



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

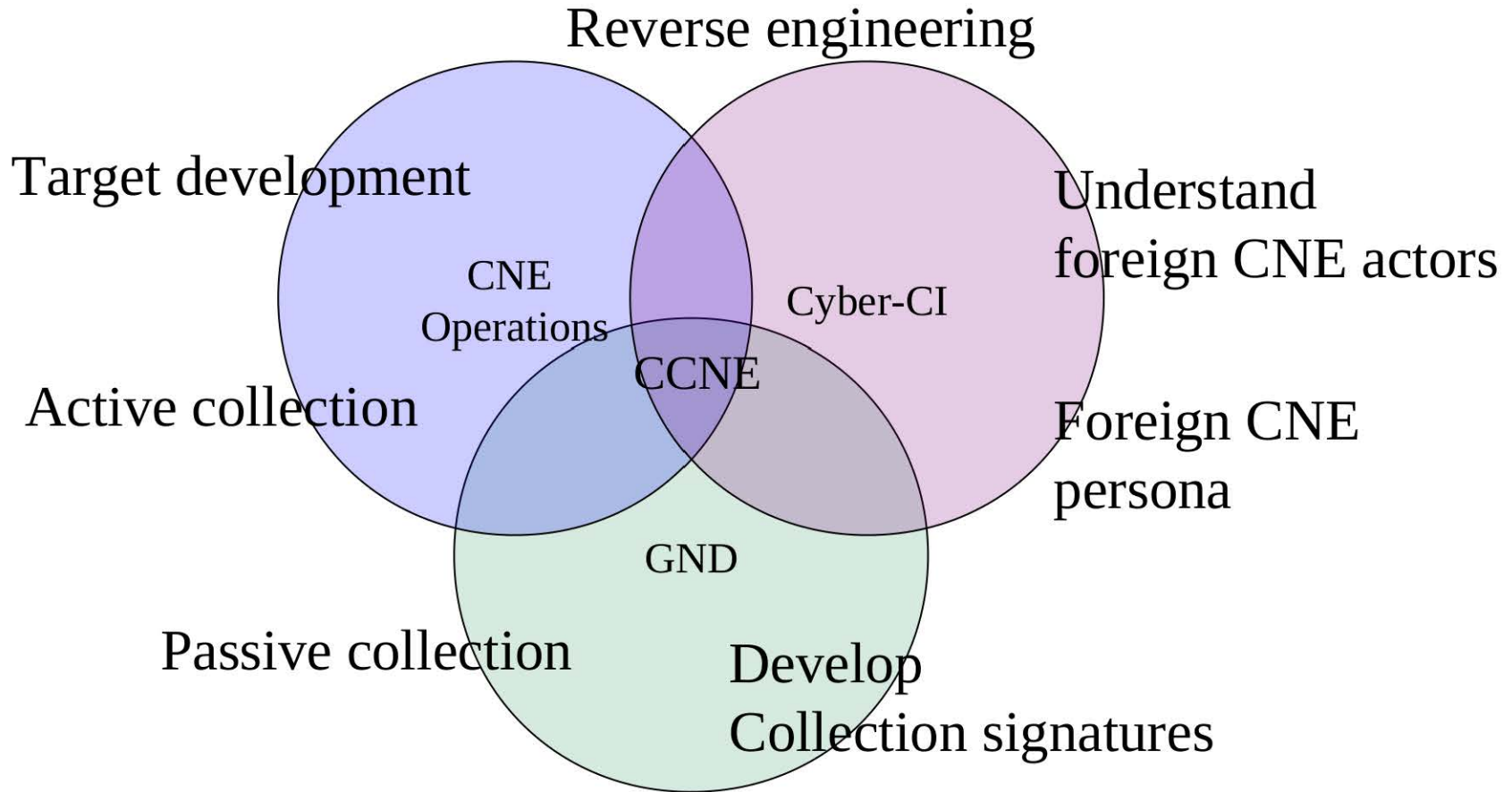


CCNE Group at CSEC

- 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





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

```

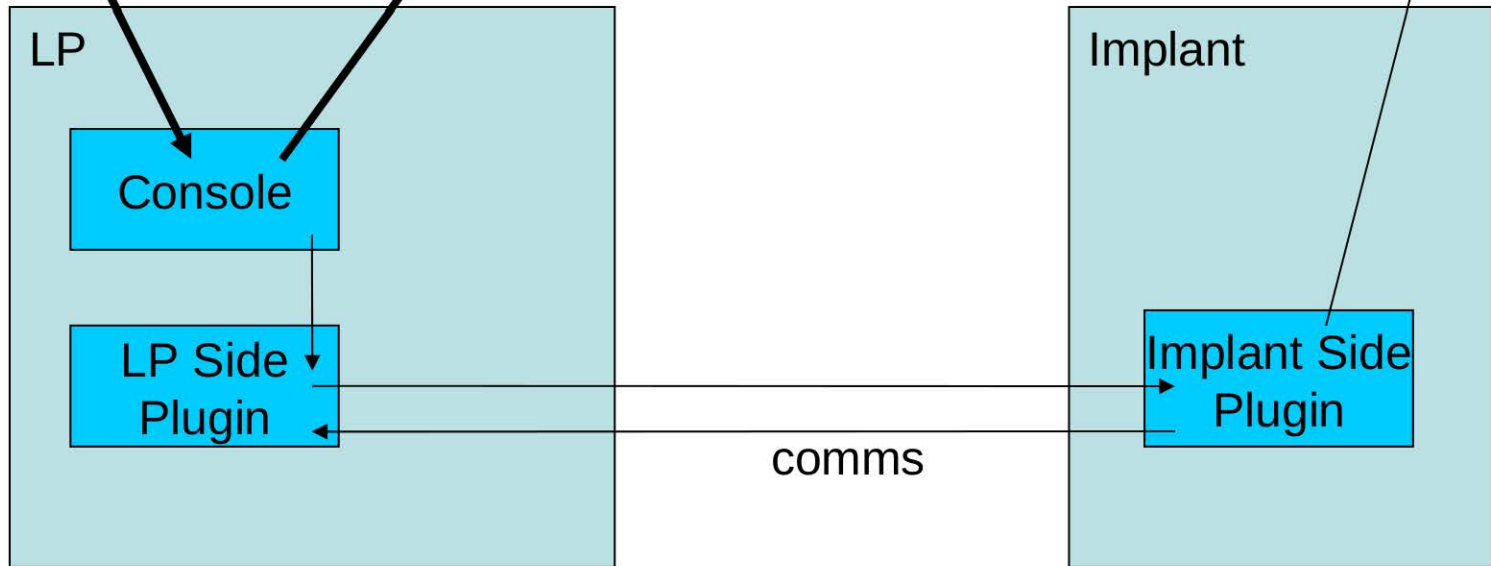
Command Prompt - U_Base x
pink:localhost> clistpeer
pink:localhost> rtlist
pink:localhost> sllistplugin
pink:localhost> ?
pink:localhost> sllistpersistent
pink:localhost> slliststore
pink:localhost> cgetimplantid
pink:localhost>

```

```

Output
Transaction Id: 138546
Core storage files for implant 127.0.0.1
=====
Plugin Store:  c:\Temp\~DF3BE9.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



WP xml output (raw)

