MIRcon 2012

Finding Evil With Data Stacking

Nick Bennett & Jake Valletta
Mandiant

Agenda

- Who We Are
- Investigative Approach
- What is Stacking?
- Stacking Basics
- Case Studies - Finding Evil by Stacking
- Questions and Answers

Nick Bennett

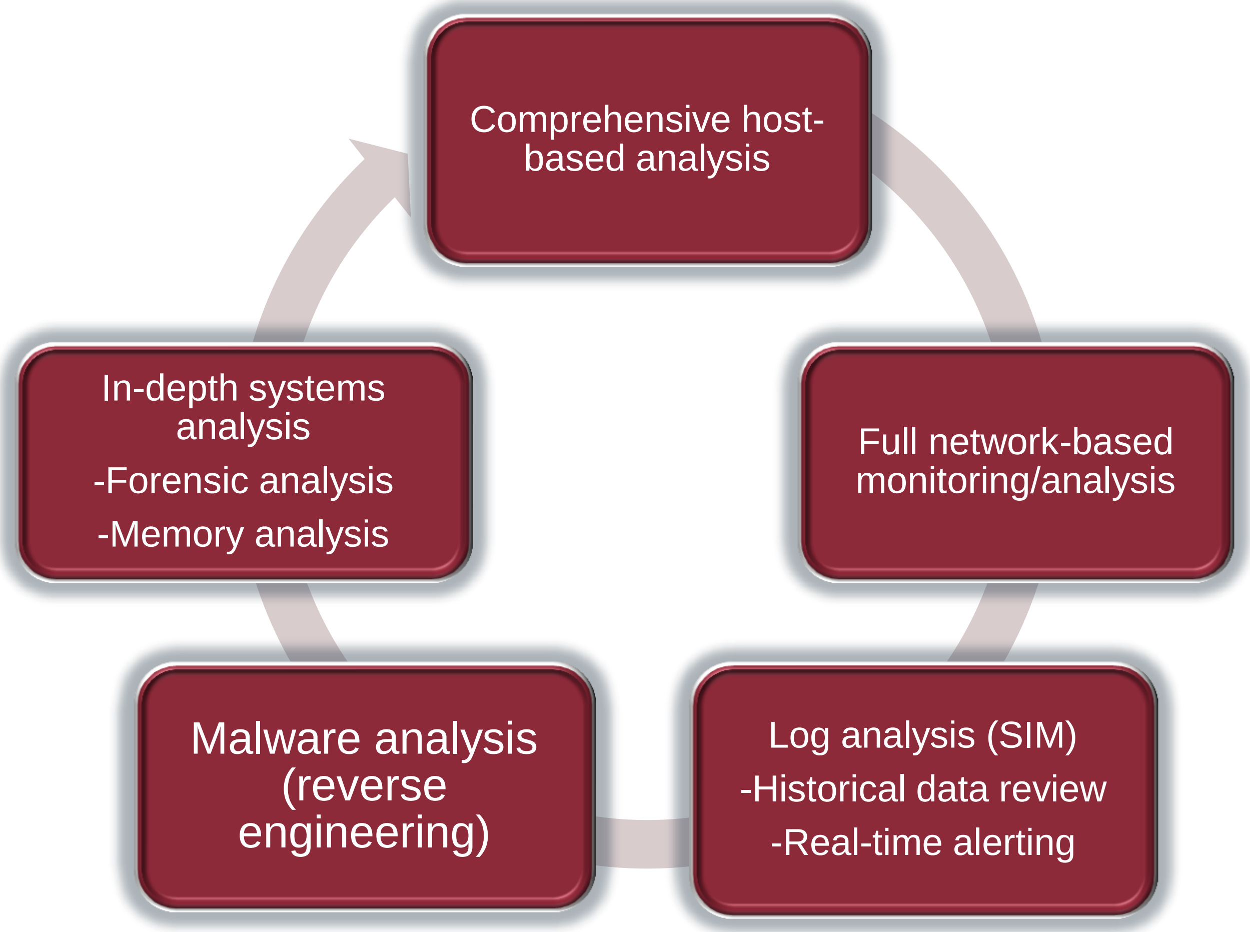
- Principal Consultant at Mandiant's NYC Office
- 7 Years experience in Information Security Field
- Application Penetration Testing, Forensics, & Incident Response
- nick.bennett@mandiant.com

Jake Valletta

- Associate Consultant at Mandiant’s NYC Office
- Mobile Security, App. Assessments, Penetration Testing, & Forensics
- Blog: http://thecobraden.blogspot.com
- @jake_valletta

INVESTIGATIVE APPROACH

Traditional Incident Investigative Approach



Comprehensive host-based analysis

Full network-based monitoring/analysis

Log analysis (SIM)

-Historical data review

-Real-time alerting

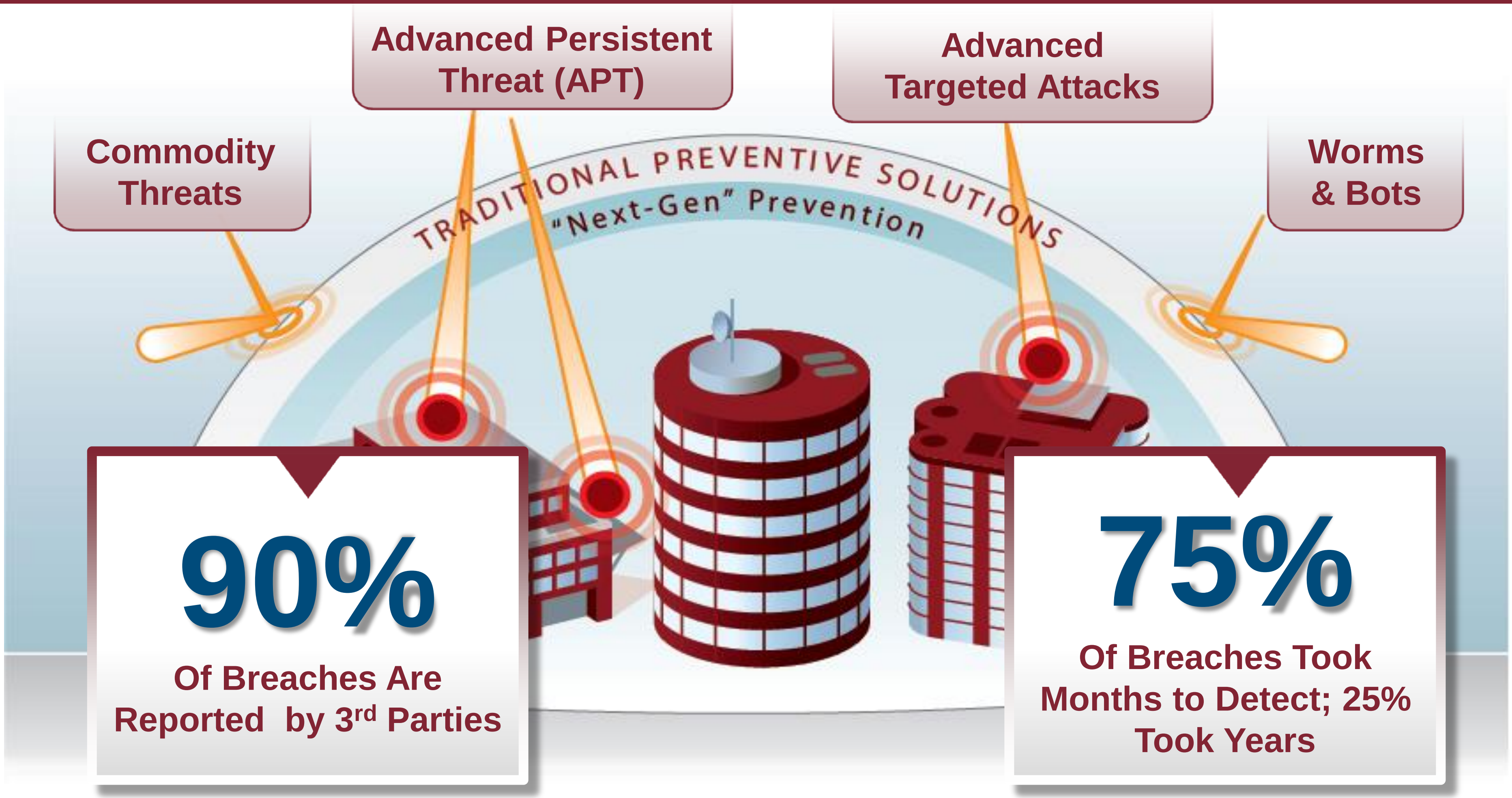
Malware analysis (reverse engineering)

