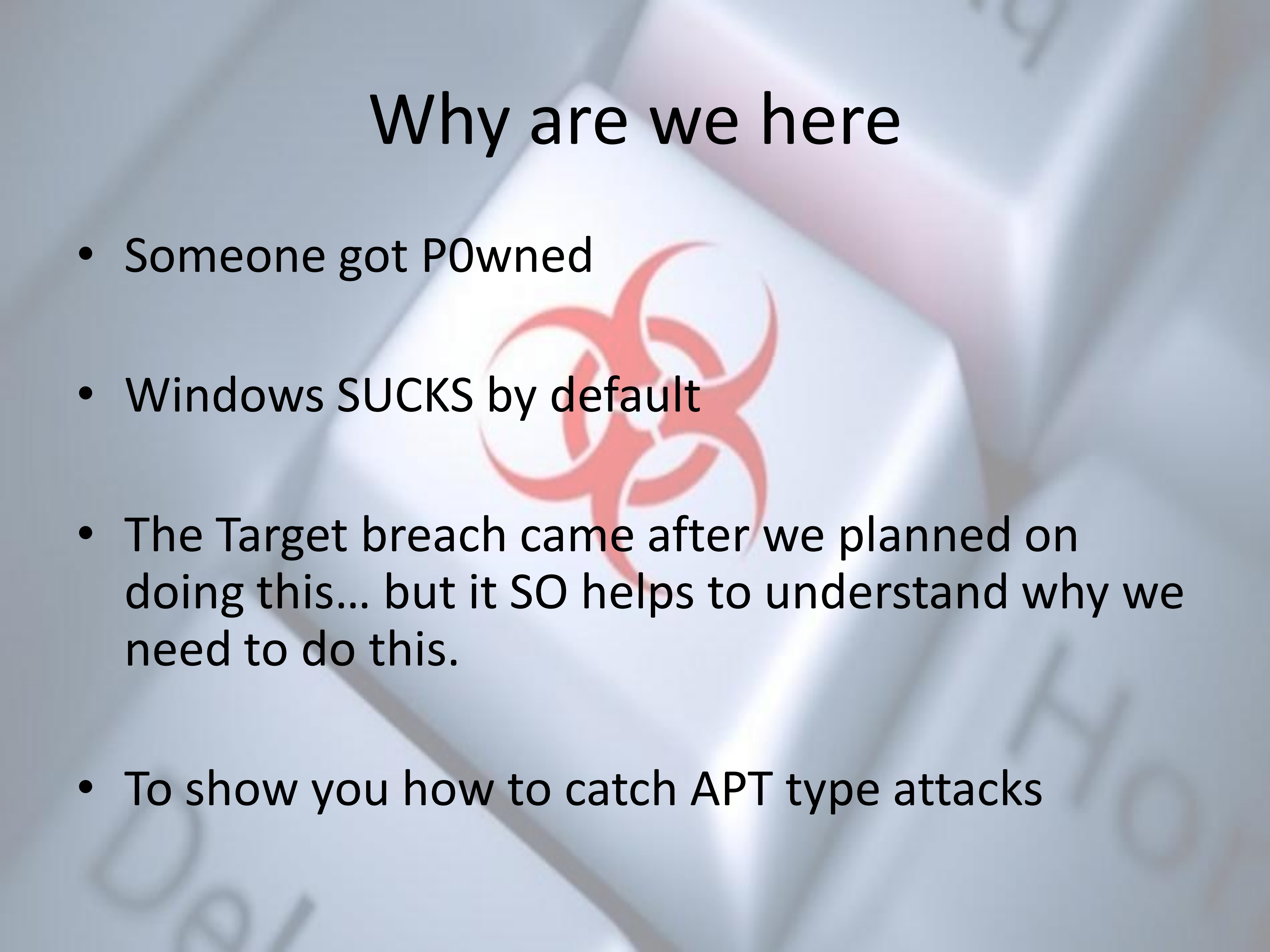
Windows Logging Workshop
You could have and SHOULD have caught the Target Breach!

Michael Gough – Principal

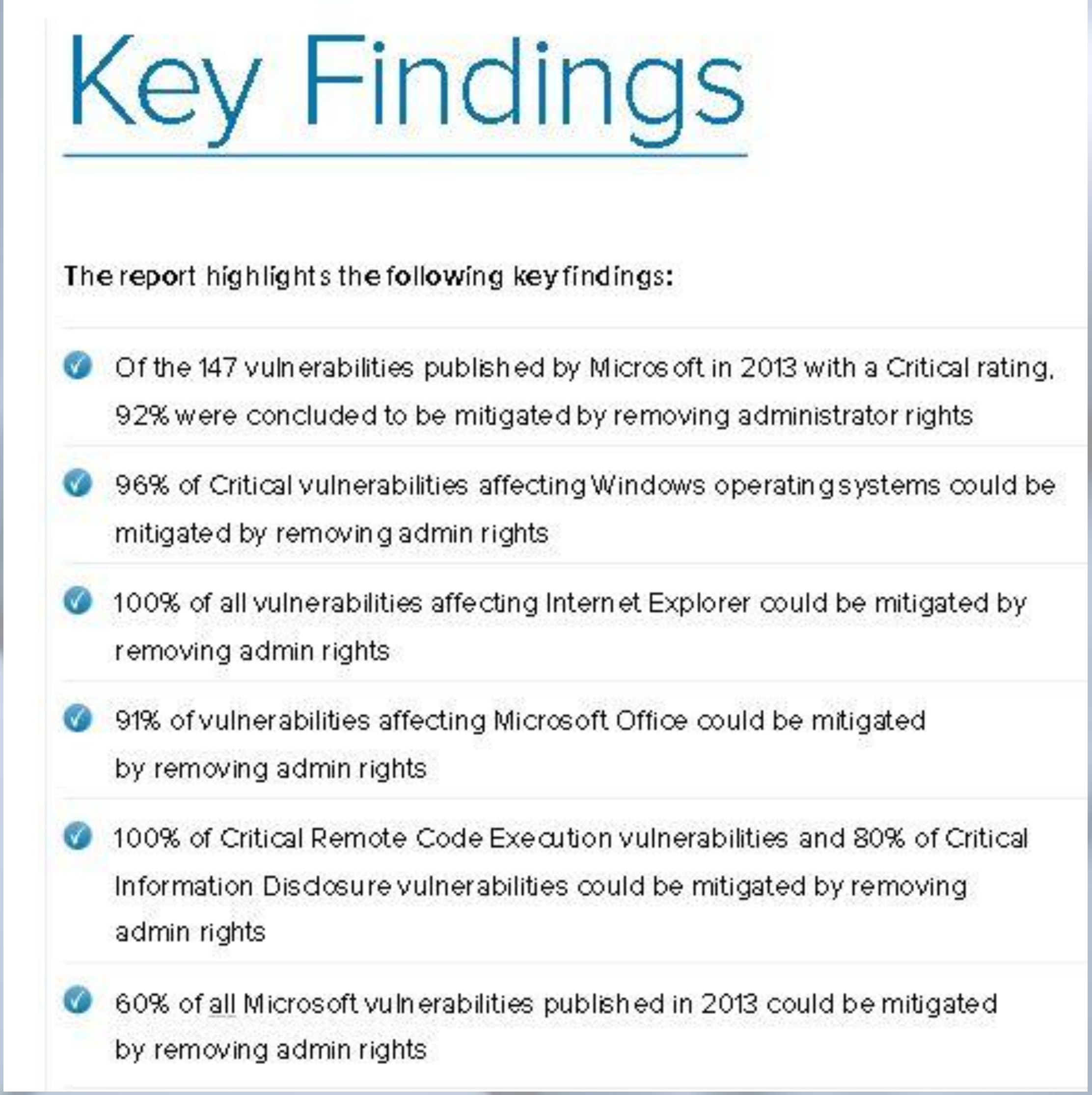
MI$_2$Security.com



Why are we here

- Someone got P0wned
- Windows SUCKS by default
- The Target breach came after we planned on doing this… but it SO helps to understand why we need to do this.
- To show you how to catch APT type attacks

Avecto Study – Admin = P0wnage



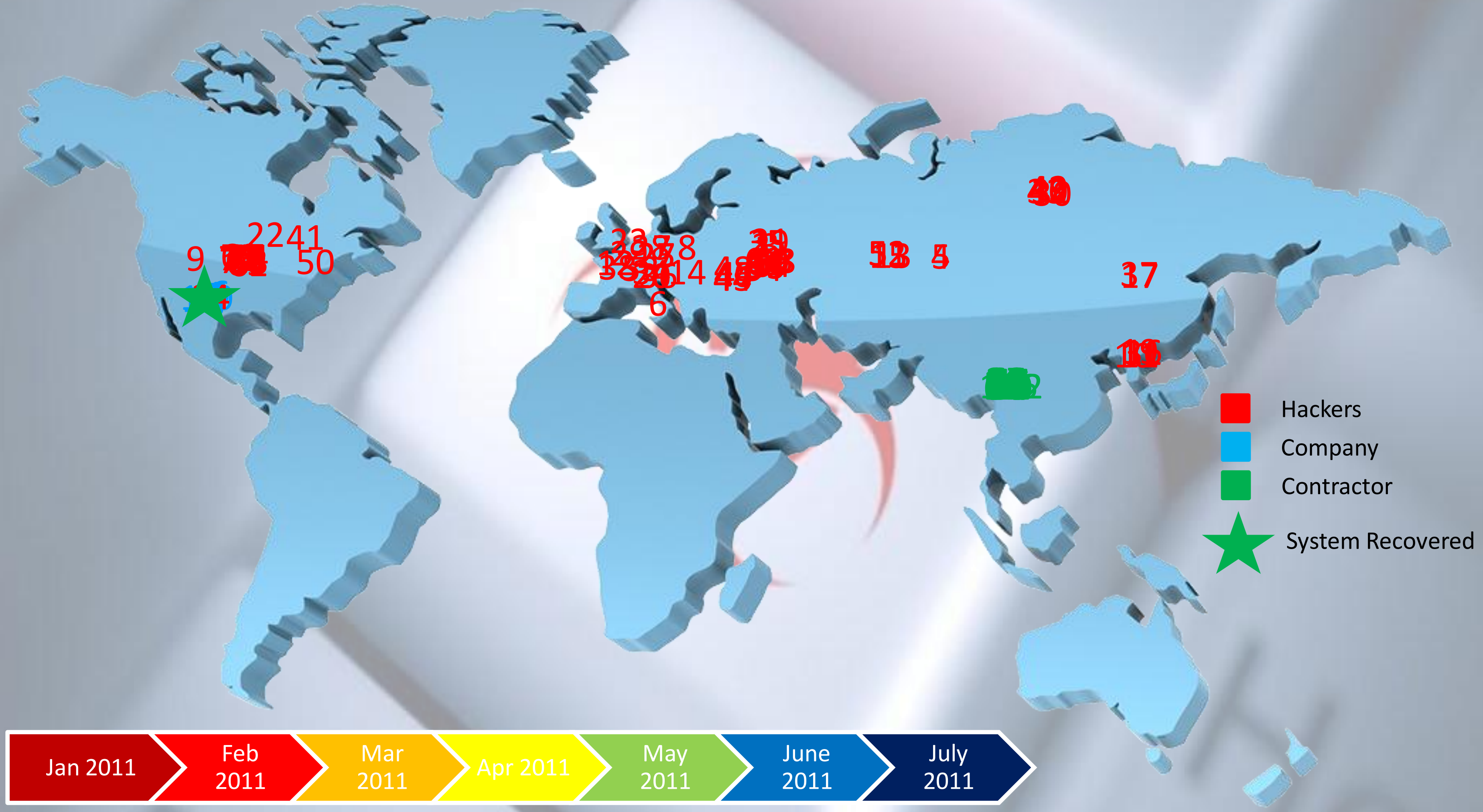
Key Findings

The report highlights the following key findings:

- ✓ Of the 147 vulnerabilities published by Microsoft in 2013 with a Critical rating, 92% were concluded to be mitigated by removing administrator rights
- ✓ 96% of Critical vulnerabilities affecting Windows operating systems could be mitigated by removing admin rights
- ✓ 100% of all vulnerabilities affecting Internet Explorer could be mitigated by removing admin rights
- ✓ 91% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights
- ✓ 100% of Critical Remote Code Execution vulnerabilities and 80% of Critical Information Disclosure vulnerabilities could be mitigated by removing admin rights
- ✓ 60% of all Microsoft vulnerabilities published in 2013 could be mitigated by removing admin rights

When and from Where?

