MANDIANT®

Finding Evil with Data Stacking

Nick Bennett and Jake Valletta
June 27, 2012

Agenda

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

Nick Bennett

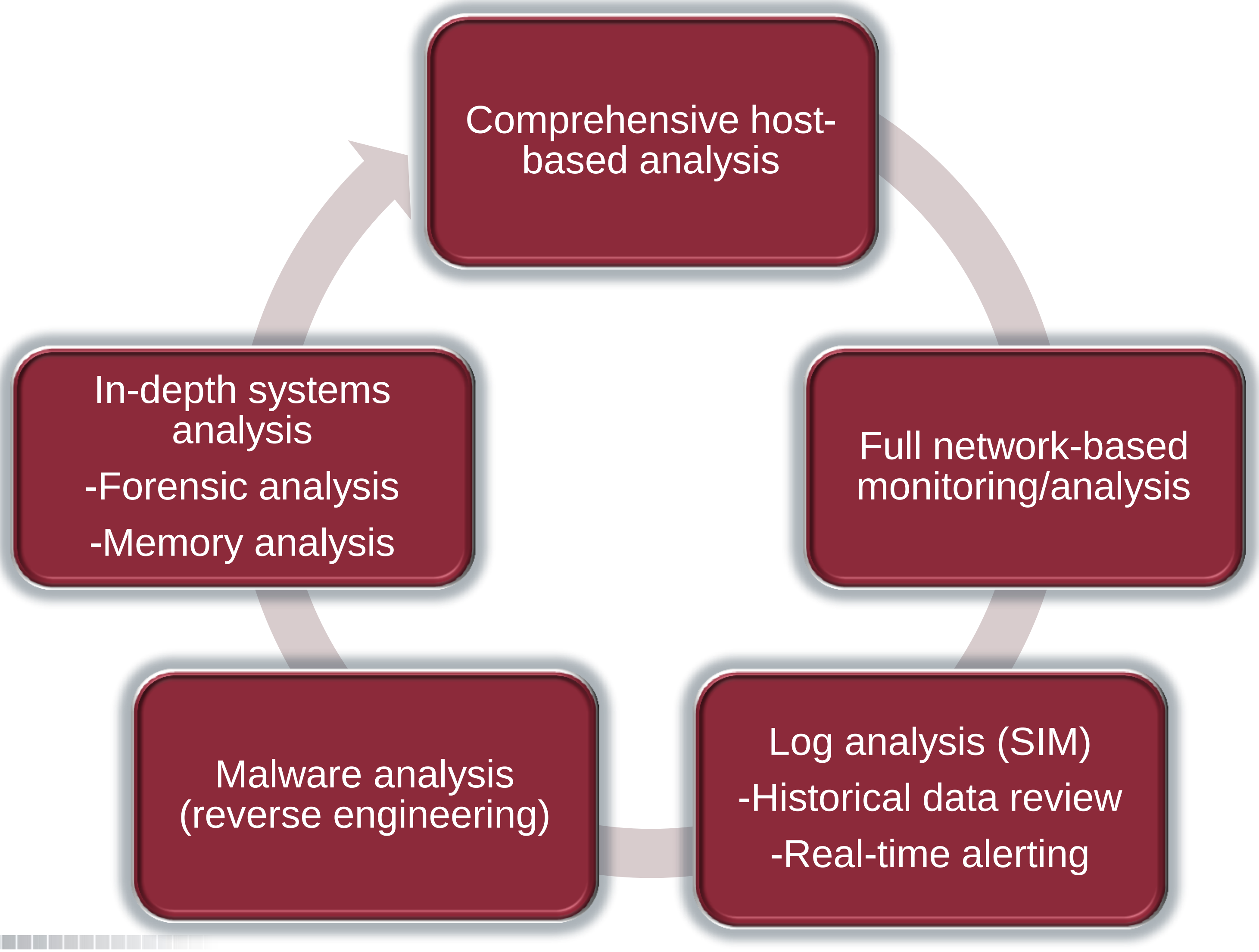
- Principal Consultant at Mandiant NYC office
- 7 years experience in Information Security Field
- Application penetration testing, forensics, incident response
- nick.bennett@mandiant.com