In-depth systems analysis

-Forensic analysis

-Memory analysis

Detection Woes


Advanced Persistent Threat (APT)
Advanced Targeted Attacks
Commodity Threats
Worms & Bots
TRADITIONAL PREVENTIVE SOLUTIONS
"Next-Gen" Prevention

90%

Of Breaches Are Reported by 3rd Parties

75%

Of Breaches Took Months to Detect; 25% Took Years

Source: Mandiant

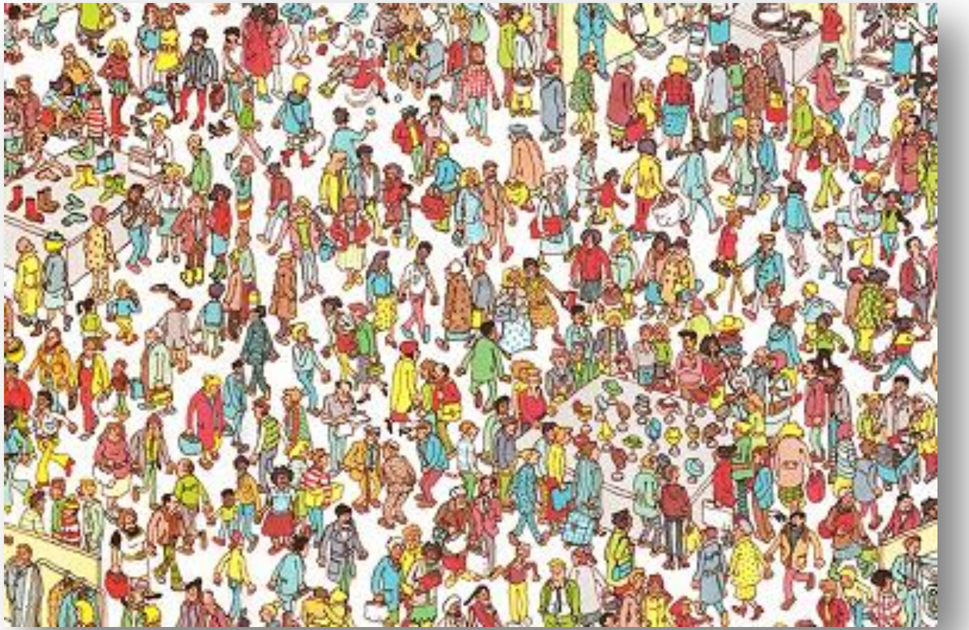
ENTER STACKING…

What is Stacking?

- Performing frequency analysis on large amounts of similar data in an attempt to isolate and identify anomalies and outliers

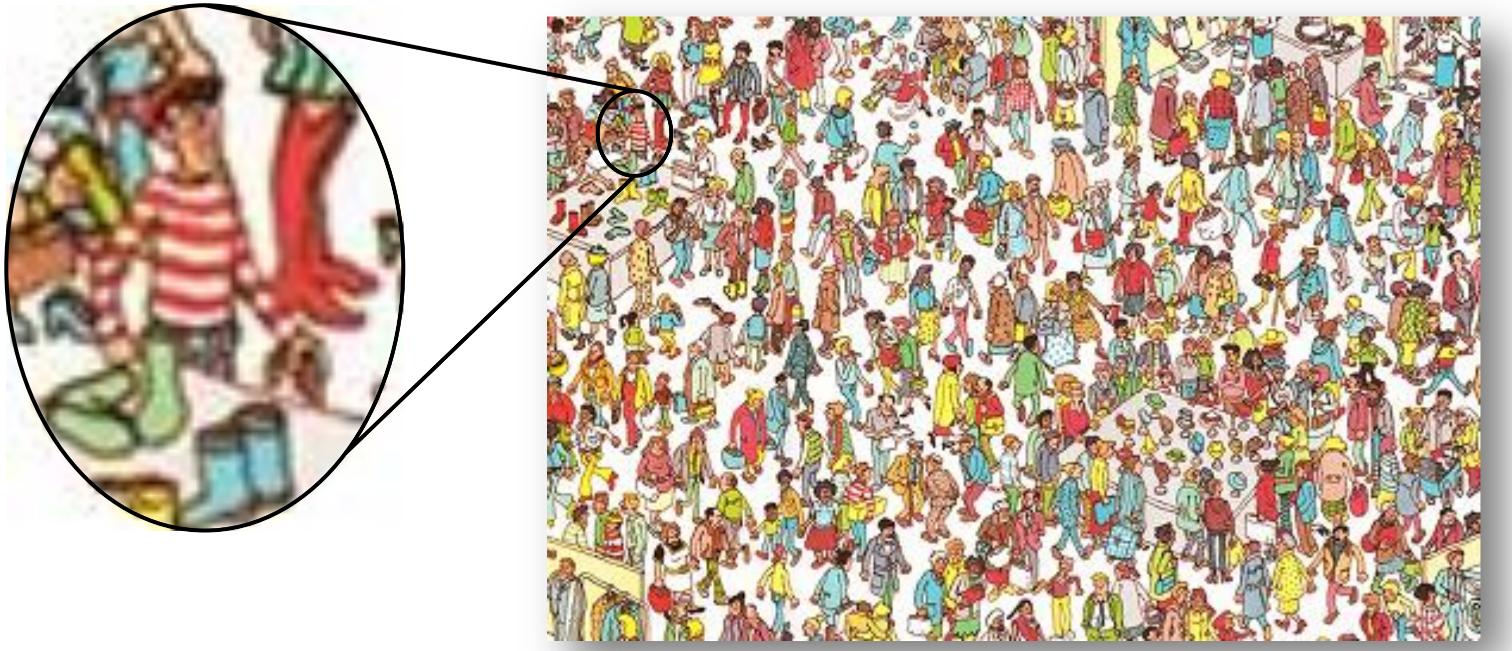
Stacking 101

- Start with a large data set
- Select attributes to group by
- Parse data and count instances of each possible grouping



Stacking 101

- Search for low occurrences or anomalies
- Manually verify to remove false positives



Known Limitations

- Data acquisition
- Potential for high false positives
  - Waldo example: Low occurrence of other outfits
- Potential for high false negatives
  - Waldo example: Several wearing red/white stripe shirts

STACKING BASICS – HOW ITS DONE

Pick Something to Stack

- Need to pick "ideal" stacking attributes
  - Something that is relatively unchanged
  - Must have an acquisition method
    - MIR!