Successful Logons – Jan 4, 2011 to July 6, 2011



🟥 Hackers

🟦 Company

🟩 Contractor

★ System Recovered

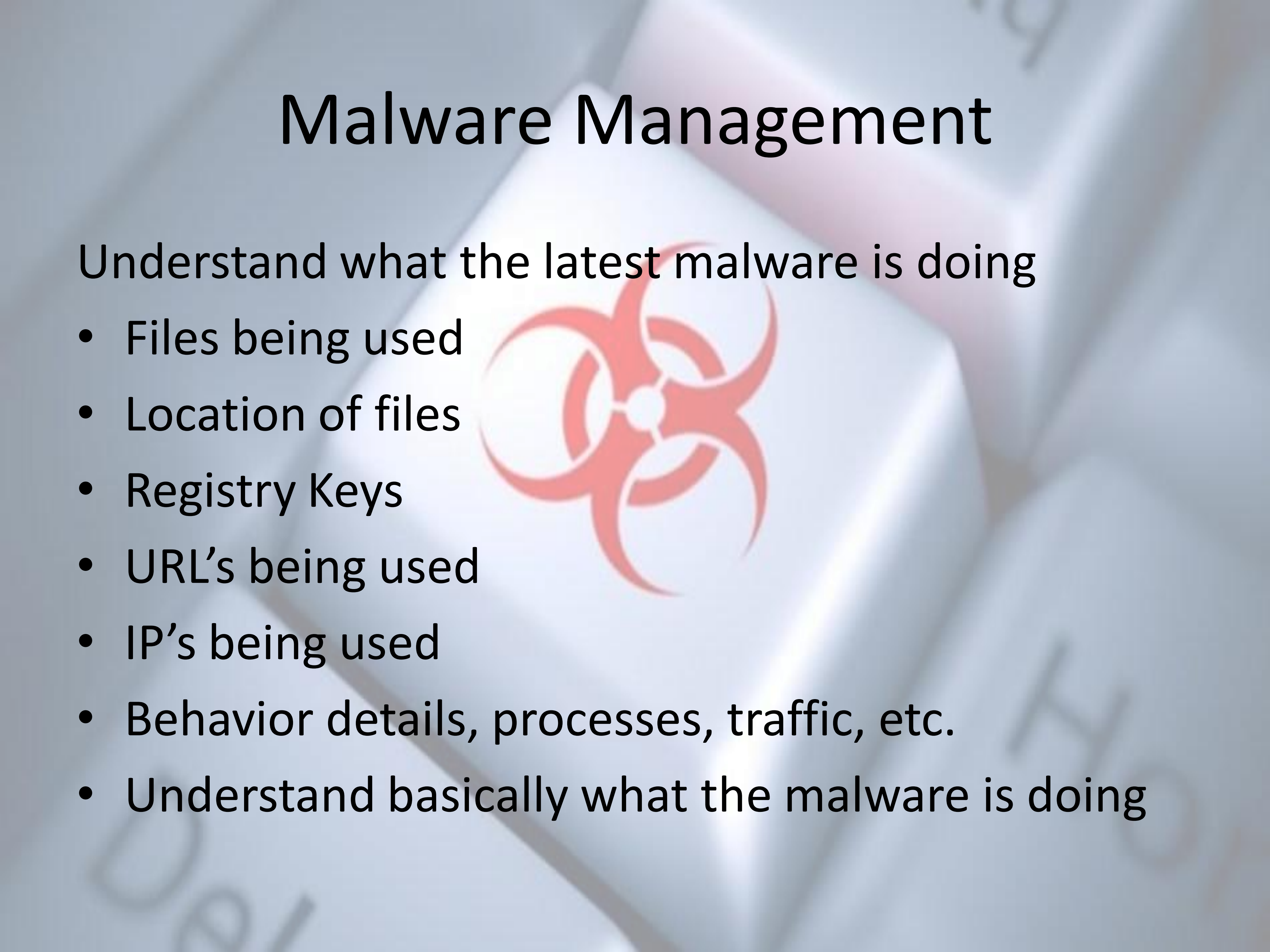
Typical Windows system on the internet with port 3389 open – Password brute forced/guessed

HackerHurricane.com

The Malware Management Framework

- This presentation, and many more we do is because we all need to start practicing Malware Management.
- Analyze the information in Malware reports wherever you can find it
- Use this Intel to feed into your security tools
- Use this Intel to feed into your logging solution and learn what to log for.