Jake Valletta

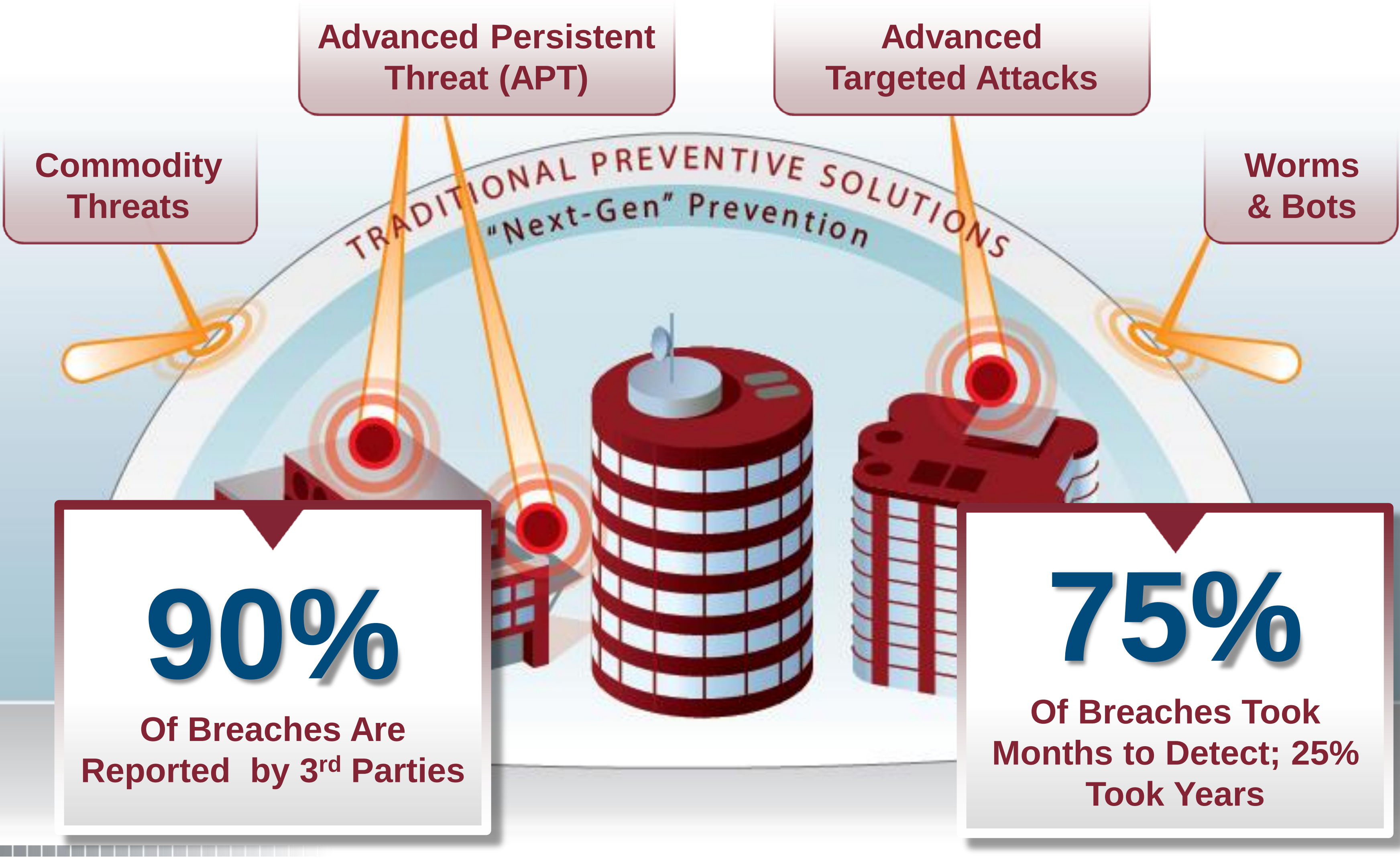
- Associate Consultant at Mandiant
- Mobile Security, App. Assessments & Penetration Testing, Forensics
- Blog: http://thecobraden.blogspot.com
- Repos: https://github.com/jakev
- jake.valletta@mandiant.com