Need a Strong Acquisition Method

- Commercial Solutions
  - Incident response tools, application metering, etc.
- "Home Grown"
  - Custom scripts, WMI, GPO, creativity
- Pros/Cons to both approaches

Pros and Cons – Commercial Tools

- Pros
  - Tried and tested
  - Multi-platform support
  - “Export data” feature
- Cons
  - Costs money!
  - Must be properly managed/maintained

Pros and Cons – Home Grown

- Pros
  - No software costs
  - No additional endpoint deployment
- Cons
  - Difficult to scale
  - Might not be easy to implement on all platforms
  - Not error free

Acquiring your Data with MIR

- Very easy to run audits and export data
- “Sweep” environment for plenty of test data
- Data in strict XML format (easy to parse)
  - Schemas are published at http://schemas.mandiant.com/

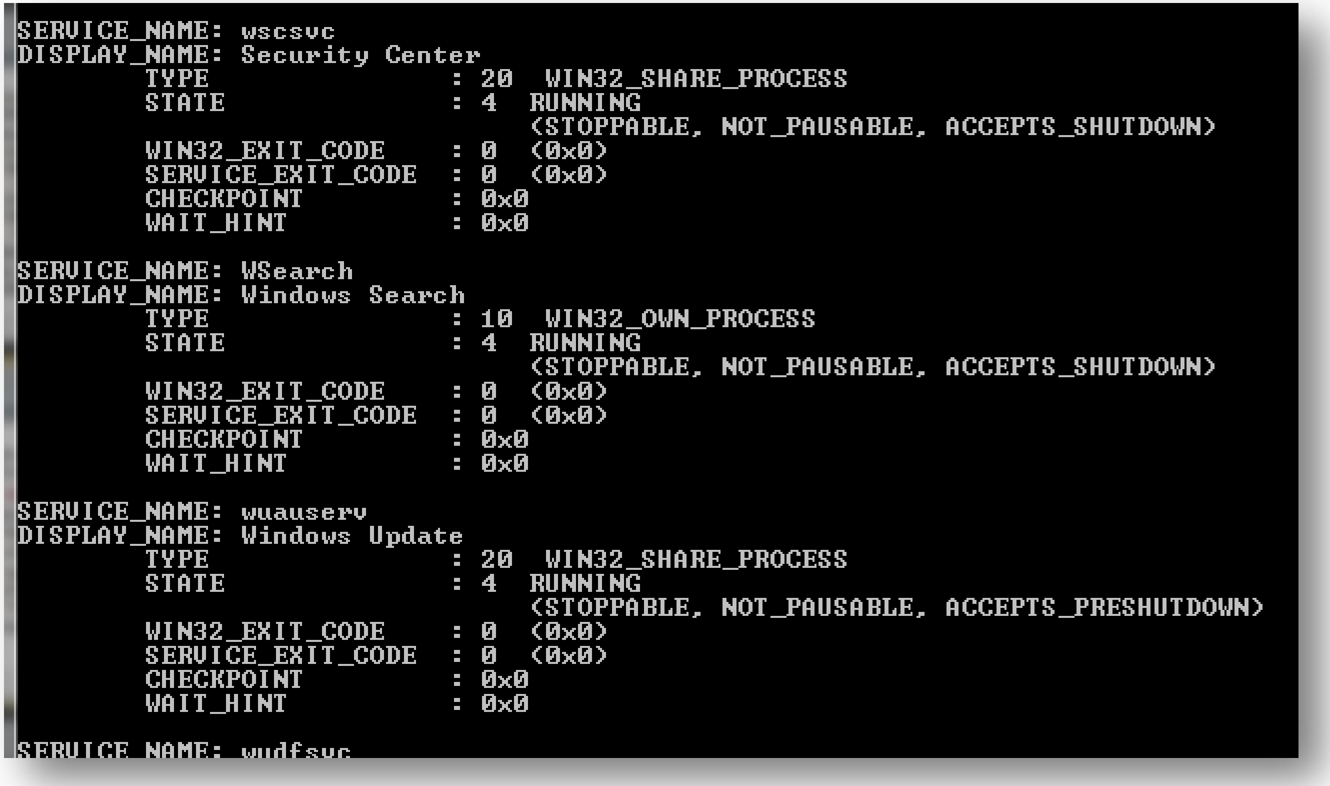
Parsing the Data

- Process is relatively similar for any data set
  - Create a script that ingests raw data, produces CSV with totals
  - Import CSV into Excel to sort and filter
- Much easier to perform when “data” is in standard format
  - XML, JSON

FINDING EVIL– EXAMPLES

Example – Service Stacking

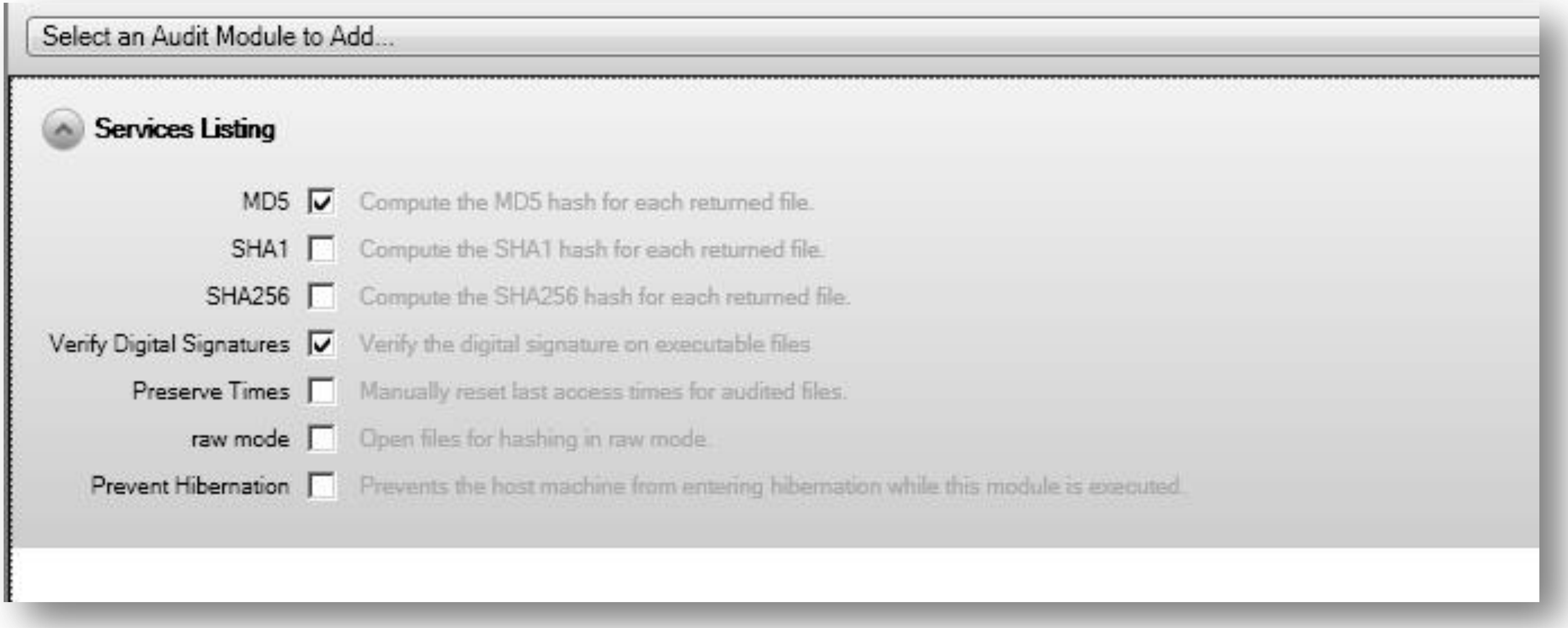
- Finding evil by stacking Windows Service’s metadata



```
SERVICE_NAME: wscsvc
DISPLAY_NAME: Security Center
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: WSearch
DISPLAY_NAME: Windows Search
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: wuauserv
DISPLAY_NAME: Windows Update
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: wudfsvc
```

Acquiring Service Data with MIR

- Create audit for “Services Listing”
  - MD5s, Digital Signatures



Select an Audit Module to Add...