www.MalwareManagement.org

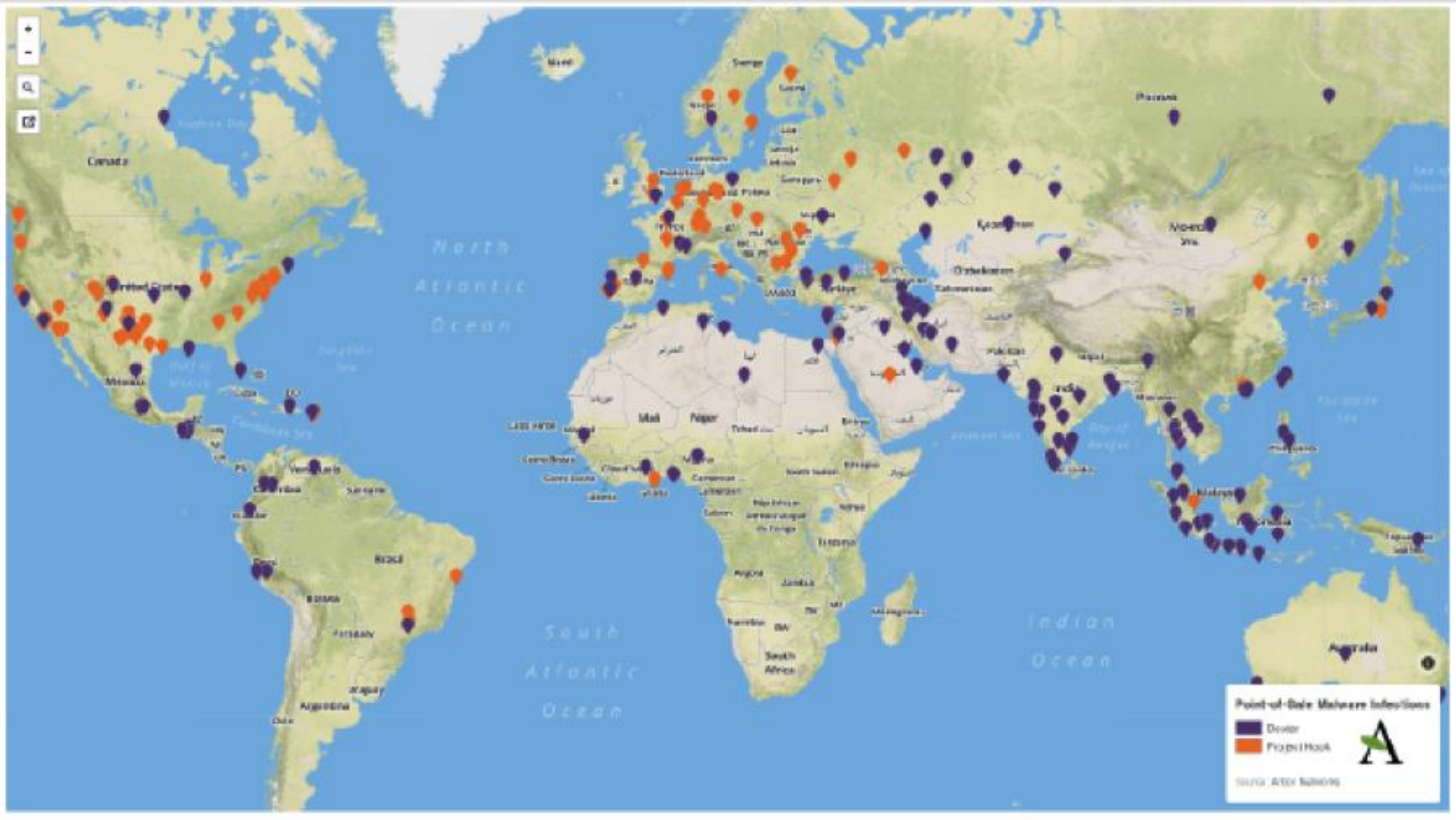


Malware Management

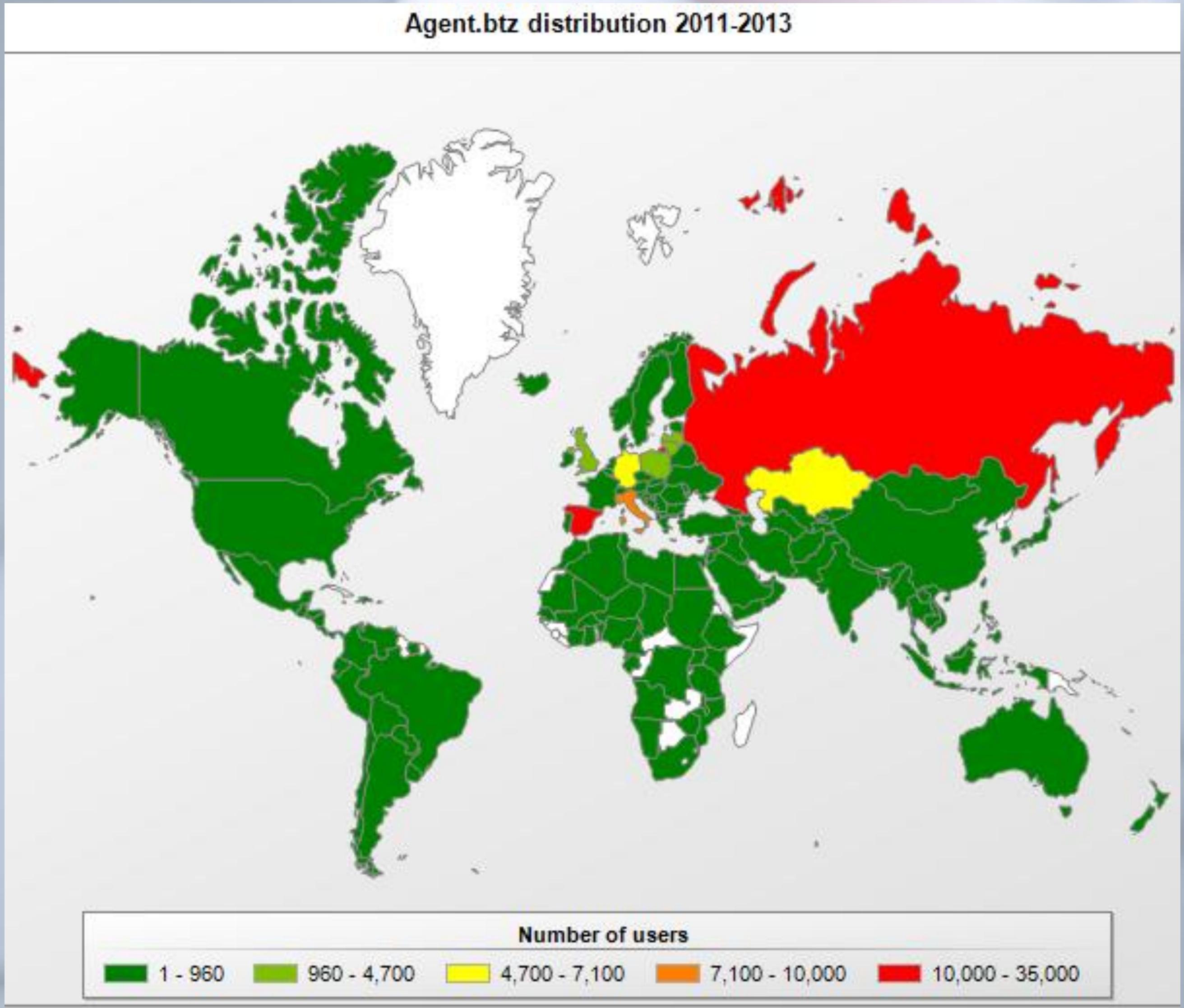
Understand what the latest malware is doing

- Files being used
- Location of files
- Registry Keys
- URL’s being used
- IP’s being used
- Behavior details, processes, traffic, etc.
- Understand basically what the malware is doing

Project-Hook & Dexter CC Malware



Agent.BTZ


Agent.btz distribution 2011-2013

ROOTKIT EXECUTION

When first executed, the driver creates device named `\Device\vstor32` with a symbolic link `\DosDevices\vstor32`. This device is used for userland/kernel communications.

Next, it drops a DLL into the `%windows%` directory - the DLL is carried in the body of the driver as a binary chunk with XOR `0xAA` applied on top of it, so the driver decrypts it first.

Depending on the variant, the DLL is dropped either under a random name or a hard-coded name, such as `mscpx32n.dll`.

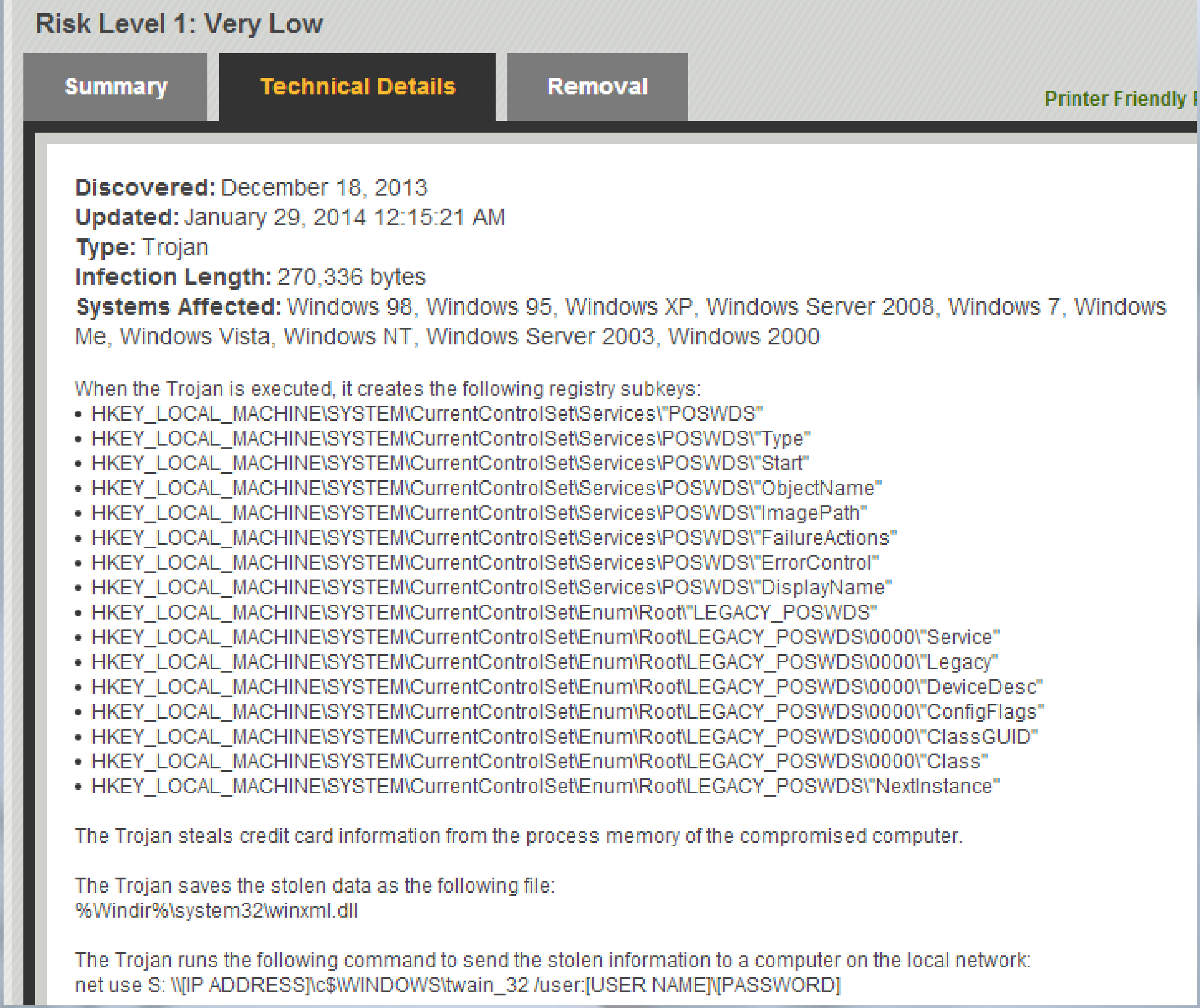
The purpose of this DLL is to be injected into the user-mode processes. Some variants of Snake carry the DLL modules that can be installed as a service, to be run within `taskhost.exe` or `services.exe` processes.

Next, the driver sets up the hooks for the following kernel-mode APIs:

- `ZwCreateThread`
- `ZwCreateUserProcess`
- `ZwShutdownSystem`

After that, it calls `PsSetCreateProcessNotifyRoutine()` in order to be notified whenever a new process is started.

BlackPoS - Symantec



Discovered: December 18, 2013
Updated: January 29, 2014 12:15:21 AM
Type: Trojan
Infection Length: 270,336 bytes
Systems Affected: Windows 98, Windows 95, Windows XP, Windows Server 2008, Windows 7, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

When the Trojan is executed, it creates the following registry subkeys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\"POSWDS"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"Type"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"Start"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"ObjectName"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"ImagePath"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"FailureActions"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"ErrorControl"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\"DisplayName"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\"LEGACY_POSWDS"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"Service"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"Legacy"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"DeviceDesc"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"ConfigFlags"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"ClassGUID"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\"Class"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\"NextInstance"

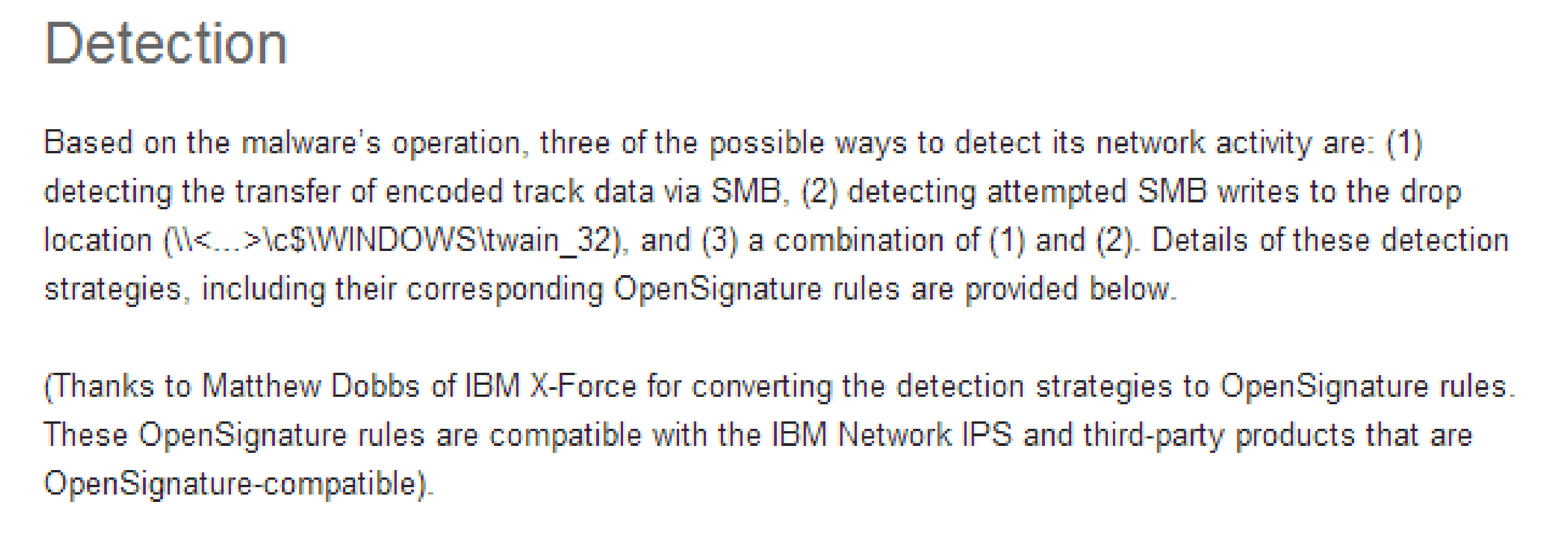
The Trojan steals credit card information from the process memory of the compromised computer.