```
<?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>
```



WP SLIPSTREAM output (parsed)

[2010/05/18 - 16:28:05 (UTC)] Transaction Id: 582966

U_SLIPSTREAM - <ssservices>

ImplantId: <51.8.1.13>

Timestamp (UTC): 2010/02/09 06:42:42

PAGE : 1 of 1

PID	Service Name	Status	Startup Type	Service Process Type	Display Name	Binary Path
924	AeLookupSvc C:\WINDOWS\system32\svchost.exe -k netsvcs	RUNNING	AUTOMATIC	SHARED	Application Experience Lookup Service	
0	Alerter LocalService	STOPPED	DISABLED	SHARED	Alerter	C:\WINDOWS\system32\svchost.exe -k
3184	ALG C:\WINDOWS\System32\alg.exe	RUNNING	MANUAL	OWN PROCESS	Application Layer Gateway Service	
0	AppMgmt -k netsvcs	STOPPED	MANUAL	SHARED	Application Management	C:\WINDOWS\system32\svchost.exe
924	AudioSrv -k netsvcs	RUNNING	AUTOMATIC	SHARED	Windows Audio	C:\WINDOWS\System32\svchost.exe
0	BITS C:\WINDOWS\system32\svchost.exe -k netsvcs	STOPPED	MANUAL	SHARED	Background Intelligent Transfer Service	
0	Browser -k netsvcs	STOPPED	AUTOMATIC	SHARED	Computer Browser	C:\WINDOWS\system32\svchost.exe
1028	ccEvtMgr Files\Symantec Shared\ccSvcHst.exe" /h ccCommon	RUNNING	AUTOMATIC	SHARED	Symantec Event Manager	"C:\Program Files\Common
1028	ccSetMgr Files\Symantec Shared\ccSvcHst.exe" /h ccCommon	RUNNING	AUTOMATIC	SHARED	Symantec Settings Manager	"C:\Program Files\Common
1708	Cissesrv Files\HP\Cissesrv\cissesrv.exe"	RUNNING	AUTOMATIC	OWN PROCESS	HP Smart Array SAS/SATA Event Notification Service	"C:\Program
0	CiSvc	STOPPED	DISABLED	SHARED	Indexing Service	C:\WINDOWS\system32\cisvc.exe
0	ClipSrv	STOPPED	DISABLED	OWN PROCESS	ClipBook	



WP SLIPSTREAM output... drivers (parsed)

[2010/05/18 - 16:28:06 (UTC)] Transaction Id: 582968
U_SLIPSTREAM - <ssdrivers>
ImplantId: <51.8.1.13>
Timestamp (UTC): 2010/02/09 06:42:43

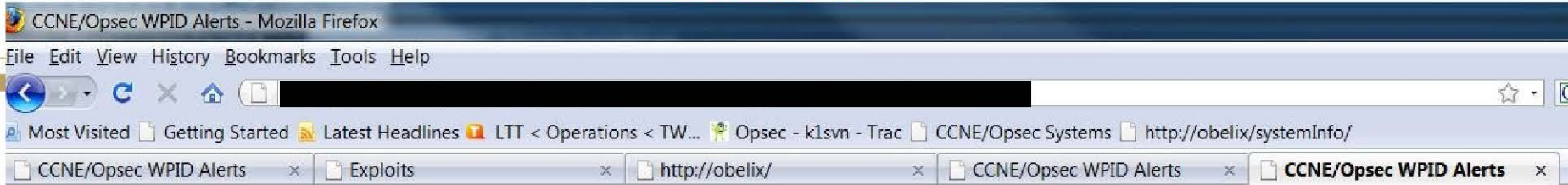
PAGE : 1 of 1

SCM\Driver Name	Status	Startup Type	Driver Type	Display Name	Binary Path
ntoskrnl.exe	RUNNING				C:\WINDOWS\system32\ntoskrnl.exe
hal.dll	RUNNING				C:\WINDOWS\system32\hal.dll
KDCOM.DLL	RUNNING				C:\WINDOWS\system32\KDCOM.DLL
BOOTVID.dll	RUNNING				C:\WINDOWS\system32\BOOTVID.dll
ACPI.sys	RUNNING				ACPI.sys
WMILIB.SYS	RUNNING				C:\WINDOWS\system32\DRIVERS\WMILIB.SYS
pci.sys	RUNNING				pci.sys
isapnp.sys	RUNNING				isapnp.sys
pciide.sys	RUNNING				pciide.sys
PCIINDEX.SYS	RUNNING				C:\WINDOWS\system32\DRIVERS\PCIINDEX.SYS
MountMgr.sys	RUNNING				MountMgr.sys
ftdisk.sys	RUNNING				ftdisk.sys
dmload.sys	RUNNING				dmload.sys
dmio.sys	RUNNING				dmio.sys
volsnap.sys	RUNNING				volsnap.sys



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

REPLICANTFARM

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

Examples:	Current Modules:	mod_1100_VO_Implant.pl	mod_115_procParents.pl	mod_200_SD_MI20.pl	mod_24_expectedArguments.pl	mod_304_UNK_WINPACP.pl	mod_310_UNK_WIDOWKEY.pl