Services Listing

MD5 ☑ Compute the MD5 hash for each returned file.

SHA1 □ Compute the SHA1 hash for each returned file.

SHA256 □ Compute the SHA256 hash for each returned file.

Verify Digital Signatures ☑ Verify the digital signature on executable files

Preserve Times □ Manually reset last access times for audited files.

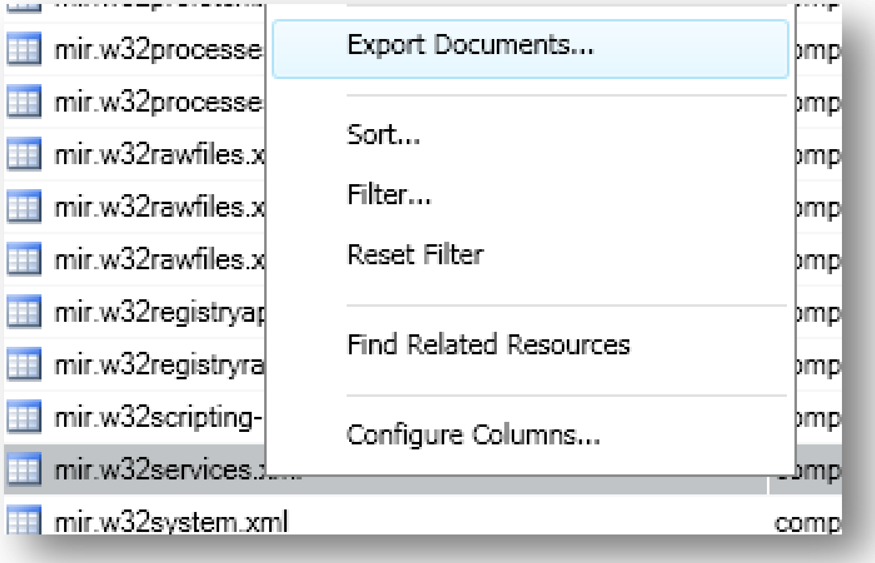
raw mode □ Open files for hashing in raw mode

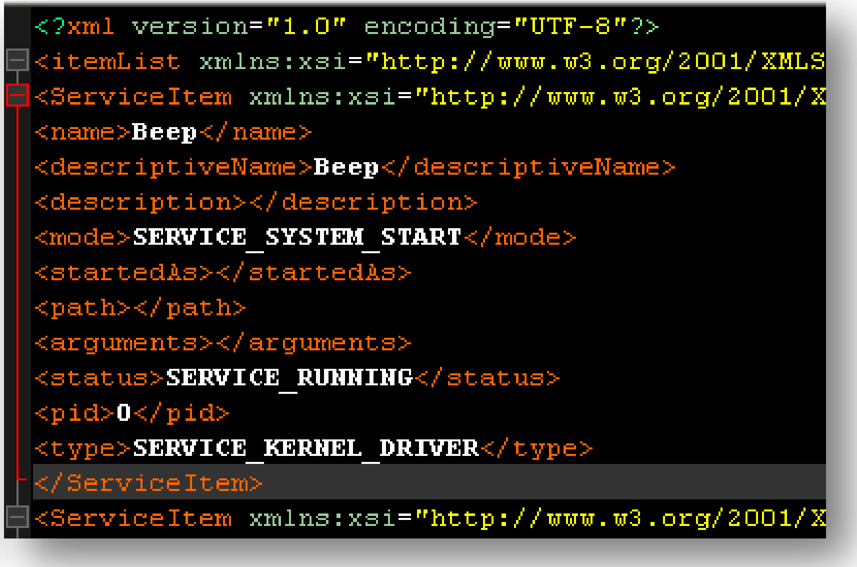
Prevent Hibernation □ Prevents the host machine from entering hibernation while this module is executed

MIRcon 2012

Exporting Data?

- Export single audit once completed
  - Exports as XML document
  - **Doesn’t Scale!!**



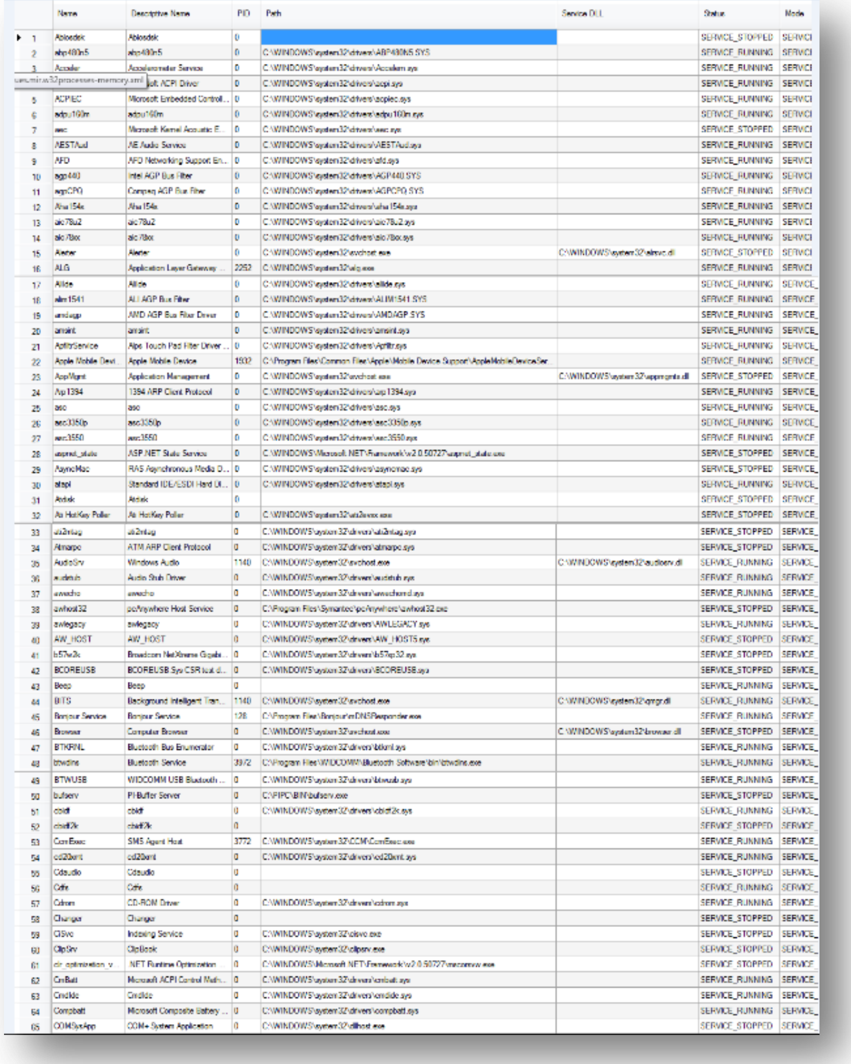


```
<?xml version="1.0" encoding="UTF-8"?>
<itemList xmlns:xsi="http://www.w3.org/2001/XMLS
<ServiceItem xmlns:xsi="http://www.w3.org/2001/X
<name>Beep</name>
<descriptiveName>Beep</descriptiveName>
<description></description>
<mode>SERVICE_SYSTEM_START</mode>
<startedAs></startedAs>
<path></path>
<arguments></arguments>
<status>SERVICE_RUNNING</status>
<pid>0</pid>
<type>SERVICE_KERNEL_DRIVER</type>
</ServiceItem>
<ServiceItem xmlns:xsi="http://www.w3.org/2001/X
```

Exporting Data

- New tool released **today** by Seth Summerset called "mir_export.py"
  - Available for free on the Mandiant forum
    - https://forums.mandiant.com/topic/mir_export-offline-audit-analysis
  - Allows for bulk export of audits

Reviewing Services is Easy?