The Trojan saves the stolen data as the following file:
%Windir%\system32\winxml.dll

The Trojan runs the following command to send the stolen information to a computer on the local network:

```
net use S: \\[IP ADDRESS]\c$\WINDOWS\twain_32 /user:[USER NAME]\[PASSWORD]
```

How cute, they tried



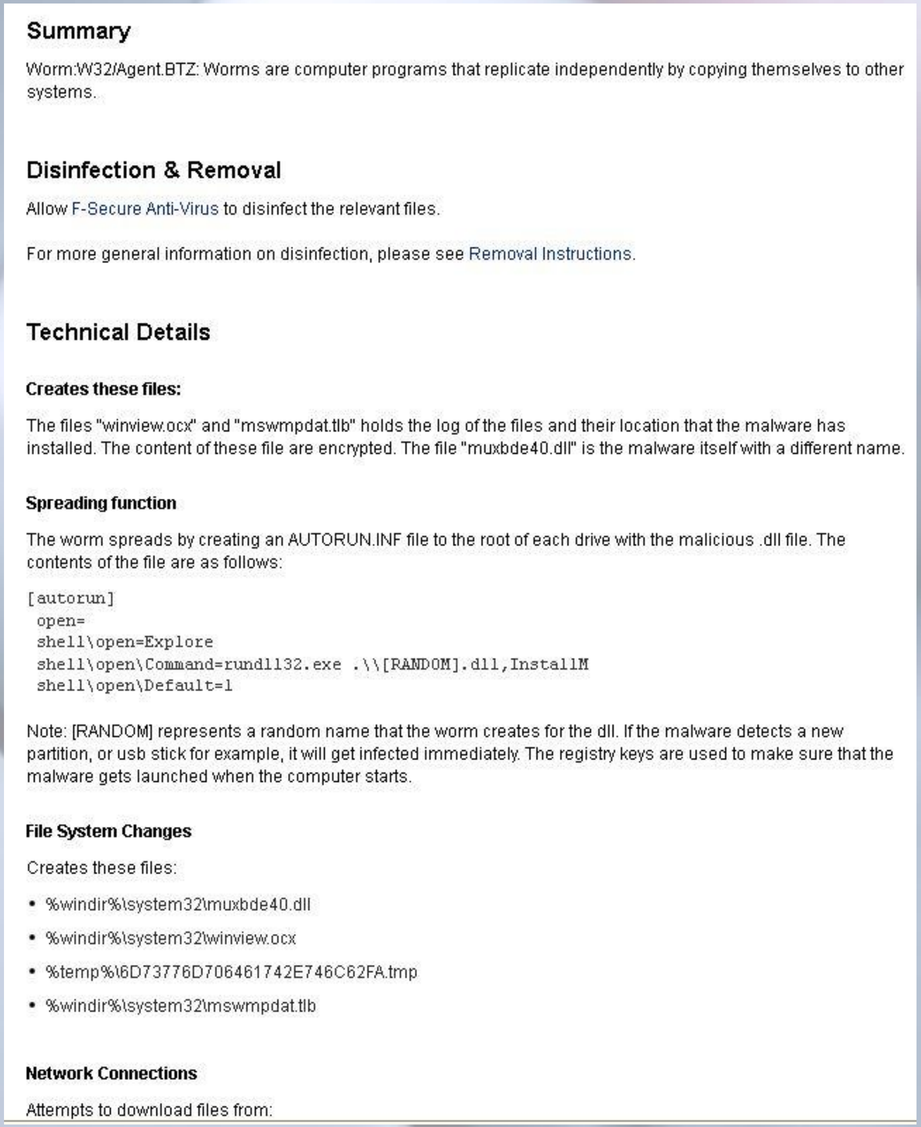
Detection

Based on the malware's operation, three of the possible ways to detect its network activity are: (1) detecting the transfer of encoded track data via SMB, (2) detecting attempted SMB writes to the drop location (\\<...>\c$\WINDOWS\twain_32), and (3) a combination of (1) and (2). Details of these detection strategies, including their corresponding OpenSignature rules are provided below.

(Thanks to Matthew Dobbs of IBM X-Force for converting the detection strategies to OpenSignature rules. These OpenSignature rules are compatible with the IBM Network IPS and third-party products that are OpenSignature-compatible).

- Hey X-Force… You have a tool called BigFix

Agent.BTZ – F-Secure



Summary

Worm:W32/Agent.BTZ: Worms are computer programs that replicate independently by copying themselves to other systems.

Disinfection & Removal

Allow F-Secure Anti-Virus to disinfect the relevant files.

For more general information on disinfection, please see Removal Instructions.

Technical Details

Creates these files:

The files "winview.ocx" and "mswmpdat.tlb" holds the log of the files and their location that the malware has installed. The content of these file are encrypted. The file "muxbde40.dll" is the malware itself with a different name.

Spreading function

The worm spreads by creating an AUTORUN.INF file to the root of each drive with the malicious .dll file. The contents of the file are as follows:

```
[autorun]
 open=
 shell\open=Explore
 shell\open\Command=rundll32.exe .\\[RANDOM].dll,InstallM
 shell\open\Default=1
```

Note: [RANDOM] represents a random name that the worm creates for the dll. If the malware detects a new partition, or usb stick for example, it will get infected immediately. The registry keys are used to make sure that the malware gets launched when the computer starts.

File System Changes

Creates these files:

- %windir%\system32\muxbde40.dll
- %windir%\system32\winview.ocx
- %temp%\6D73776D706461742E746C62FA.tmp
- %windir%\system32\mswmpdat.tlb

Network Connections

Attempts to download files from:

Urburos – G-Data

Uroburos

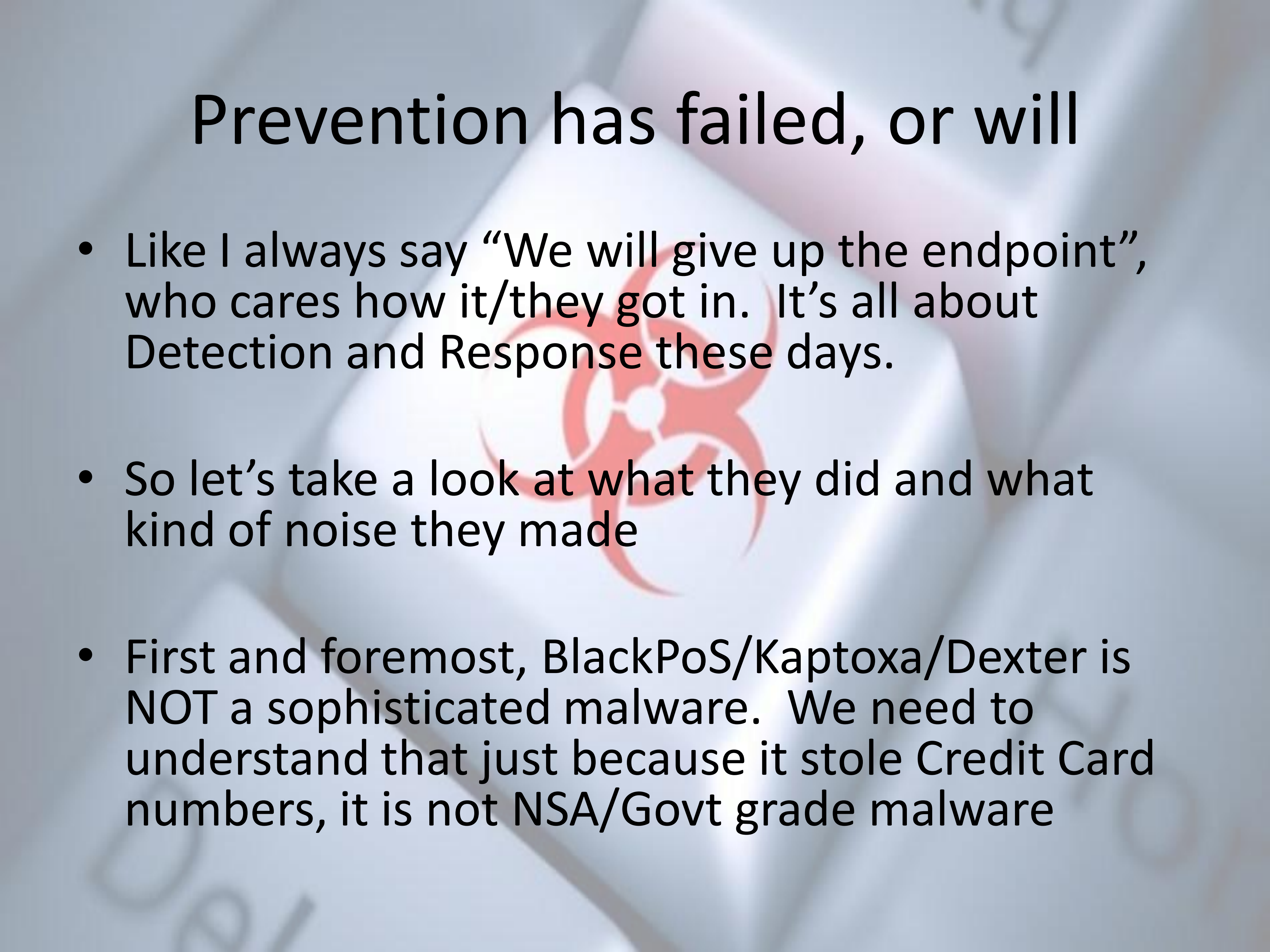
Highly complex espionage software with Russian roots

G Data discovers alleged intelligence agency software

G Data SecurityLabs

Contact:
intelligence@gdata.de

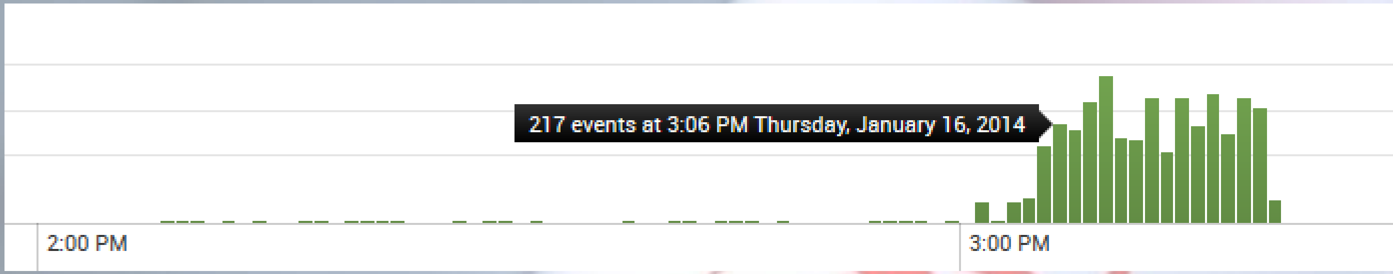
G Data. Security Made in Germany.