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

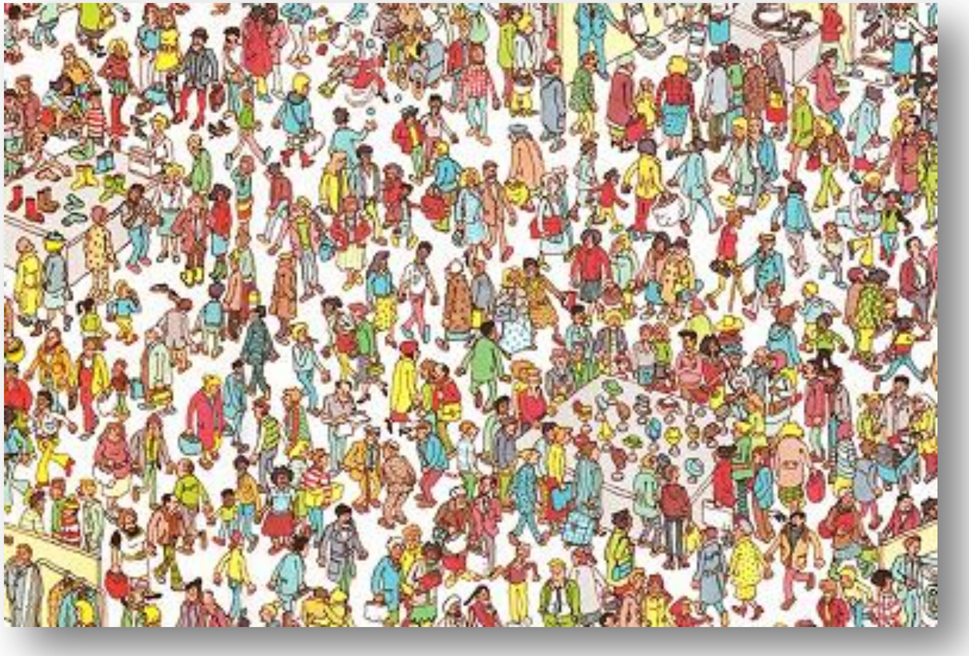
Enter Stacking…

What is Stacking?