	Name	Descriptive Name	PID	Path	Service DLL	Status	Mode
1	Abiosdsk	Abiosdsk	0			SERVICE_STOPPED	SERVICI
2	abp480n5	abp480n5	0	C:\WINDOWS\system32\drivers\ABP480N5.SYS		SERVICE_RUNNING	SERVICI
3	Accelerometer	Accelerometer Service	0	C:\WINDOWS\system32\drivers\Accelern.sys		SERVICE_RUNNING	SERVICI
4	...mir.w32processes-memory.xml	oft ACPI Driver	0	C:\WINDOWS\system32\drivers\acpi.sys		SERVICE_RUNNING	SERVICI
5	ACPIEC	Microsoft Embedded Controll...	0	C:\WINDOWS\system32\drivers\acpiec.sys		SERVICE_RUNNING	SERVICI
6	adpu160m	adpu160m	0	C:\WINDOWS\system32\drivers\adpu160m.sys		SERVICE_RUNNING	SERVICI
7	aec	Microsoft Kernel Acoustic E...	0	C:\WINDOWS\system32\drivers\aec.sys		SERVICE_STOPPED	SERVICI
8	AESTAud	AE Audio Service	0	C:\WINDOWS\system32\drivers\AESTAud.sys		SERVICE_RUNNING	SERVICI
9	AFD	AFD Networking Support En...	0	C:\WINDOWS\system32\drivers\afd.sys		SERVICE_RUNNING	SERVICI
10	agp440	Intel AGP Bus Filter	0	C:\WINDOWS\system32\drivers\AGP440.SYS		SERVICE_RUNNING	SERVICI
11	agpCPQ	Compaq AGP Bus Filter	0	C:\WINDOWS\system32\drivers\AGPCPQ.SYS		SERVICE_RUNNING	SERVICI
12	Aha154x	Aha154x	0	C:\WINDOWS\system32\drivers\aha154x.sys		SERVICE_RUNNING	SERVICI
13	aic78u2	aic78u2	0	C:\WINDOWS\system32\drivers\aic78u2.sys		SERVICE_RUNNING	SERVICI
14	aic78xx	aic78xx	0	C:\WINDOWS\system32\drivers\aic78xx.sys		SERVICE_RUNNING	SERVICI
15	Alerter	Alerter	0	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\system32\alrsvc.dll	SERVICE_STOPPED	SERVICI
16	ALG	Application Layer Gateway ...	2252	C:\WINDOWS\system32\alg.exe		SERVICE_RUNNING	SERVICI
17	Aliide	Aliide	0	C:\WINDOWS\system32\drivers\aliide.sys		SERVICE_RUNNING	SERVICE_
18	alim1541	ALI AGP Bus Filter	0	C:\WINDOWS\system32\drivers\ALIM1541.SYS		SERVICE_RUNNING	SERVICE_
19	amdagp	AMD AGP Bus Filter Driver	0	C:\WINDOWS\system32\drivers\AMDAGP.SYS		SERVICE_RUNNING	SERVICE_
20	amsint	amsint	0	C:\WINDOWS\system32\drivers\amsint.sys		SERVICE_RUNNING	SERVICE_
21	ApfiltrService	Alps Touch Pad Filter Driver ...	0	C:\WINDOWS\system32\drivers\Apfiltr.sys		SERVICE_RUNNING	SERVICE_
22	Apple Mobile Devi...	Apple Mobile Device	1932	C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceSer...		SERVICE_RUNNING	SERVICE_
23	AppMgmt	Application Management	0	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\system32\appmgmts.dll	SERVICE_STOPPED	SERVICE_
24	Arp1394	1394 ARP Client Protocol	0	C:\WINDOWS\system32\drivers\arp1394.sys		SERVICE_RUNNING	SERVICE_
25	asc	asc	0	C:\WINDOWS\system32\drivers\asc.sys		SERVICE_RUNNING	SERVICE_
26	asc3350p	asc3350p	0	C:\WINDOWS\system32\drivers\asc3350p.sys		SERVICE_RUNNING	SERVICE_
27	asc3550	asc3550	0	C:\WINDOWS\system32\drivers\asc3550.sys		SERVICE_RUNNING	SERVICE_
28	aspnet_state	ASP.NET State Service	0	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe		SERVICE_STOPPED	SERVICE_
29	AsyncMac	RAS Asynchronous Media D...	0	C:\WINDOWS\system32\drivers\asyncmac.sys		SERVICE_STOPPED	SERVICE_
30	atapi	Standard IDE/ESDI Hard Di...	0	C:\WINDOWS\system32\drivers\atapi.sys		SERVICE_RUNNING	SERVICE_
31	Atdisk	Atdisk	0			SERVICE_STOPPED	SERVICE_
32	Ati HotKey Poller	Ati HotKey Poller	0	C:\WINDOWS\system32\ati2evxx.exe		SERVICE_STOPPED	SERVICE_
33	ati2mtag	ati2mtag	0	C:\WINDOWS\system32\drivers\ati2mtag.sys		SERVICE_STOPPED	SERVICE_
34	Atmarpc	ATM ARP Client Protocol	0	C:\WINDOWS\system32\drivers\atmarpc.sys		SERVICE_STOPPED	SERVICE_
35	AudioSrv	Windows Audio	1140	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\system32\audiosrv.dll	SERVICE_RUNNING	SERVICE_
36	audstub	Audio Stub Driver	0	C:\WINDOWS\system32\drivers\audstub.sys		SERVICE_RUNNING	SERVICE_
37	awacho	awacho	0	C:\WINDOWS\system32\drivers\awachord.sys		SERVICE_RUNNING	SERVICE_
38	awhost32	pcAnywhere Host Service	0	C:\Program Files\Symantec\pcAnywhere\awhost32.exe		SERVICE_STOPPED	SERVICE_
39	awlegacy	awlegacy	0	C:\WINDOWS\system32\drivers\AWLEGACY.sys		SERVICE_RUNNING	SERVICE_
40	AW_HOST	AW_HOST	0	C:\WINDOWS\system32\drivers\AW_HOST5.sys		SERVICE_STOPPED	SERVICE_
41	b57w2k	Broadcom NetXtreme Gigabi...	0	C:\WINDOWS\system32\drivers\b57xp32.sys		SERVICE_STOPPED	SERVICE_
42	BCOREUSB	BCOREUSB Sys CSR test d...	0	C:\WINDOWS\system32\drivers\BCOREUSB.sys		SERVICE_STOPPED	SERVICE_
43	Beep	Beep	0			SERVICE_RUNNING	SERVICE_
44	BITS	Background Intelligent Tran...	1140	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\system32\qmgr.dll	SERVICE_RUNNING	SERVICE_
45	Bonjour Service	Bonjour Service	128	C:\Program Files\Bonjour\mDNSResponder.exe		SERVICE_RUNNING	SERVICE_
46	Browser	Computer Browser	0	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\system32\browser.dll	SERVICE_STOPPED	SERVICE_
47	BTKRNL	Bluetooth Bus Enumerator	0	C:\WINDOWS\system32\drivers\btkrnl.sys		SERVICE_RUNNING	SERVICE_
48	btwdins	Bluetooth Service	3972	C:\Program Files\WIDCOMM\Bluetooth Software\bin\btwdins.exe		SERVICE_RUNNING	SERVICE_
49	BTWUSB	WIDCOMM USB Bluetooth ...	0	C:\WINDOWS\system32\drivers\btwusb.sys		SERVICE_RUNNING	SERVICE_
50	bufserv	PI-Buffer Server	0	C:\PIPC\BIN\bufserv.exe		SERVICE_STOPPED	SERVICE_
51	cbidf	cbidf	0	C:\WINDOWS\system32\drivers\cbidf2k.sys		SERVICE_RUNNING	SERVICE_
52	cbidf2k	cbidf2k	0			SERVICE_STOPPED	SERVICE_
53	CcmExec	SMS Agent Host	3772	C:\WINDOWS\system32\CCM\CcmExec.exe		SERVICE_RUNNING	SERVICE_
54	cd20xrnt	cd20xrnt	0	C:\WINDOWS\system32\drivers\cd20xrnt.sys		SERVICE_RUNNING	SERVICE_
55	Cdaudio	Cdaudio	0			SERVICE_STOPPED	SERVICE_
56	Cdfs	Cdfs	0			SERVICE_RUNNING	SERVICE_
57	Cdrom	CD-ROM Driver	0	C:\WINDOWS\system32\drivers\cdrom.sys		SERVICE_RUNNING	SERVICE_
58	Changer	Changer	0			SERVICE_STOPPED	SERVICE_
59	CiSvc	Indexing Service	0	C:\WINDOWS\system32\cisvc.exe		SERVICE_STOPPED	SERVICE_
60	ClipSrv	ClipBook	0	C:\WINDOWS\system32\clipsrv.exe		SERVICE_STOPPED	SERVICE_
61	clr_optimization_v...	.NET Runtime Optimization ...	0	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe		SERVICE_STOPPED	SERVICE_
62	CmBatt	Microsoft ACPI Control Meth...	0	C:\WINDOWS\system32\drivers\cmbatt.sys		SERVICE_RUNNING	SERVICE_
63	Cmdide	Cmdide	0	C:\WINDOWS\system32\drivers\cmdide.sys		SERVICE_RUNNING	SERVICE_
64	Compbatt	Microsoft Composite Battery ...	0	C:\WINDOWS\system32\drivers\compbatt.sys		SERVICE_RUNNING	SERVICE_
65	COMSysApp	COM+ System Application	0	C:\WINDOWS\system32\dllhost.exe		SERVICE_STOPPED	SERVICE_