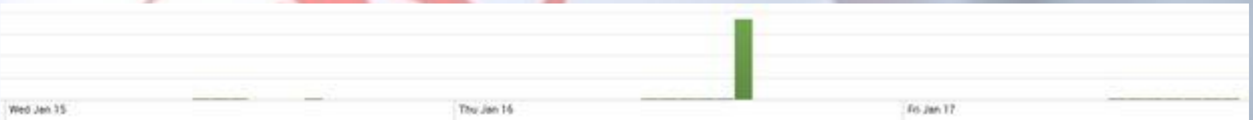


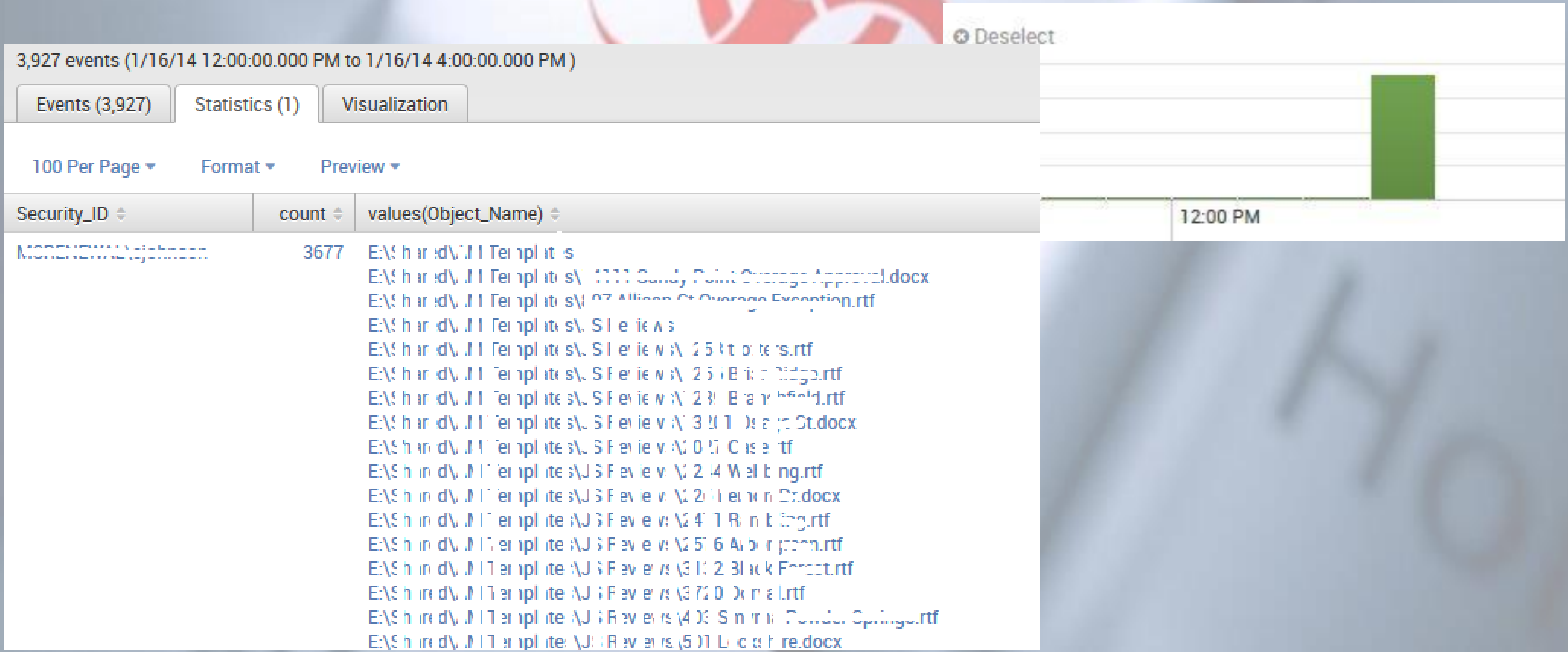
Prevention has failed, or will

- Like I always say "We will give up the endpoint", who cares how it/they got in. It's all about Detection and Response these days.
- So let's take a look at what they did and what kind of noise they made
- First and foremost, BlackPoS/Kaptoxa/Dexter is NOT a sophisticated malware. We need to understand that just because it stole Credit Card numbers, it is not NSA/Govt grade malware

You could catch CryptoLocker



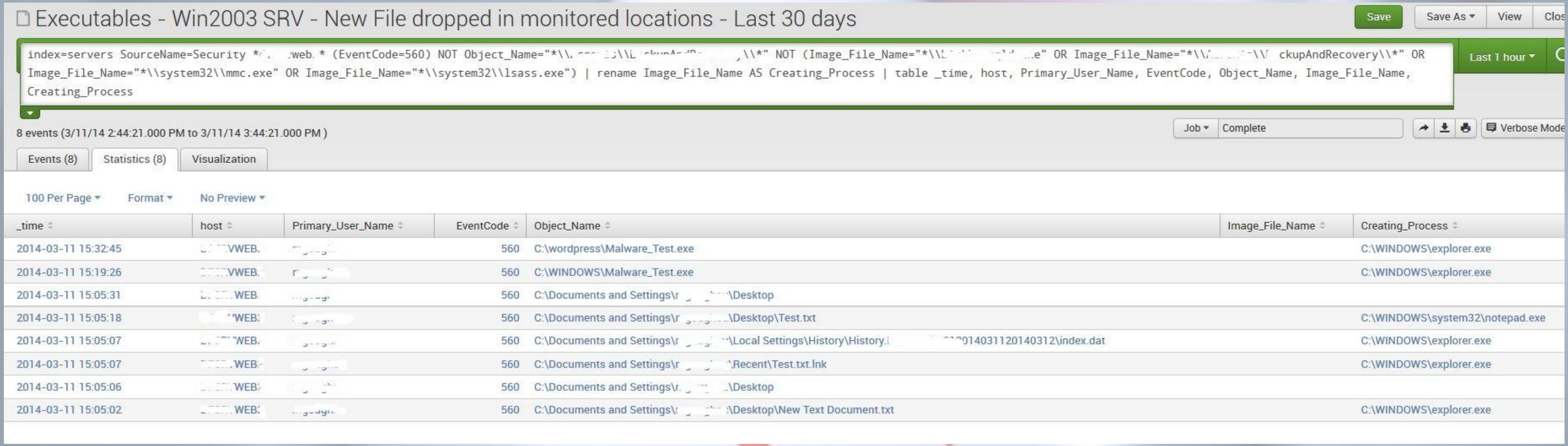




3,927 events (1/16/14 12:00:00.000 PM to 1/16/14 4:00:00.000 PM)

Security_ID	count	values(Object_Name)
MSRENEWAL\sjohnson	3677	E:\Shared\[illegible] Templates E:\Shared\[illegible] Templates\[illegible] Sandy Point Overage Approval.docx E:\Shared\[illegible] Templates\[illegible]07 Allison Ct Overage Exception.rtf E:\Shared\[illegible] Templates\[illegible] Reviews E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 25[illegible] [illegible]rs.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 25[illegible] [illegible] Ridge.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 23[illegible] Bra[illegible]field.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 3[illegible] [illegible] St.docx E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 0[illegible] Case[illegible]tf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 2[illegible]4 Wal[illegible]ng.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 2[illegible] [illegible] Dr.docx E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 24[illegible] 1 R[illegible]ing.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 25[illegible] 6 Ar[illegible]green.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 3[illegible] 2 Black Forest.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 3720 [illegible]l.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 40[illegible] S[illegible] Powder Springs.rtf E:\Shared\[illegible] Templates\[illegible] Reviews\[illegible] 50[illegible] L[illegible]re.docx

You can catch Malwarians



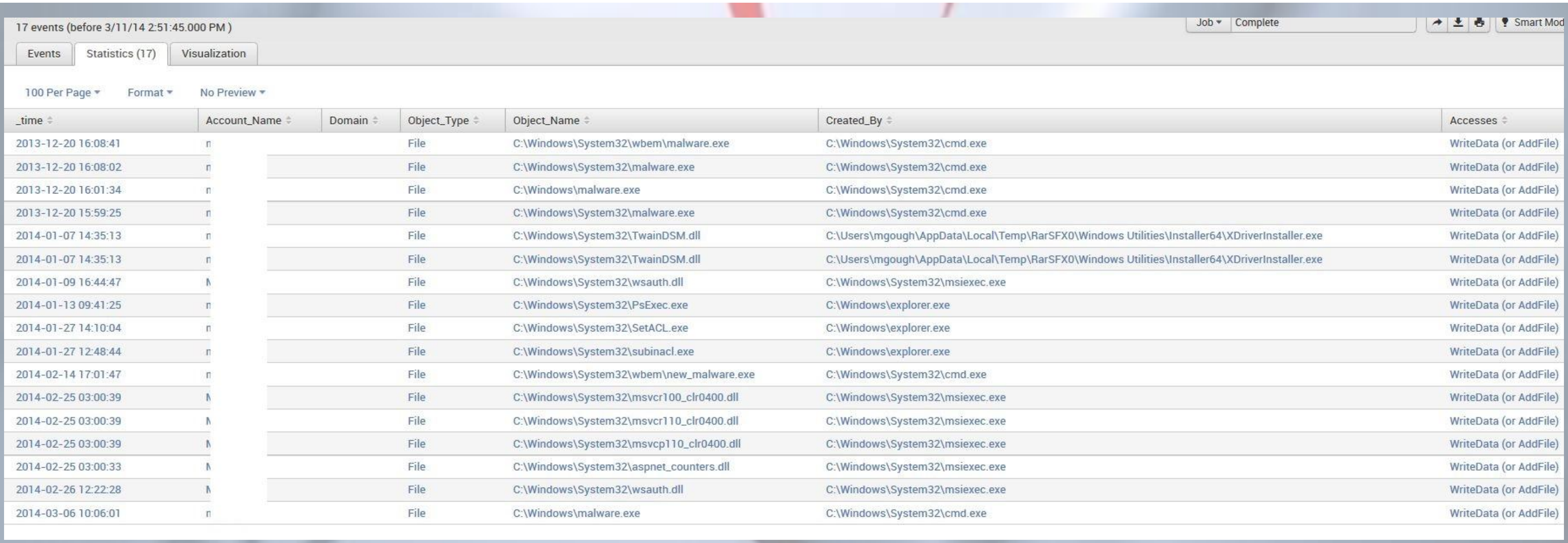
Executables - Win2003 SRV - New File dropped in monitored locations - Last 30 days

```
index=servers SourceName=Security *[redacted]web[redacted]* (EventCode=560) NOT Object_Name="*\\[redacted]\\[redacted]\\*" NOT (Image_File_Name="*\\[redacted]e" OR Image_File_Name="*\\[redacted]\\[redacted]ckupAndRecovery\\*" OR
Image_File_Name="*\\system32\\mmc.exe" OR Image_File_Name="*\\system32\\lsass.exe") | rename Image_File_Name AS Creating_Process | table _time, host, Primary_User_Name, EventCode, Object_Name, Image_File_Name,
Creating_Process
```

8 events (3/11/14 2:44:21.000 PM to 3/11/14 3:44:21.000 PM)