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

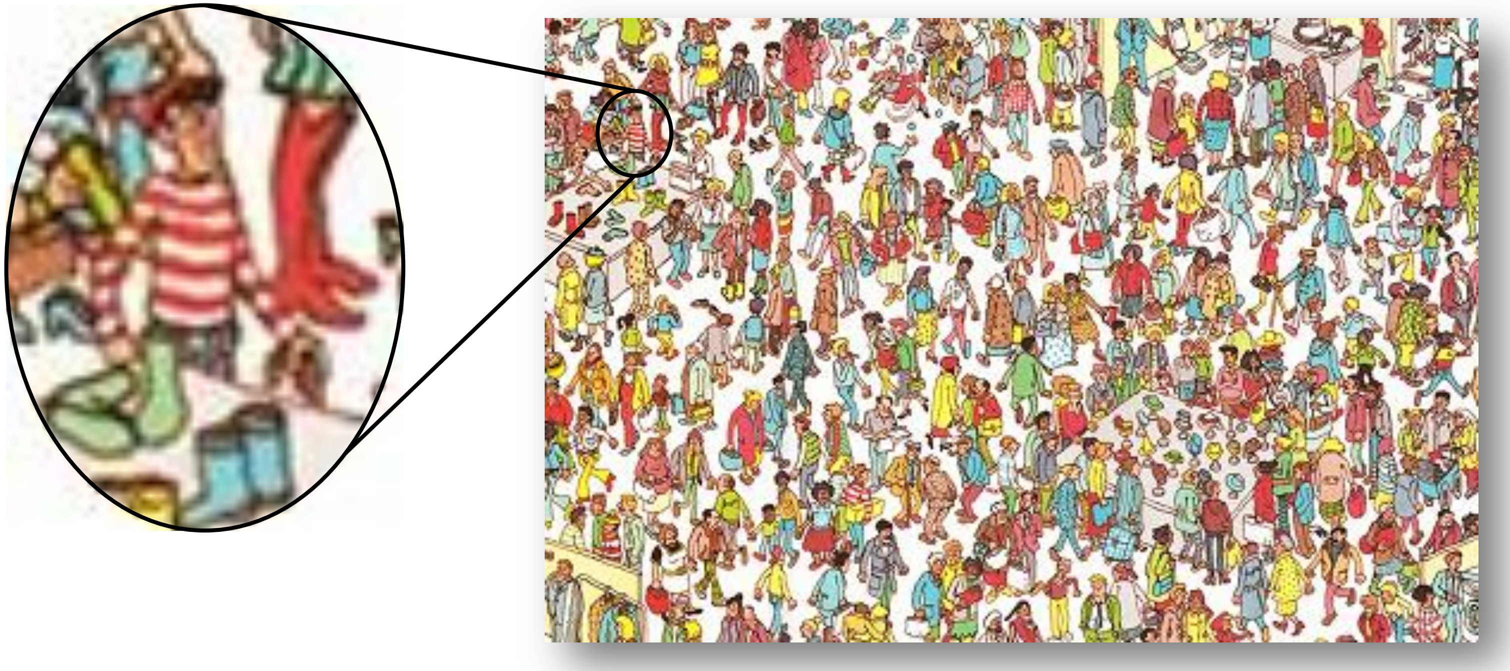
Stacking 101

- Start with a large data set
- Select attributes you want to group
- 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 positive rate
  - Waldo example: low occurrence of other outfits
- Potential for high false negative
  - Waldo example: several others wearing red/write stripe shirt

Stacking Basics – How It’s Done

Need a Strong Acquisition Method

- Commercial Solutions
  - Incident response tools, application metering, HIPS, etc
- “Home Grown”
  - Scripts, WMI, GPO, and creativity
- Pros and cons to both approaches

Pros and Cons – Commercial Tools

- Pros
  - Tried and tested
  - Support for various platforms
  - “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
  - Have to manually parse data

Acquiring Lots of Data - Commercial

- Acquiring data with commercial solutions should be straightforward
  - Many solutions allow a variety of information to be collected
  - Export and consolidate to a server

Acquiring Lots of Data – Home Grown

- Manually obtaining data requires you to be more creative
- Push needed files to clients, execute custom .bat/.vbs script
- Send data to consolidation server
- Don’t forget to record which host the data is coming from!!

Parsing Data

- Process is relatively similar for any data set
  - Create a script that takes raw data, produces CSV
  - Import CSV into Excel for sorting/filtering
- Much easier to perform when "data" is in a standard format
  - XML, JSON objects