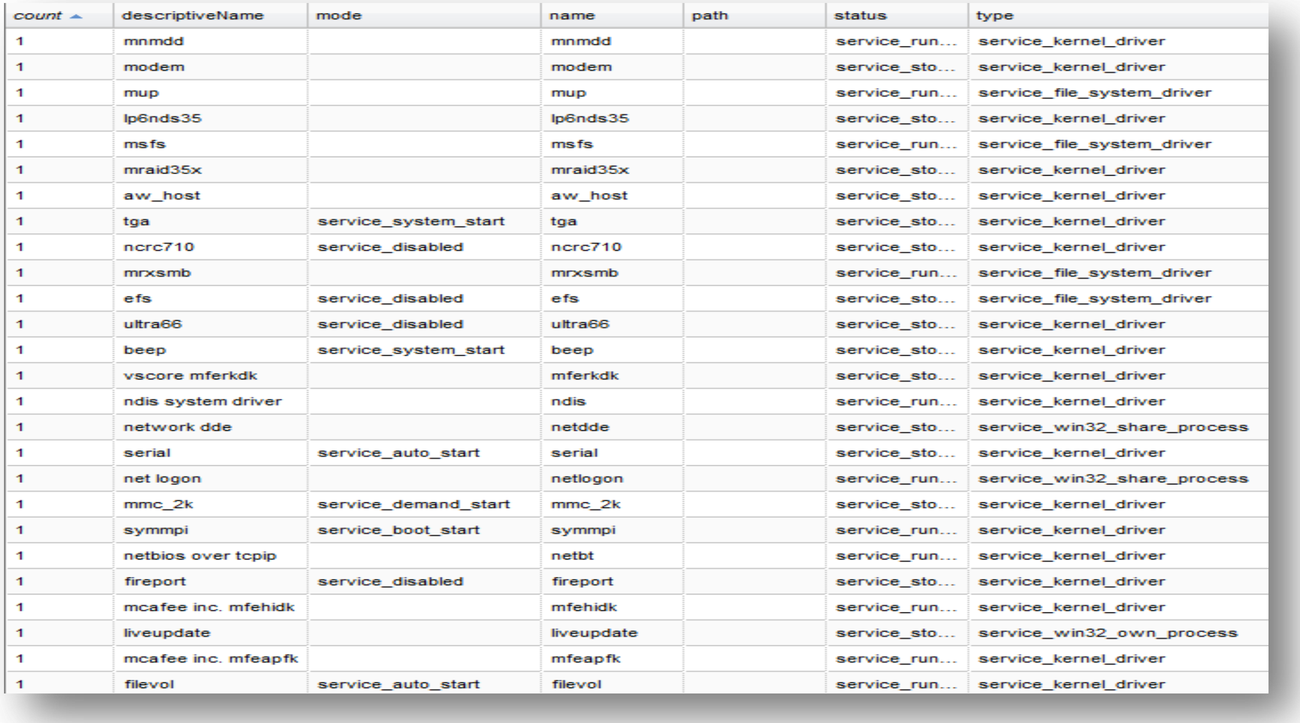
MIRcon 2012

Grouping Attributes

- Name
- Descriptive Name
- Service Executable Path
- Service Executable MD5
- Service DLL Path
- Service DLL MD5

Where is the Evil?

- Data is not going to look perfect
- False positives must be manually verified



count ▲	descriptiveName	mode	name	path	status	type
1	mnmdd		mnmdd		service_run...	service_kernel_driver
1	modem		modem		service_sto...	service_kernel_driver
1	mup		mup		service_run...	service_file_system_driver
1	lp6nds35		lp6nds35		service_sto...	service_kernel_driver
1	msfs		msfs		service_run...	service_file_system_driver
1	mraid35x		mraid35x		service_sto...	service_kernel_driver
1	aw_host		aw_host		service_sto...	service_kernel_driver
1	tga	service_system_start	tga		service_sto...	service_kernel_driver
1	ncrc710	service_disabled	ncrc710		service_sto...	service_kernel_driver
1	mrxsmb		mrxsmb		service_run...	service_file_system_driver
1	efs	service_disabled	efs		service_sto...	service_file_system_driver
1	ultra66	service_disabled	ultra66		service_sto...	service_kernel_driver
1	beep	service_system_start	beep		service_sto...	service_kernel_driver
1	vscore mferkdk		mferkdk		service_sto...	service_kernel_driver
1	ndis system driver		ndis		service_run...	service_kernel_driver
1	network dde		netdde		service_sto...	service_win32_share_process
1	serial	service_auto_start	serial		service_sto...	service_kernel_driver
1	net logon		netlogon		service_run...	service_win32_share_process
1	mmc_2k	service_demand_start	mmc_2k		service_sto...	service_kernel_driver
1	symmpi	service_boot_start	symmpi		service_run...	service_kernel_driver
1	netbios over tcpip		netbt		service_run...	service_kernel_driver
1	fireport	service_disabled	fireport		service_sto...	service_kernel_driver
1	mcafee inc. mfehidk		mfehidk		service_run...	service_kernel_driver
1	liveupdate		liveupdate		service_sto...	service_win32_own_process
1	mcafee inc. mfeapfk		mfeapfk		service_run...	service_kernel_driver
1	filevol	service_auto_start	filevol		service_run...	service_kernel_driver