Complete

_time	host	Primary_User_Name	EventCode	Object_Name	Image_File_Name	Creating_Process
2014-03-11 15:32:45	[redacted]VWEB.[redacted]	[redacted]	560	C:\wordpress\Malware_Test.exe		C:\WINDOWS\explorer.exe
2014-03-11 15:19:26	[redacted]VWEB.[redacted]	[redacted]	560	C:\WINDOWS\Malware_Test.exe		C:\WINDOWS\explorer.exe
2014-03-11 15:05:31	[redacted]WEB.[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Desktop		
2014-03-11 15:05:18	[redacted]WEB[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Desktop\Test.txt		C:\WINDOWS\system32\notepad.exe
2014-03-11 15:05:07	[redacted]WEB.[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Local Settings\History\History.[redacted]014031120140312\index.dat		C:\WINDOWS\explorer.exe
2014-03-11 15:05:07	[redacted].WEB[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Recent\Test.txt.lnk		C:\WINDOWS\explorer.exe
2014-03-11 15:05:06	[redacted]WEB[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Desktop		
2014-03-11 15:05:02	[redacted]WEB[redacted]	[redacted]	560	C:\Documents and Settings\[redacted]\Desktop\New Text Document.txt		C:\WINDOWS\explorer.exe

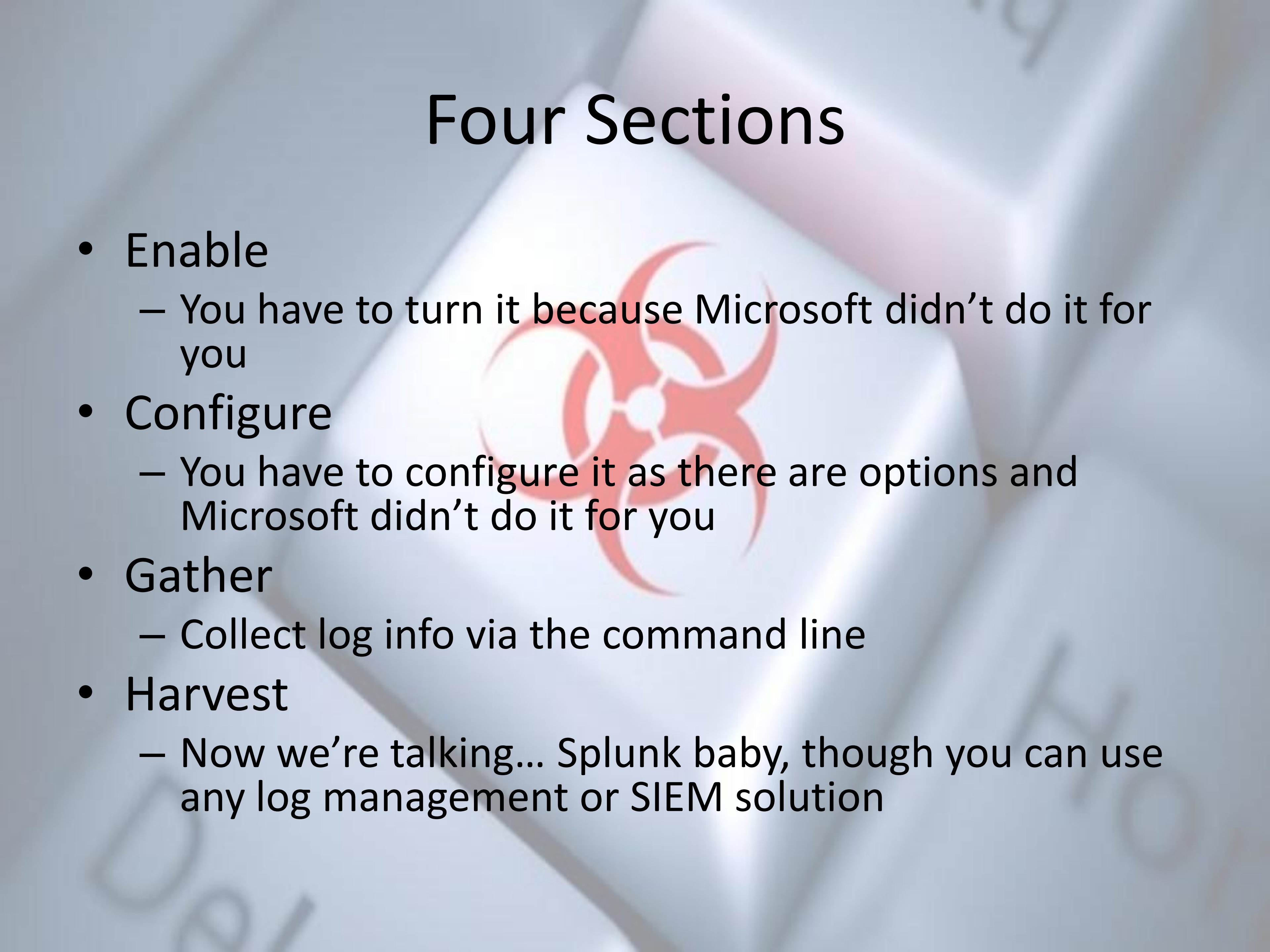


17 events (before 3/11/14 2:51:45.000 PM)

Complete

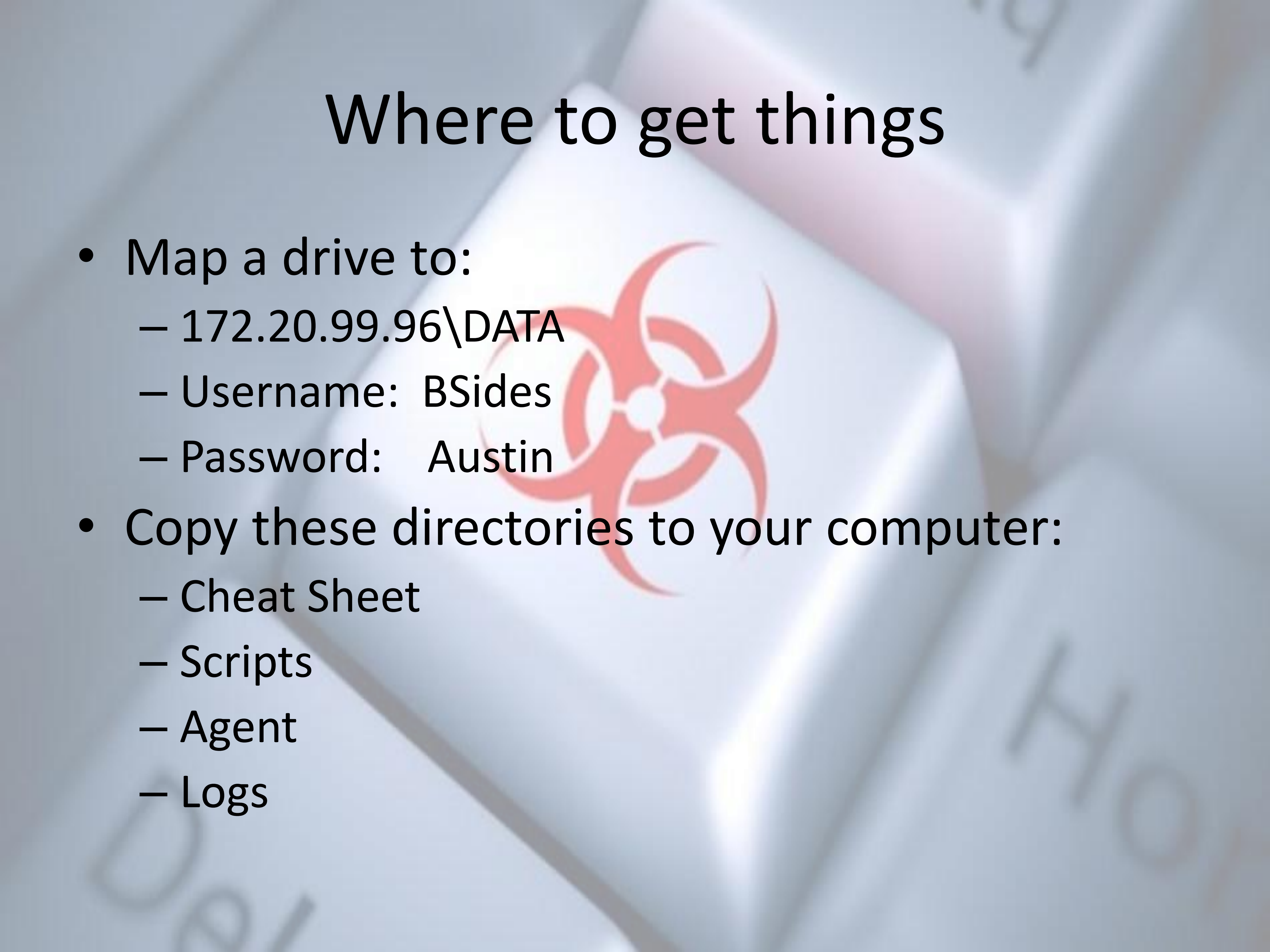
_time	Account_Name	Domain	Object_Type	Object_Name	Created_By	Accesses
2013-12-20 16:08:41	n[redacted]		File	C:\Windows\System32\wbem\malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)
2013-12-20 16:08:02	n[redacted]		File	C:\Windows\System32\malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)
2013-12-20 16:01:34	n[redacted]		File	C:\Windows\malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)
2013-12-20 15:59:25	n[redacted]		File	C:\Windows\System32\malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)
2014-01-07 14:35:13	n[redacted]		File	C:\Windows\System32\TwainDSM.dll	C:\Users\mgough\AppData\Local\Temp\RarSFX0\Windows Utilities\Installer64\XDriverInstaller.exe	WriteData (or AddFile)
2014-01-07 14:35:13	n[redacted]		File	C:\Windows\System32\TwainDSM.dll	C:\Users\mgough\AppData\Local\Temp\RarSFX0\Windows Utilities\Installer64\XDriverInstaller.exe	WriteData (or AddFile)
2014-01-09 16:44:47	N[redacted]		File	C:\Windows\System32\wsauth.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-01-13 09:41:25	n[redacted]		File	C:\Windows\System32\PsExec.exe	C:\Windows\explorer.exe	WriteData (or AddFile)
2014-01-27 14:10:04	n[redacted]		File	C:\Windows\System32\SetACL.exe	C:\Windows\explorer.exe	WriteData (or AddFile)
2014-01-27 12:48:44	n[redacted]		File	C:\Windows\System32\subinacl.exe	C:\Windows\explorer.exe	WriteData (or AddFile)
2014-02-14 17:01:47	n[redacted]		File	C:\Windows\System32\wbem\new_malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)
2014-02-25 03:00:39	N[redacted]		File	C:\Windows\System32\msvcr100_clr0400.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-02-25 03:00:39	N[redacted]		File	C:\Windows\System32\msvcr110_clr0400.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-02-25 03:00:39	N[redacted]		File	C:\Windows\System32\msvcp110_clr0400.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-02-25 03:00:33	N[redacted]		File	C:\Windows\System32\aspnet_counters.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-02-26 12:22:28	N[redacted]		File	C:\Windows\System32\wsauth.dll	C:\Windows\System32\msiexec.exe	WriteData (or AddFile)
2014-03-06 10:06:01	n[redacted]		File	C:\Windows\malware.exe	C:\Windows\System32\cmd.exe	WriteData (or AddFile)

Windows Logging



Four Sections

- Enable
  - You have to turn it because Microsoft didn’t do it for you
- Configure
  - You have to configure it as there are options and Microsoft didn’t do it for you
- Gather
  - Collect log info via the command line
- Harvest
  - Now we’re talking… Splunk baby, though you can use any log management or SIEM solution



Where to get things

- Map a drive to:
  - 172.20.99.96\DATA
  - Username: BSides
  - Password: Austin
- Copy these directories to your computer:
  - Cheat Sheet
  - Scripts
  - Agent
  - Logs

- 1. If you did not sign up for the BSides Austin Conference, you will not be allowed to attend – Sorry, but this is how we pay for the room, strictly enforced - sorry.
- 2. You will need some type of Windows 7, Server 2008 or later Windows OS.
- 3. You will need to alter the Local Security Policy and Advanced Auditing of your Windows OS. So if it is a work issued laptop under Group Policy restrictions, ask your IT folks if they can remove them the day prior to the training. If not.. Read #4
- 4. If you are paranoid and do not want to alter your laptop settings then these are other options you can do. You are on your own for this step, no help will be provided.
- a. Dual Boot into a throw away Win 7/Server 2008/Server 2012 image All changes can be easily undone.
- b. Use VMWare of Virtual Box to build a VM and use that
- c. Create an Amazon AWS Account and use their FREE Windows Server 2008/2012 option and RDP into that system
- d. Of course you can use your regular system, we won’t break anything, you can uninstall the agent and reverse the settings that we will tweak. So take screen shots of what the settings are or use AuditPol to capture them before we tweak them. This step we will do in class.