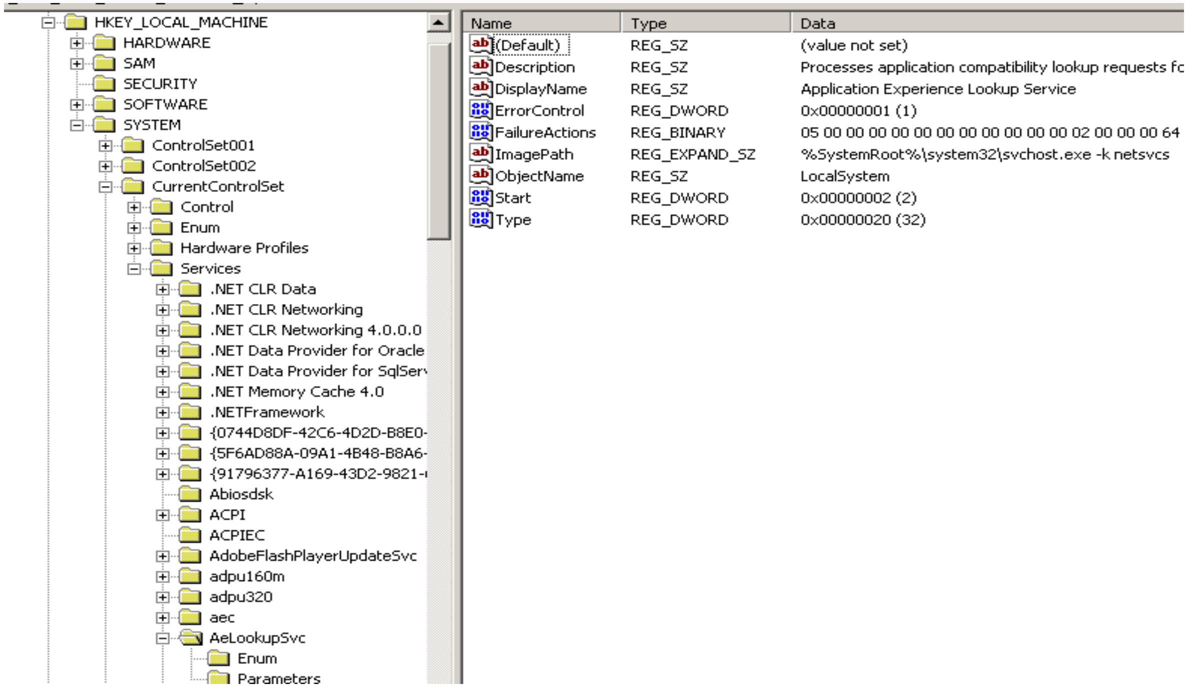
Finding Evil – Examples

Example – Service Stacking

- Finding evil by stacking service metadata
- Need to enumerate various information about service
  - Service Name
  - Service Descriptive Name
  - Service Path + MD5 sum
  - Service DLL + MD5 sum
  - etc.
- Start with *SC QUERY* to get a service listing

Example – Service Stacking

- Service details are maintained in the Windows Registry
  - *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*

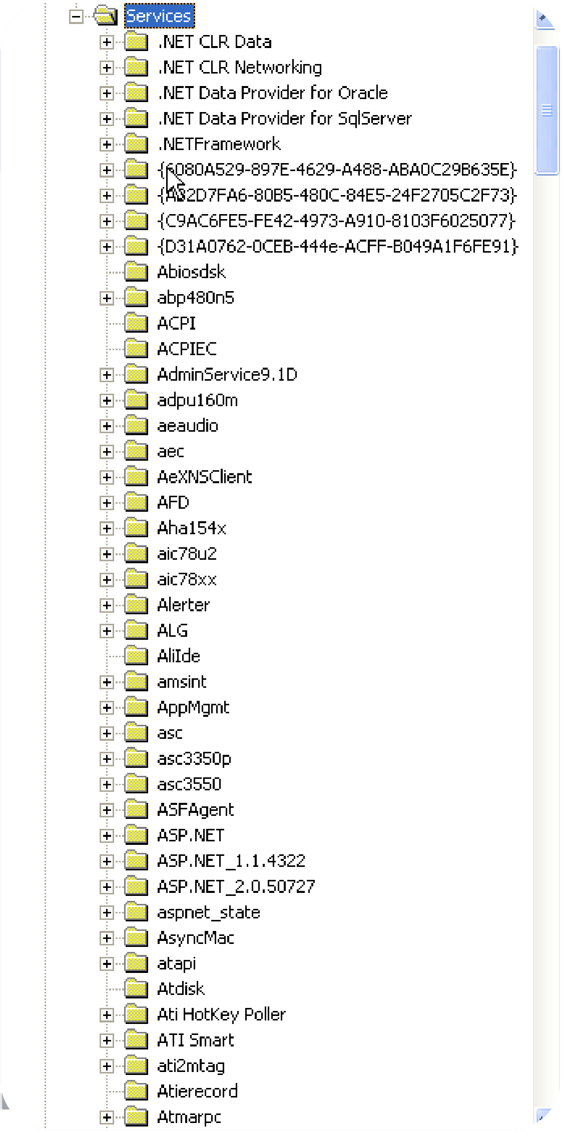


Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Processes application compatibility lookup requests fc
DisplayName	REG_SZ	Application Experience Lookup Service
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 64
ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k netsvcs
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000020 (32)