Where is the Evil – Reducing

- Remove known good hashes
- Remove services with verified signature for Service DLL or Service Path
- Services with unusual Service DLL location should be investigated
  - GOOD - "wauaserv" -> %SystemRoot%\System32\w**a**uaserv.dll
  - BAD - "wauaserv" -> %SystemRoot%\System32\wuaserv.dll
  - BAD – “wauaserv” -> %SystemRoot%\Users\Bob\wauaserv.dll

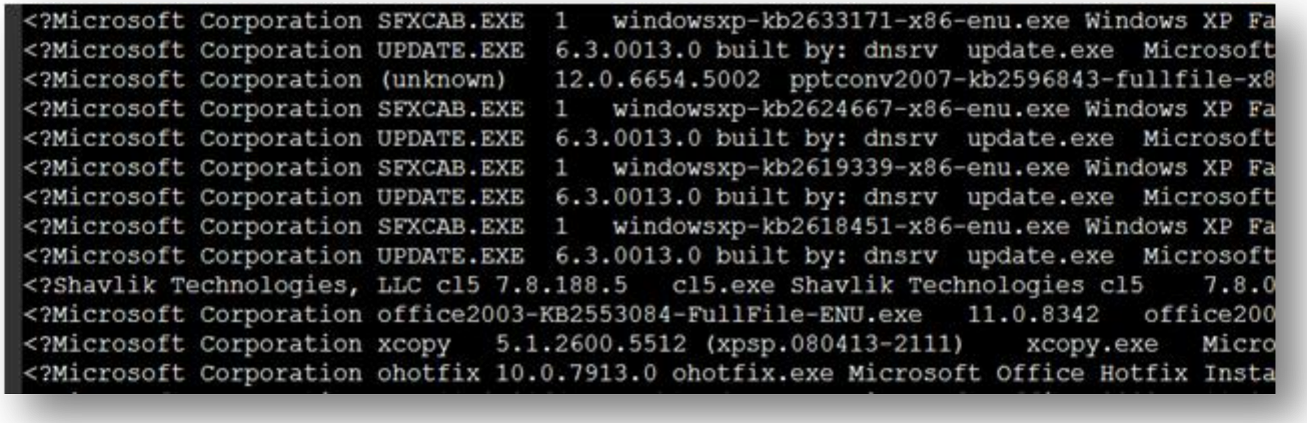
Evil Services

- Anomalies start to stand out

Count	Service Name	Path	Service DLL
5,598	59p	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\seclogon.dll
2	Seclogon	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\selogon.dll
1,233	NWCworkstation	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\nwwks.dll
2	NWCworkstation	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\nwwwks.dll
5,235	iprip	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\iprip.dll
2	iprip	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\iprinp.dll
3	iprip	C:\WINDOWS\System32\svchost.exe	%Tmp%\iprip.dll
5,598	wuauserv	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\system32\wuauserv.dll
8	wuauserv	C:\WINDOWS\System32\svchost.exe	%SystemRoot%\System32\wauaserv.dll

Example – Altiris Application Metering

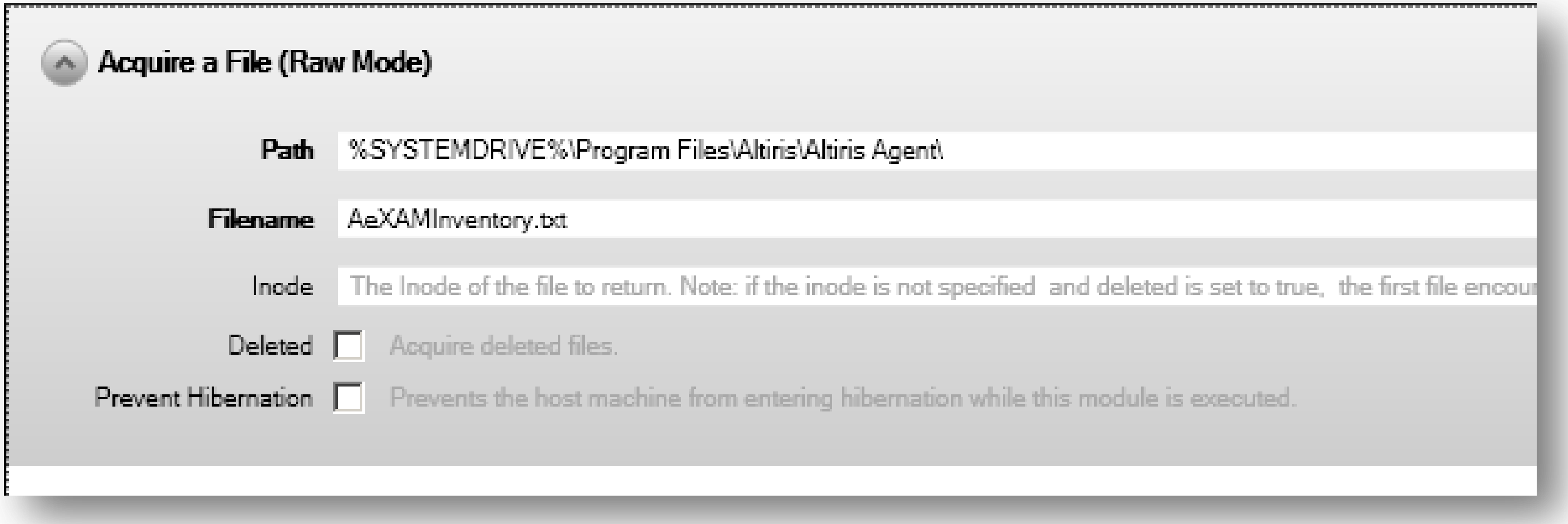
- A feature of the Altiris Agent
  - Monitor and manage applications on the endpoint
- Contains metadata of executed applications
  - *C:\Program Files\Altiris\Altiris Agent\AeXAMInventory.txt*
  - Tab-delimited text file



```
<?Microsoft Corporation SFXCAB.EXE  1   windowsxp-kb2633171-x86-enu.exe Windows XP Fa
<?Microsoft Corporation UPDATE.EXE  6.3.0013.0 built by: dnsrv  update.exe  Microsoft
<?Microsoft Corporation (unknown)   12.0.6654.5002  pptconv2007-kb2596843-fullfile-x8
<?Microsoft Corporation SFXCAB.EXE  1   windowsxp-kb2624667-x86-enu.exe Windows XP Fa
<?Microsoft Corporation UPDATE.EXE  6.3.0013.0 built by: dnsrv  update.exe  Microsoft
<?Microsoft Corporation SFXCAB.EXE  1   windowsxp-kb2619339-x86-enu.exe Windows XP Fa
<?Microsoft Corporation UPDATE.EXE  6.3.0013.0 built by: dnsrv  update.exe  Microsoft
<?Microsoft Corporation SFXCAB.EXE  1   windowsxp-kb2618451-x86-enu.exe Windows XP Fa
<?Microsoft Corporation UPDATE.EXE  6.3.0013.0 built by: dnsrv  update.exe  Microsoft
<?Shavlik Technologies, LLC cl5 7.8.188.5   cl5.exe Shavlik Technologies cl5    7.8.0
<?Microsoft Corporation office2003-KB2553084-FullFile-ENU.exe   11.0.8342   office200
<?Microsoft Corporation xcopy   5.1.2600.5512 (xpsp.080413-2111)    xcopy.exe   Micro
<?Microsoft Corporation ohotfix 10.0.7913.0 ohotfix.exe Microsoft Office Hotfix Insta
```

Acquiring Altiris Data with MIR

- Create audit for “Acquire a File (Raw/API)”
  - Might be install dependent (do a test batch!)



Acquire a File (Raw Mode)

Path: %SYSTEMDRIVE%\Program Files\Altiris\Altiris Agent\

Filename: AeXAMInventory.txt

Inode: The Inode of the file to return. Note: if the inode is not specified and deleted is set to true, the first file encou

Deleted □ Acquire deleted files.