- 5. We will be doing command line gathering as well and showing you tips and tricks as many do not have a Log Management solution. We will talk about other agents and Logging options.
- 6. If you have a MAC or Linux system – See #4 If you have a MAC or Linux system – See #4 Sign up for a Splunk Storm account (www.SplunkStorm.com). This is a FREE Cloud service from Splunk that we will be able to send your log data to so you can see how to use a real log management solution over the command line options we will do in class. I will be demonstrating what you can find in your logs using Splunk to make it easier to understand. Again, you can delete the Log data in Splunk Storm after the training, so no need to be paranoid on what your log data will contain.

- 7. Install the Splunk Universal Forwarder – Get your Splunk Storm Account 1st! you need a key. Use verions 5.x (splunkforwarder-5.0.X-163460-x64-release.msi) NOT the latest version 6.x. Splunk Storm has instructions on how to do this or wait for the class. We will walk through the agent install early on. You can find the Agent at:
- a. http://www.splunk.com/page/previous_releases
- b. How to install the agent - http://docs.splunk.com/Documentation/Storm/Storm/User/SetupauniversalforwarderonWindows

Splunk Storm

- You need an account to Harvest logs.
- Splunk Storm will be our SIM/SIEM/LMS

- If you don’t want to send your logs to the Cloud… then you will watch or go home early

- www.SplunkStorm.com

Let’s get the agent collecting

- Agent install
  - Launch the installer

- Pay attention to the server – This is for the Instructor, yours will vary
  - udp.h7vj-kx2k.data.splunkstorm.com
  - Port 48784

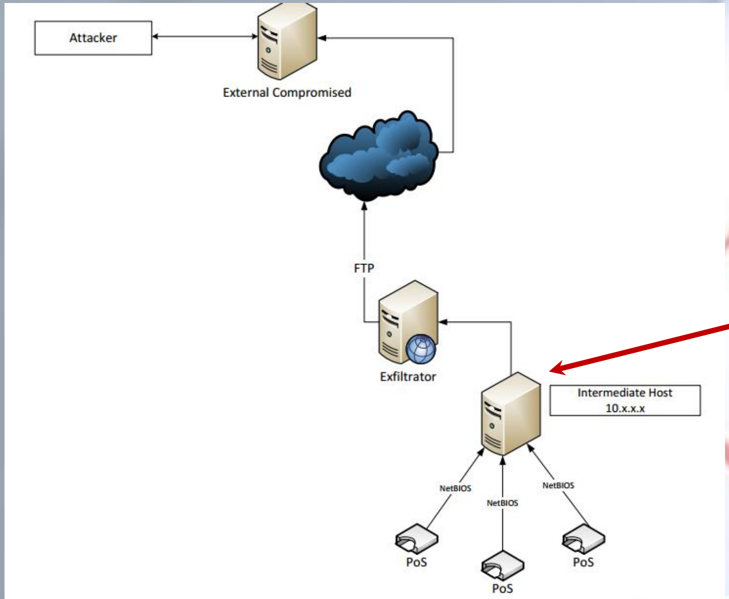
- In about 15 mins you should see some data
- We will check back.

Let’s get into it

- The Goal… What do I want you to learn?
- To Catch BlackPoS, Kaptoxa or Dexter
  - Stuxnet, Duqu, Flamer, WinNTI too

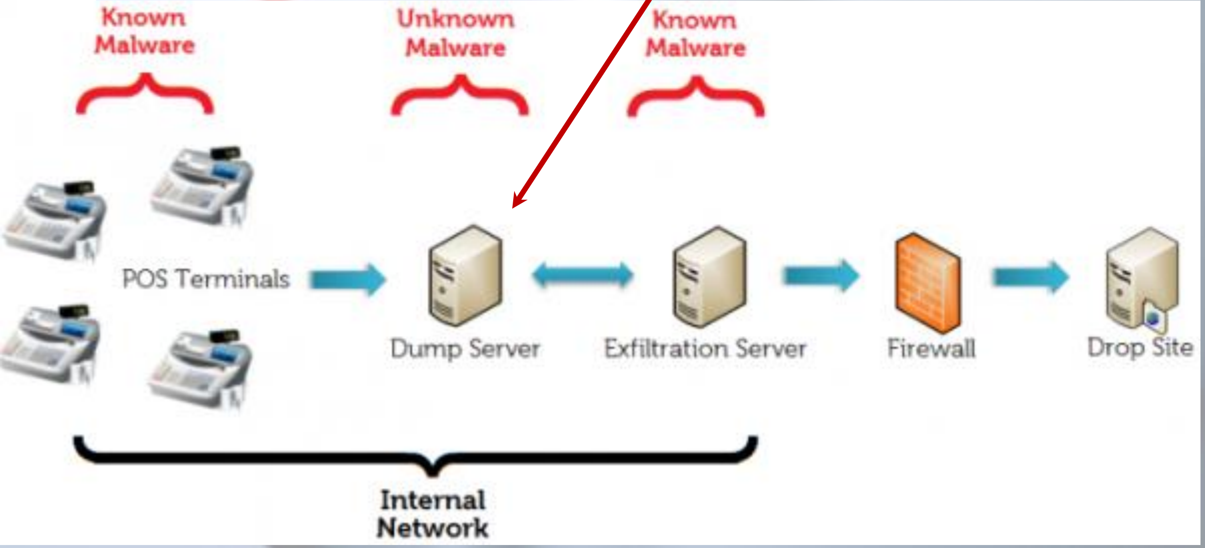
- Yes, yes you can
- It is/was NOT sophisticated malware like they would like you to believe, I have seen better

We need a Picture of a Network

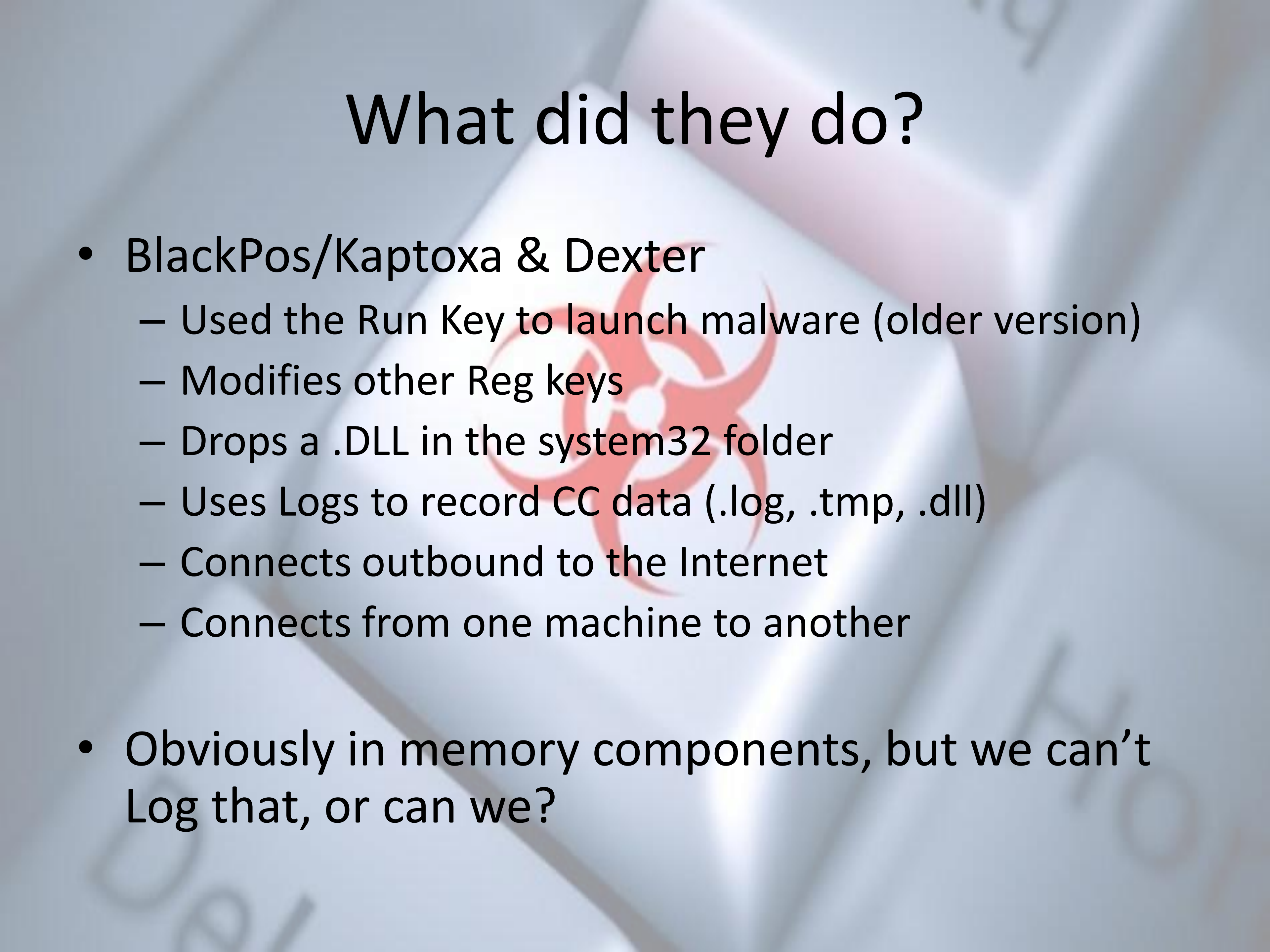


Patient 0

Where they jump from

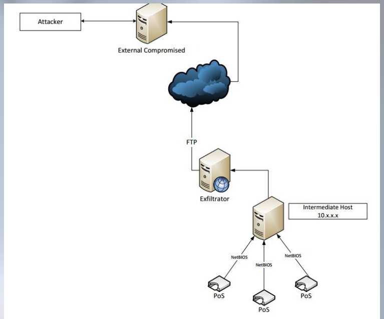


Network Diagrams from McAfee and Brian Krebs



What did they do?