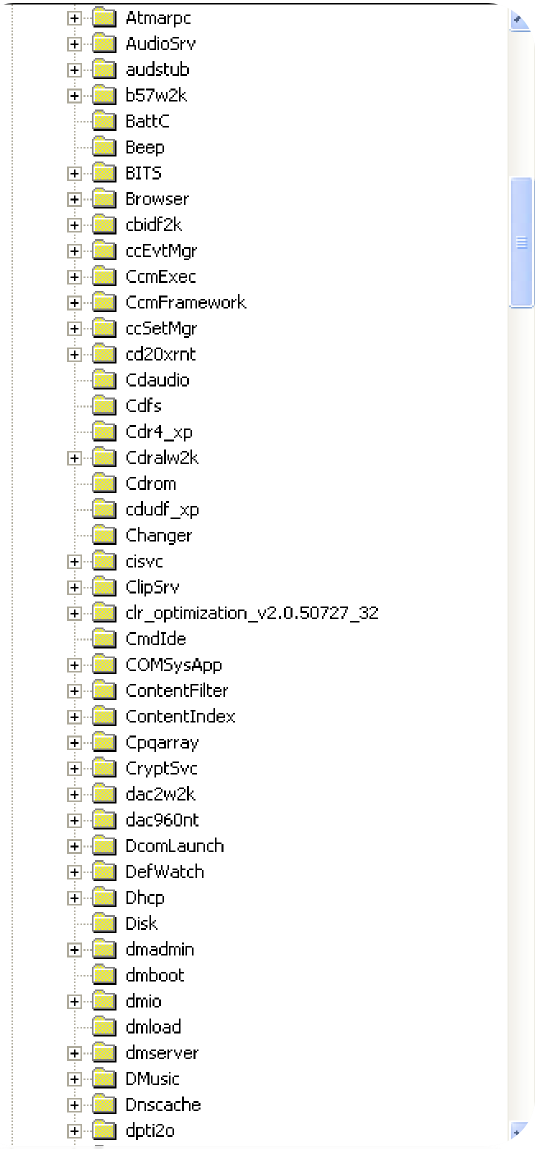
Example – Service Stacking

- Access registry keys using *REG QUERY*
- Validating digital signatures of Service DLLs
  - *sigcheck* by SysInternals makes use of Windows API to validate known signatures
- Calculating MD5 sum of Service executable
  - Numerous free utilities

Reviewing Services is Easy?



