Check a known drivers present
my @driversPresent = xml_isDriverPresent( $xml, 'usbdev\sys', 'acpimem32\sys',
                             'usblink32\exe', '\$NtUninstallQ722833\$' );

foreach my $driver (@driversPresent)
{
    $alertText .= "Possible MM CARBON driver detected: ". $driver . ".\n";
}
Operations

• Routine operations for CCNE investigations on current targets
  – Execution of OPSEC related plugins
  – Collection of files
  – Examination of network activity

• Blanket approvals for addition of selectors to level 4 OPs against known actors: example WATERMARK operations against MAKERSMARK

• Standard operating procedures for level 2 – level 4 operations against foreign CCNE actor infrastructures
CCNE / OPSEC page on 5-Eyes K1SVN Wiki

- Contains reverse engineering reports for CNE / IO consumption

- Even logs and notes for several actors
CCNE operations – Covert Infrastructure

• Some fusion of the WP and CCNE infrastructures
  – Dedicated ORB for CCNE
  – Unattributed dialups to the ORB

• Philosophy: use low hanging fruits against the actors (public exploits and tools if available)

• Discussions regarding repurpose of foreign toolkits

• De-confliction
SNOWGLOBE

• Provide the historical account of the activity on DOURMAGNUM (Imam Hussein University)

• Implant identified while investigating another unattributed actor

• rar archiving of emails on target

• Beaconving using HTTP to php-based listening post
SNOWGLOBE on target

Possible SNOWGLOBE CHOCOPOP process detected:

cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplockless -aprfeghhi -tn1d temp\168.rar c:\MDAEMON\Users\ihu.ac.ir\rfeghhi\md5*.msg">nul.
SNOWGLOBE implant

- Injects itself in svchost.exe
- No cloaking / no hooking
- Bootstraps in service called MSDTC64 (distributed transaction coordinator 64b)
- Service entry is permanent
- Executable kept on disk in system32
- Crypto: 16 byte string XOR
- http beacons and tasking
- Actor observed upgrading on target
SNOWGLOBE activity and attribution

- Targeting is scarce but resembles CT / CP priorities
- French localisation seen in exploit PDFs (GCHQ)
- French commentary in the binary
- French binary name / developer path
- Observed in Iran, Norway, Greece, Belgium, Algeria, France, US targets
- Listening posts worldwide – several French legit sites

- Now seen in passive collection, several reports
De-confliction: on CCNE operations

- State-sponsored landscape is very busy
- CCNE Targets are de-conflicted
- Actors on CCNE targets are not
- Covert nature of foreign (and friendly actors) make de-confliction challenging
- Often need to refer to precise technology for identification
- CNE/CCNE from SIGINT + HUMINT need to get together on this issue
De-confliction FAIL

- Actor discovered
- 5 eyes effort
- Several cohabitations
- At CSEC: 400 man-hours:
  - Over 20 CNE Operations
  - Passive Collection
  - 4 Reports
  - Reverse engineering
  - Planning of active operations
Conclusion

• CCNE effort essential to the national cyber mandate:
  – CNE situational awareness
  – New actor discovery
  – Tracking known actors

• Several new actors discovered using this process

• De-confliction needs to be improved
MM CCNE contacts