<ul style="list-style-type: none"> Dots (.) are single-character wildcards Dot-Star (.*) means any number of characters Single WPID: 51\.\8\1\13 Class C WPID: 51\.\8\1\. Infrastructure: ^50\. 	mod_1000_WH_Implant.pl mod_100_MM_SHEPHERD.pl mod_101_MM_CARBON.pl mod_102_MM_REGBACKUP.pl mod_103_MM_DOGHOUSE.pl mod_104_MM_WALKER.pl	mod_111_cloaked.pl mod_1200_AF_ALOOFNESS.pl mod_12_system32var.pl mod_13_rarpasword.pl mod_14_strangedllextensions.pl	mod_16_recycleexec.pl mod_17_tmpexec.pl mod_18_passwordfilters.pl mod_19_kernelcloaking.pl mod_1_packed.pl	mod_201_SD_MI25FTP.pl mod_20_pebmodification.pl mod_21_scheduleat.pl mod_22_ntuninstallexec.pl mod_23_hidden.pl	mod_25_privileges.pl mod_300_UNK_TCP3RV32.pl mod_301_UNK_BLAZINGANGEL.pl mod_302_TINYWEB.pl mod_303_UNK_CYDLL.pl	mod_305_UNK_IASEX.pl mod_306_UNK_WINUPDATE.pl mod_307_UNK_QUIVERINGSQUAB.pl mod_308_UNK_WINDO.pl mod_309_UNK_DIESELRATTLE.pl	mod_311_UNK_CIVETCAT.pl mod_3_mspretender.pl mod_400_SS_WINBEE.pl mod_401_SS_SSLINST.pl mod_402_SS_SharpR.pl

WPID Regexp:

Module Regexp:

Type: 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_Y2010M01D21_H15M28S59_MS642MU500NS0_RXID050_000_0
Details:				
Possible MM DOGHOUSE driver file: C:\WINNT\%NtUninstallQ244598\$.				
Possible MM DOGHOUSE driver file: C:\WINNT\%NtUninstallQ244598\$\afd.sys.				
Possible MM DOGHOUSE driver file: C:\WINNT\%NtUninstallQ244598\$\netbt.sys.				
Possible MM DOGHOUSE driver file: C:\WINNT\%NtUninstallQ244598\$\tcpip.sys.				
Possible MM DOGHOUSE driver file: C:\WINNT\%NtUninstallQ244598\$\hotfix.inf.				
--PULLEDPORK--				



CCNE/Opsec Mondumptracker viewer

Note that the search is done on the wpids with a simple wildcard and a perl regex for the command lines...

Example:

- A value of * in a wpid indicates that "class" is a wildcard.
- Single WPID: 51.8.1.13
- Class B WPID: 51.1.*.*
- Class C WPID: 51.8.1.*
- The *-Regex is a perl regular expression applied to the command line. Only command lines satisfying the expression will be displayed.
- The !-Regex is a perl regular expression applied to the command line. Only command lines NOT satisfying the expression will be displayed.

WPID Regex: 51.8.1.13
 Date from: -2 months
 Date to:
 -Regex:
 !Regex:
 Group:
 Submit Query

proc	cmdLine	parent	wpid	lastSeen
msf6dosync.exe	C:\WINDOWS\system32\msf6dosync.exe sync	&{unknown_omn}		2010-05-24 12:13
dwfhwid.exe	"C:\Program Files\Symantec\Symantec Endpoint Protection\DWHW\id.exe"	&{unknown_omn}		2010-05-24 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{812CD25E-1049-4086-9DDD-A4FAE649FBDF}	&{unknown_omn}		2010-05-24 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{E5A3EBEE-D580-421e-86DF-54C0B3739522}	&{unknown_omn}		2010-05-24 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{D3769926-05B7-4ad1-9DCF-23051EBE78E3}	&{unknown_omn}		2010-05-24 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{C60DC234-65F9-4674-94AE-62158EFC433}	&{unknown_omn}		2010-05-24 04:05
lucoms-1.exe	"C:\PROGRA~1\Symantec LIVEUP~1\LUCOMS~1.EXE"	&{unknown_omn}		2010-05-24 04:05