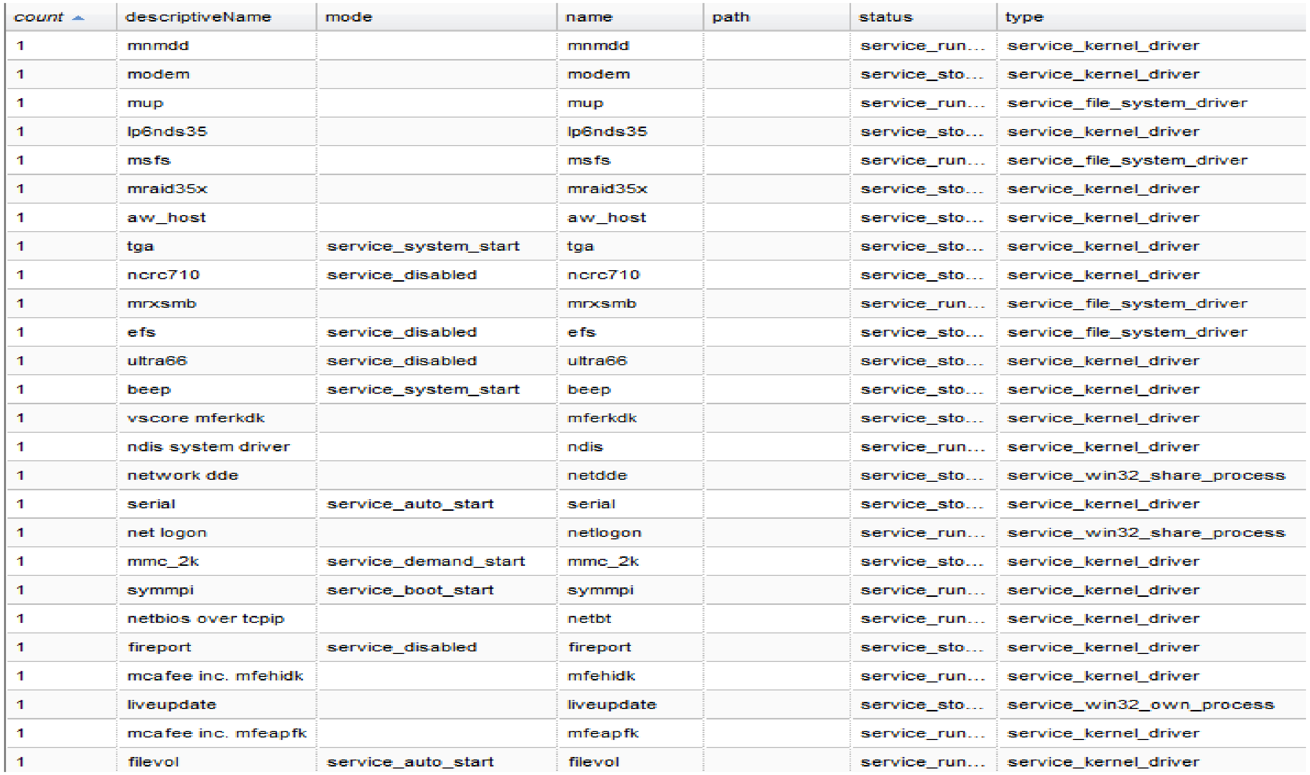
```
Services
  .NET CLR Data
  .NET CLR Networking
  .NET Data Provider for Oracle
  .NET Data Provider for SqlServer
  .NETFramework
  {6080A529-897E-4629-A488-ABA0C29B635E}
  {A52D7FA6-80B5-480C-84E5-24F2705C2F73}
  {C9AC6FE5-FE42-4973-A910-8103F6025077}
  {D31A0762-0CEB-444e-ACFF-B049A1F6FE91}
  Abiosdsk
  abp480n5
  ACPI
  ACPIEC
  AdminService9.1D
  adpu160m
  aeaudio
  aec
  AeXNSClient
  AFD
  Aha154x
  aic78u2
  aic78xx
  Alerter
  ALG
  AliIde
  amsint
  AppMgmt
  asc
  asc3350p
  asc3550
  ASFAgent
  ASP.NET
  ASP.NET_1.1.4322
  ASP.NET_2.0.50727
  aspnet_state
  AsyncMac
  atapi
  Atdisk
  Ati HotKey Poller
  ATI Smart
  ati2mtag
  Atierecord
  Atmarpc
```



```
  Atmarpc
  AudioSrv
  audstub
  b57w2k
  BattC
  Beep
  BITS
  Browser
  cbidf2k
  ccEvtMgr
  CcmExec
  CcmFramework
  ccSetMgr
  cd20xrnt
  Cdaudio
  Cdfs
  Cdr4_xp
  Cdralw2k
  Cdrom
  cdudf_xp
  Changer
  cisvc
  ClipSrv
  clr_optimization_v2.0.50727_32
  CmdIde
  COMSysApp
  ContentFilter
  ContentIndex
  Cpqarray
  CryptSvc
  dac2w2k
  dac960nt
  DcomLaunch
  DefWatch
  Dhcp
  Disk
  dmadmin
  dmboot
  dmio
  dmload
  dmserver
  DMusic
  Dnscache
  dpti2o
```

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?