Prevent Hibernation □ Prevents the host machine from entering hibernation while this module is executed.

Parsing the Altiris Data

- Lots of useful columns to stack
  - Company
  - File Path
  - Executable Name
  - Version
  - MD5 Sum (some versions)
- Need to convert the text files to something ingestible
  - XML, JSON, etc.

Altiris – Example Case

- Financial Sector
- FBI reported evidence of spear-phishing email
- Approximately 1,600 hosts in environment
- ~400 hosts with Altiris App. Metering enabled
- Very little evidence of attacker activity (mass-malware)
- Collected Altiris Application Metering data for every available system

Altiris Case Results

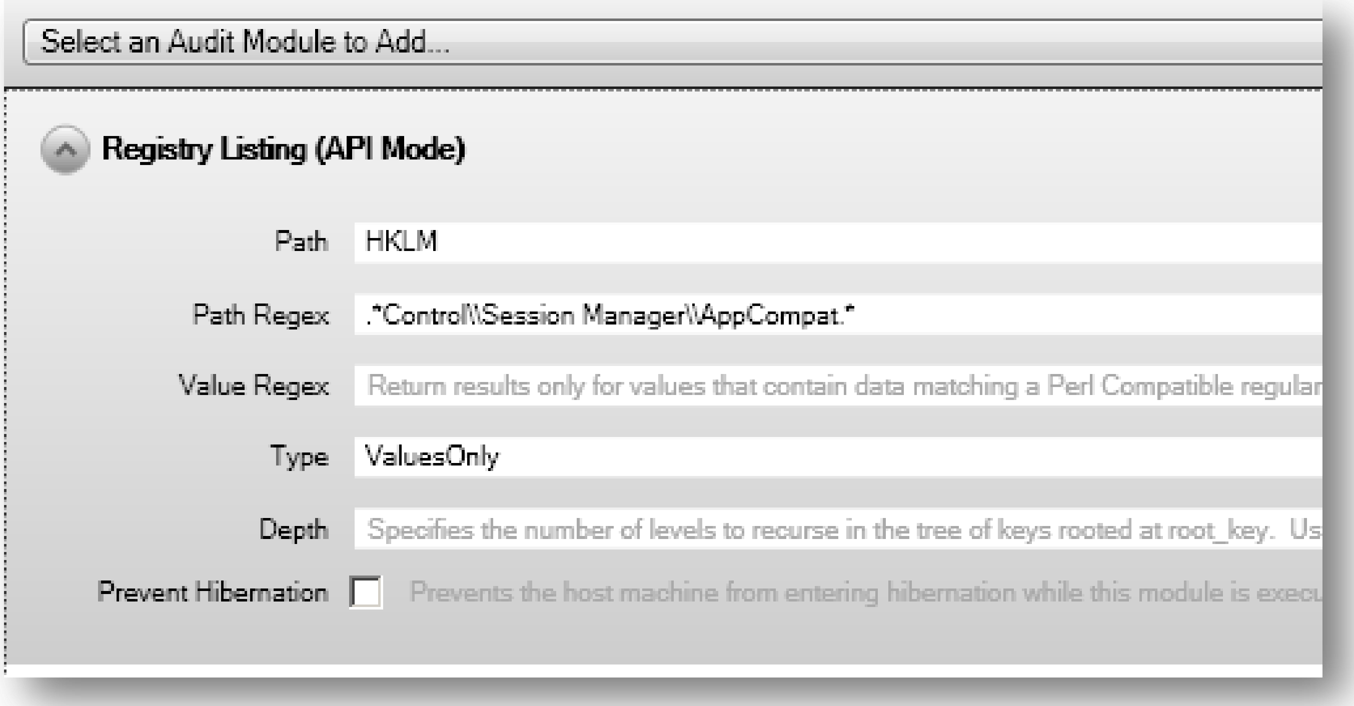
Count	Executable	Path	Company
54	cupc.exe	C:\Program Files\Common Files\Cisco Systems\Client Services Framework	Cisco Systems, inc.
73	custom.exe	C:\progra~1\alritis\altiri~1\agents\softwa~1\000b8~1\cache\setup	Altiris, inc.
65	custom.exe	C:\progra~1\alritis\altiri~1\agents\softwa~1\48009~1\cache\setup	Altiris, inc.
5	custom.exe	C:\Documents and Settings\All Users\Local Settings\Temp	(Unknown)
80	cvpnd.exe	C:\Program Files\Cisco Systems\VPN Client	Cisco Systems, inc.

Example – AppCompat Stacking

- Windows Application Compatibility Database contains interesting forensic artifacts
- Consists of two registry keys
  - *HKLM\SYSTEM\Control\Session Manager\AppCompatibility\AppCompatCache*
    - Windows XP
  - *HKLM\SYSTEM\Control\Session Manager\AppCompatCache\AppCompatCache*
    - Everything else
- Stores metadata of files written/executed on the system
- Only files with specific extensions are logged (i.e. “.exe”,”.bat”,”.dll”)

Acquiring AppCompat Data with MIR

- Create audit for "Registry Listing (API Mode)"



Select an Audit Module to Add...

Registry Listing (API Mode)

Path: HKLM

Path Regex: .*Control\\Session Manager\\AppCompat.*

Value Regex: Return results only for values that contain data matching a Perl Compatible regular

Type: ValuesOnly

Depth: Specifies the number of levels to recurse in the tree of keys rooted at root_key. Us

Prevent Hibernation ☐ Prevents the host machine from entering hibernation while this module is execu

Parsing AppCompat Data

- ShimCacheParser.py - Tool released by Andrew Davis of Mandiant to extract AppCompat data
  - https://blog.mandiant.com/archives/2459
- Extracts this data from a number of inputs
  - Registry hives
  - MIR XML
  - Mass MIR registry key acquisitions contained in ZIP archives
  - The current system
  - Exported binary files
- Convert tool output to standard format

AppCompat Example Case

- Energy sector
- Notified by FBI
- Approximately 7,000 hosts
- Attackers were present for over 2 years
- Heavy recent activity from attackers
- Email of top executives stolen weekly
- Collected AppCompat data for every system, including MD5 sums of each file

AppCompat Case Results

File Path	MD5 Sum	File Owner	Count
c:\windows\system32\msiexec.exe	21b81c98d786cec9c1e82cc5e57d993b	builtin\administrators	1
c:\Documents and Settings\All Users\Application Data\Symantec\Resource\msiexec.exe	5172ce4d0752d847cfd7677a7d896336	builtin\administrators	1
c:\WINDOWS\Temp\msiexec.exe	a87b1a2de5093fd42f2c271e69236846	builtin\administrators	2
c:\compaq\wbem\certs\msiexec.exe	d29028d462b8fd60aa4ea53f7766487f	builtin\administrators	3
c:\windows\system32\msiexec.exe	97474784b079ad522da049b0c196e8b9	nt service\trustedinstaller	10
c:\windows\system32\msiexec.exe	97474784b079ad522da049b0c196e8b9	builtin\administrators	244
c:\windows\system32\msiexec.exe	a190da6546501cb4146bbcc0b6a3f48b	nt service\trustedinstaller	491
c:\windows\system32\msiexec.exe	eee470f2a771fc0b543bdeef74fceca0	nt service\trustedinstaller	788

Get Creative!

- Stack data and find anomalies across your enterprise
- Can be used on many forensic artifacts on systems
  - Logons
  - Software management logs (Altiris, LanDesk, etc.)
  - Windows Prefetch
  - Persistence methods
  - Etc.
- If you can acquire the data, you can stack it!

MIRcon 2012

Questions and Answers