luall.exe	"C:\Program Files\Symantec LiveUpdate\luall.exe" -S	&{unknown_omn}		2010-05-24 04:05
secclu.exe	"C:\Program Files\Symantec\Symantec Endpoint Protection\SecLU.exe" -Embedding	&{unknown_omn}		2010-05-24 04:04
wmiprvse.exe	C:\WINDOWS\system32\wbem\wmiprvse.exe -secured -Embedding	&{unknown_omn}		2010-05-24 02:10
helpsvc.exe	"C:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpSvc.exe" /Embedding	&{unknown_omn}		2010-05-24 02:10
accountprune.exe	"C:\MDaemon\APP\AccountPrune.exe" ;/d=1 /s="C:\MDaemon\Logs\OldLogs\Logs-2010-05-22-Sat-00-00-20.zip" ;p="C:\MDaemon\Logs" ;r	&{unknown_omn}		2010-05-23 19:32
sa-learn.exe	"C:\MDaemon\SpamAssassin\sa-learn.exe" --ham --configpath="C:\MDaemon\APP\SpamAssassin\default_rules" --siteconfigpath="C:\MDaemon\SpamAssassin\rules" --dir "C:\MDaemon\PUBLIC~1\BAYESI~1\IMA\NON-SP~1\IMA* .msg"	&{unknown_omn}		2010-05-23 19:30
accountprune.exe	"C:\MDaemon\APP\AccountPrune.exe" ;a	&{unknown_omn}		2010-05-23 19:30
listprune.exe	"C:\MDaemon\APP>ListPrune.exe" ;s	&{unknown_omn}		2010-05-23 19:30
sa-learn.exe	"C:\MDaemon\SpamAssassin\sa-learn.exe" --spam --configpath="C:\MDaemon\APP\SpamAssassin\default_rules" --siteconfigpath="C:\MDaemon\SpamAssassin\rules" --dir "C:\MDaemon\PUBLIC~1\BAYESI~1\IMA\SPAM~1\IMA* .msg"	&{unknown_omn}		2010-05-23 19:30
mdupdate.exe	"C:\MDaemon\APP\MDUpdater.exe" ;p="C:\MDaemon\Server" ;s	&{unknown_omn}		2010-05-23 19:30
cmd.exe	"C:\WINDOWS\system32\cmd.exe" ;c "C:\MDaemon\APP\Learn.bat"	&{unknown_omn}		2010-05-23 19:30
cmd.exe	"C:\WINDOWS\system32\cmd.exe" ;c "C:\MDaemon\APP\Cleanup.bat"	&{unknown_omn}		2010-05-23 19:30
avupdate.exe	"C:\MDaemon\SecurityPlus\avupdate.exe" ;q ;n	&{unknown_omn}		2010-05-23 14:21
rundll32.exe	C:\WINDOWS\system32\rundll32.exe C:\DOCUME~1\ALLUSE~1\WINAPPLIC~1\Symantec\SyKnApp5\SyKnApp5.dll, UpdateSyKnApp5	&{unknown_omn}		2010-05-23 04:05
accountprune.exe	"C:\MDaemon\APP\AccountPrune.exe" ;/d=1 /s="C:\MDaemon\Logs\OldLogs\Logs-2010-05-21-Fri-00-00-03.zip" ;p="C:\MDaemon\Logs" ;r	&{unknown_omn}		2010-05-22 19:32
msf6dosync.exe	C:\WINDOWS\system32\msf6dosync.exe sync	&{unknown_omn}		2010-05-22 08:16
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{812CD25E-1049-4086-9DDD-A4FAE649FBDF}	&{unknown_omn}		2010-05-22 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{E5A3EBEE-D580-421e-86DF-54C0B3739522}	&{unknown_omn}		2010-05-22 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{D3769926-05B7-4ad1-9DCF-23051EBE78E3}	&{unknown_omn}		2010-05-22 04:05
lucallbackproxy	"C:\Program Files\Symantec LiveUpdate\LuCallbackProxy.exe" ;{C60DC234-65F9-4674-94AE-62158EFC433}	&{unknown_omn}		2010-05-22 04:05
lucoms-1.exe	"C:\PROGRA~1\Symantec LIVEUP~1\LUCOMS~1.EXE"	&{unknown_omn}		2010-05-22 04:05
luall.exe	"C:\Program Files\Symantec LiveUpdate\luall.exe" -S	&{unknown_omn}		2010-05-22 04:05



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....



Generic modules : example