- Remove known good hashes
- Look for services with unverified signature for Service DLL or Service Path
- Services with unusual Service DLL location should be investigated
  - GOOD - "wauaserv" -> %SystemRoot%\System32\wauaserv.dll
  - BAD - "wauaserv" -> %SystemRoot%\System32\wuaserv.dll

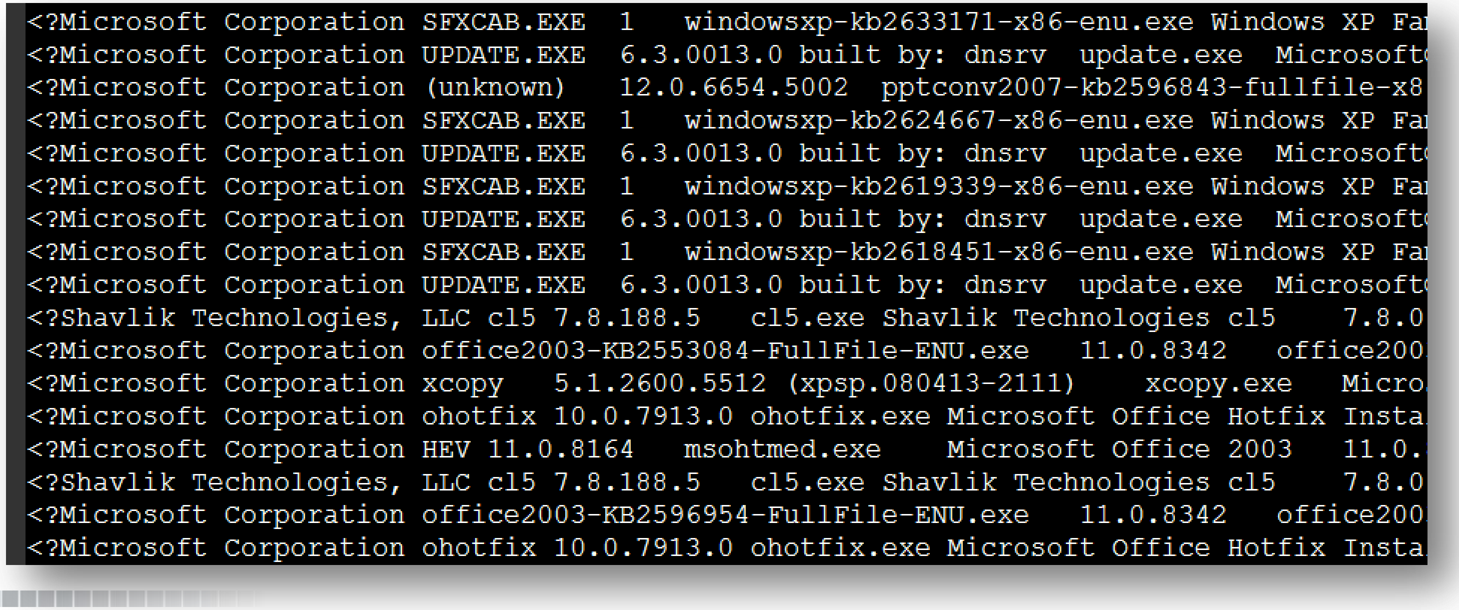
Evil Services

- Anomalies 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 system
- Logs various metadata of executed applications
  - *C:\Program Files\Altiris\Altiris Agent\AeXAMInventory.txt*
  - Tab-delimited 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
<?Microsoft Corporation HEV 11.0.8164   msohtmed.exe    Microsoft Office 2003   11.0.
<?Shavlik Technologies, LLC cl5 7.8.188.5   cl5.exe Shavlik Technologies cl5    7.8.0
<?Microsoft Corporation office2003-KB2596954-FullFile-ENU.exe   11.0.8342   office200
<?Microsoft Corporation ohotfix 10.0.7913.0 ohotfix.exe Microsoft Office Hotfix Insta
```

Example – Altiris Application Metering

- Some useful columns to stack:
  - Company
  - File Path
  - Executable Name
  - Version
  - MD5 sum (some versions)

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 - Example

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")

Example - AppCompat Stacking

- 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

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 Example Case

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

MANDIANT®

Questions and Answers