```
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',  
        'wscntfy.{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( $xml, 'usbdev\\\.sys', 'acpimem32\\\.sys',  
    'usblink32i\\\.exe', '\\$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
- Beaconing using HTTP to php-based listening post



CCNE/Opsec WPID Alerts - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Most Visited Getting Started Latest Headlines LTT < Operations < TW... Opsec - k1svn - Trac CCNE/Opsec Systems http://obelix/systemInfo/

http://obelix/ CCNE/Opsec WPID Alerts CCNE/Opsec WPID Alerts Opsec - k1svn Opsec - k1svn

CCNE/Opsec WPID Alerts

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

Examples:	<ul style="list-style-type: none"> Dots (.) are single-character wildcards Dot-Star (*) means any number of characters Single WPID: 511.8.10.13 Class C WPID: 511.8.10. Infrastructure: <501. 	Current Modules: mod_1000_WH_Implant.pl mod_100_MM_SHEPHERD.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_cloaked.pl mod_1200_AF_ALOOFNESS.pl mod_12_system32var.pl mod_13_rpassword.pl mod_14_stranged1extensions.pl	mod_15_procParents.pl mod_16_recyclerec.pl mod_17_tmpexec.pl mod_18_passwordfilters.pl mod_19_kernelcloning.pl mod_1_packed.pl	mod_200_SD_MID20.pl mod_201_SD_MID25FTP.pl mod_20_pdbmodification.pl mod_21_scheduler.pl mod_22_rnminstallexec.pl mod_23_hidden.pl	mod_24_expectedArguments.pl mod_25_privileges.pl mod_300_UNK_TCPSRV32.pl mod_301_UNK_BLAZINGANGEL.pl mod_302_TINYWEB.pl mod_303_UNK_CYDLL.pl	mod_304_UNK_WINPACP.pl mod_305_UNK_IASEX.pl mod_306_UNK_WINUPDATE.pl mod_307_UNK_QUIVERINGSQUAB.pl mod_308_UNK_WINDO.pl mod_309_UNK_DIESELRAATTLE.pl	mod_310_UNK_WIDOWKEY.pl mod_311_UNK_CIVETCAT.pl mod_3_mspretender.pl mod_400_SS_WINBEE.pl mod_401_SS_SSLINST.pl mod_402_SS_SharpR.pl	mod_500_SJ_DDNT.pl mod_5_knownmips.pl mod_500_GR_IMPLANT.pl mod_601_GR_FLAME.pl mod_6_knownvids.pl mod_700_SG_CHOCOPOP.pl	mod_7_err mod_8001 mod_9001 mod_RFI mod_RFI
------------------	---	--	--	---	---	---	---	---	--	---

WPID Regexp: Module Regexp:

Type: Historic: Live:

Submit Query

ALERTS

WPID: [REDACTED]	Module: mod_700_SG_CHOCOPOP.pl	Date: 2009-09-30T10:18:41.906	Tag: SG	File name: .../datastore/archive/2009/09/30/10/TXID0000074573_18_Y2009M09D30_H10M1
-------------------------	---------------------------------------	--------------------------------------	----------------	---

Details:

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -aprfeghhi -tn1d temp\168.rar c:\MDAEMON\Users\ihu.a

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -aprfeghhi -tn1d temp\168.rar c:\MDAEMON\Users\ihu.a

Possible SNOWGLOBE CHOCOPOP process detected: "c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apSNazarian -tn1d C:\WINDOWS\TEMP\166.rar c:\MDAEMON\U

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apSNazarian -tn1d temp\166.rar c:\MDAEMON\Users\ih

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apSNazarian -tn1d temp\166.rar c:\MDAEMON\Users\ih

Possible SNOWGLOBE CHOCOPOP process detected: "c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apkpnazari -tn1d C:\WINDOWS\TEMP\166.rar c:\MDAEMON\User

Possible SNOWGLOBE CHOCOPOP process detected: "c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apkpnazari -tn1d C:\WINDOWS\TEMP\166.rar c:\MDAEMON\User

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apkpnazari -tn1d temp\166.rar c:\MDAEMON\Users\ihu.

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apkpnazari -tn1d temp\166.rar c:\MDAEMON\Users\ihu.

Possible SNOWGLOBE CHOCOPOP process detected: "c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apmsaadati -tn1d C:\WINDOWS\TEMP\166.rar c:\MDAEMON\User

Possible SNOWGLOBE CHOCOPOP process detected: "c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apmsaadati -tn1d C:\WINDOWS\TEMP\166.rar c:\MDAEMON\User

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apmsaadati -tn1d temp\166.rar c:\MDAEMON\Users\ihu

Possible SNOWGLOBE CHOCOPOP process detected: cmd.exe /C ""c:\RECYCLER\S-1-5-21-101796669-4102346875-220983236-500\rar.exe" a -r -inul -hplckless -apmsaadati -tn1d temp\166.rar c:\MDAEMON\Users\ihu

==DOURMAGNUM==



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  
-hplckless -aprfeghi -tn1d temp\168.rar  
c:\MDAEMON\Users\ihu.ac.ir\rfeghi\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



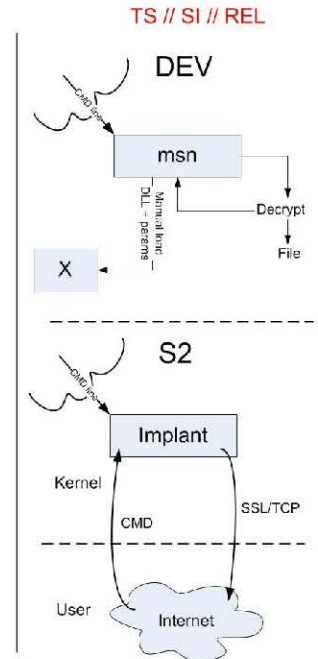
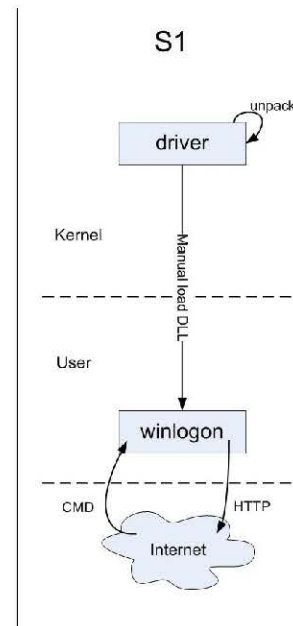
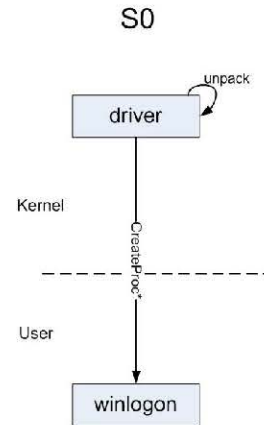
De-confliction : on CCNE operations

- 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