- BlackPos/Kaptoxa & Dexter
  - Used the Run Key to launch malware (older version)
  - Modifies other Reg keys
  - Drops a .DLL in the system32 folder
  - Uses Logs to record CC data (.log, .tmp, .dll)
  - Connects outbound to the Internet
  - Connects from one machine to another
- Obviously in memory components, but we can’t Log that, or can we?



BlackPoS / Kaptoxa

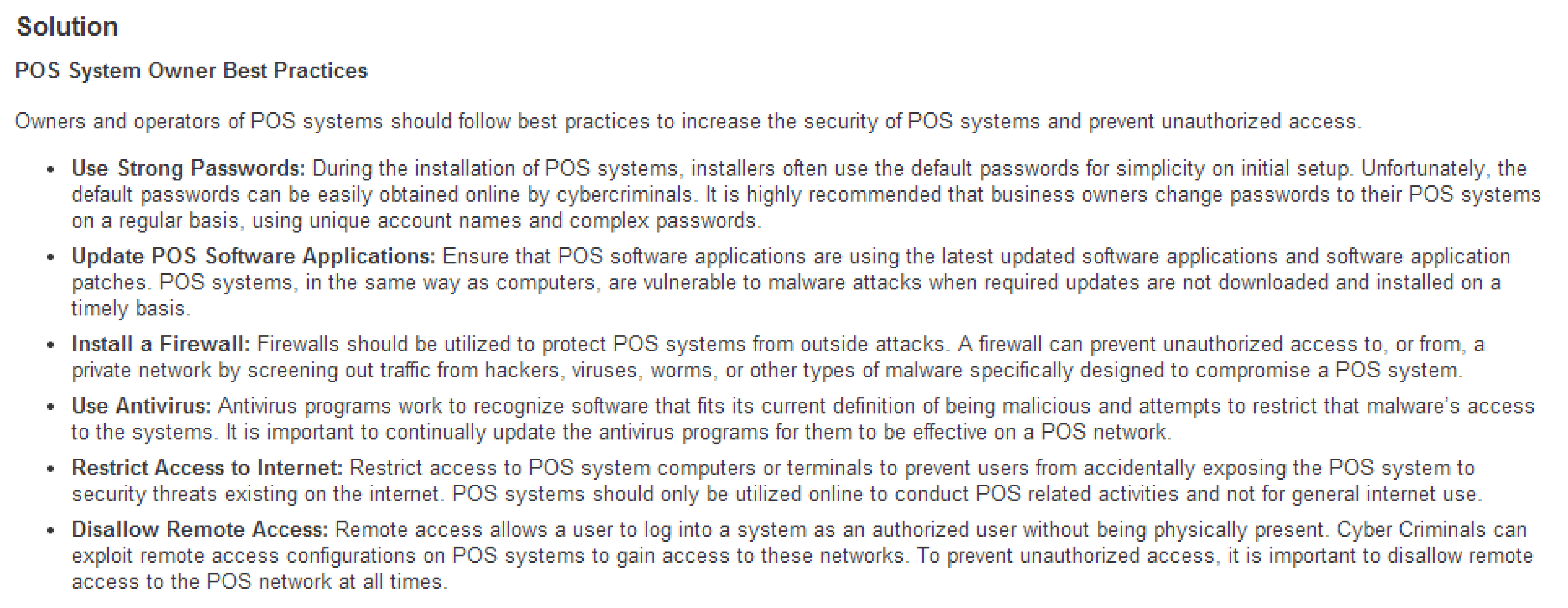
- Connects from Patient 0 to the PoS System
  - Share via Port 445
- Login with some account (Best1_user)
  - Network login Type 3
- Executed commands to infect
  - Cmd.exe, Net.exe, psexec, psexecsvc
- And the malware
  - Bladelogic.exe’ or ‘POSWDS.EXE’

BlackPoS / Kaptoxa

- Drops files
  - Msxml.dll – actually not a .DLL (CC Log file)
  - in C:\windows\system32, with the malware
- Logs
  - C:\windows\system32\Winxml.dll
- Collected Credit Card Logs
  - FTP.exe
  - C:\Windows\Twain_32 – Twain_32.dll
- In the end, this is a lot of noise and we can detect and respond to this information

US-CERT has the answer

- US-CERT – TA14-002A



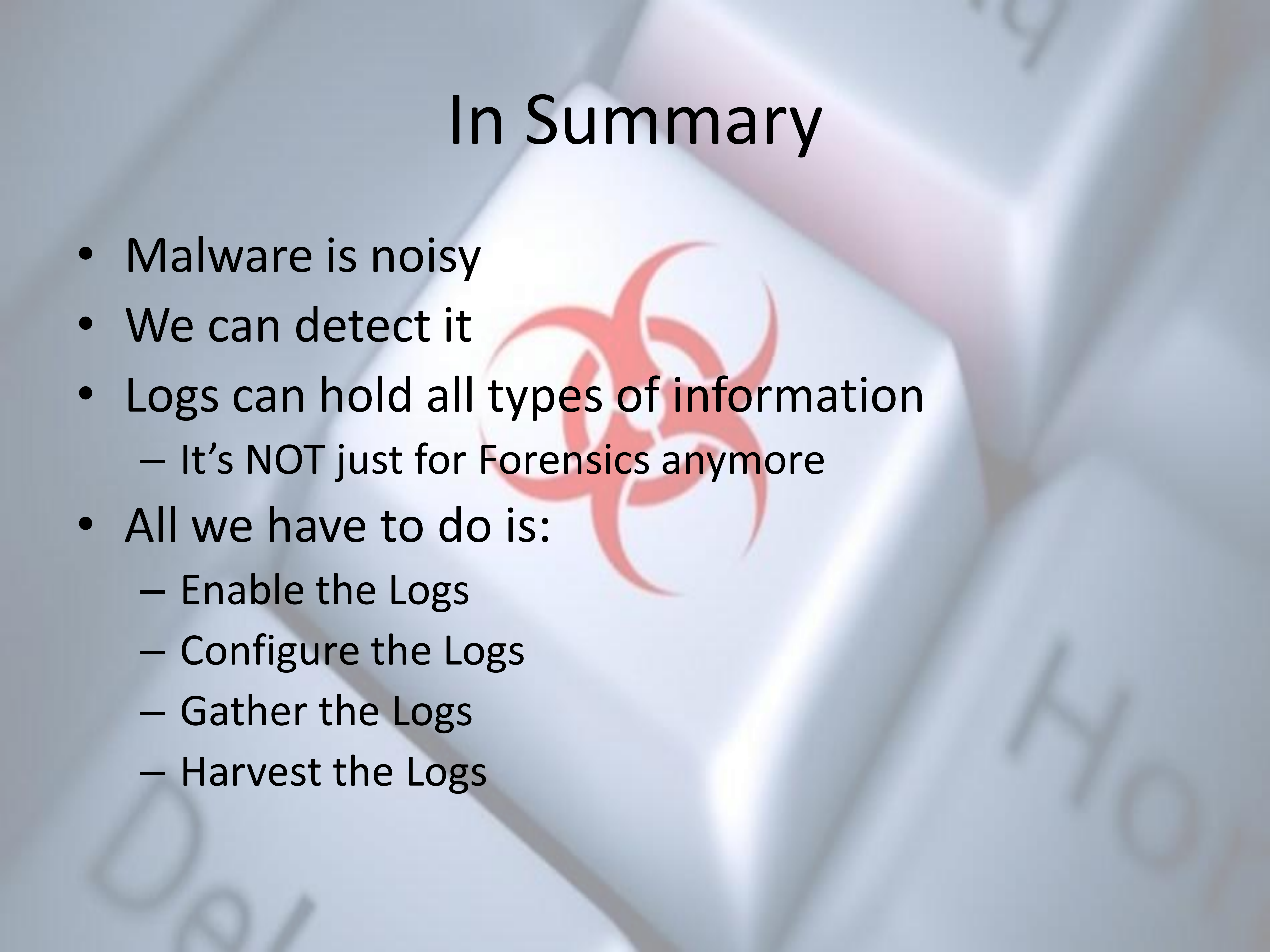
Solution

POS System Owner Best Practices

Owners and operators of POS systems should follow best practices to increase the security of POS systems and prevent unauthorized access.

- **Use Strong Passwords:** During the installation of POS systems, installers often use the default passwords for simplicity on initial setup. Unfortunately, the default passwords can be easily obtained online by cybercriminals. It is highly recommended that business owners change passwords to their POS systems on a regular basis, using unique account names and complex passwords.
- **Update POS Software Applications:** Ensure that POS software applications are using the latest updated software applications and software application patches. POS systems, in the same way as computers, are vulnerable to malware attacks when required updates are not downloaded and installed on a timely basis.
- **Install a Firewall:** Firewalls should be utilized to protect POS systems from outside attacks. A firewall can prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system.
- **Use Antivirus:** Antivirus programs work to recognize software that fits its current definition of being malicious and attempts to restrict that malware's access to the systems. It is important to continually update the antivirus programs for them to be effective on a POS network.
- **Restrict Access to Internet:** Restrict access to POS system computers or terminals to prevent users from accidentally exposing the POS system to security threats existing on the internet. POS systems should only be utilized online to conduct POS related activities and not for general internet use.
- **Disallow Remote Access:** Remote access allows a user to log into a system as an authorized user without being physically present. Cyber Criminals can exploit remote access configurations on POS systems to gain access to these networks. To prevent unauthorized access, it is important to disallow remote access to the POS network at all times.

- Anyone think this is a good solution?



In Summary

- Malware is noisy
- We can detect it
- Logs can hold all types of information
  - It’s NOT just for Forensics anymore
- All we have to do is:
  - Enable the Logs
  - Configure the Logs
  - Gather the Logs
  - Harvest the Logs

LOGGING OVERVIEW

Logging Overview

Log Management consists of these components

1. A system with logs
2. A Log agent
3. A Log collector
4. A Log Management solution
    1. Manual, Syslog
    2. Application
    3. SIEM

Local Logging

- Turn it on, disks are no where near full
- Systems are capable of a lot more than you think.
- It’s FUD to think you can’t enable local logging
- CPU’s are fast enough now
- If you are limited in space, use Syslog to send off the system (network devices, etc.)
- Syslog is a de-facto standard built into most everything. Use it

Logging Agents

*NIX

- syslog-ng
- rsyslog
- RELP
- OSSEC
- Splunk

UNIX®

Celebrating 40 years uptime

Logging Agents

Windows

- Syslog of course
- rsyslog server
- uberAgent for Splunk
- Snare
- Splunk Universal Forwarder
- NTsyslog
- nxlog
- syslog-ng for Windows
- OSSEC
- https://code.google.com/p/eventlog-to-syslog/
- PowerShell scripts

- Ready for something BRAND SPANKING new?

Introducing the…

Windows Logging Service

WLS

Log Management Solutions

- Way too many to cover
- But you know I love (Pssst – Look around)
- And we will get to play with it !
- FREE!!!!!

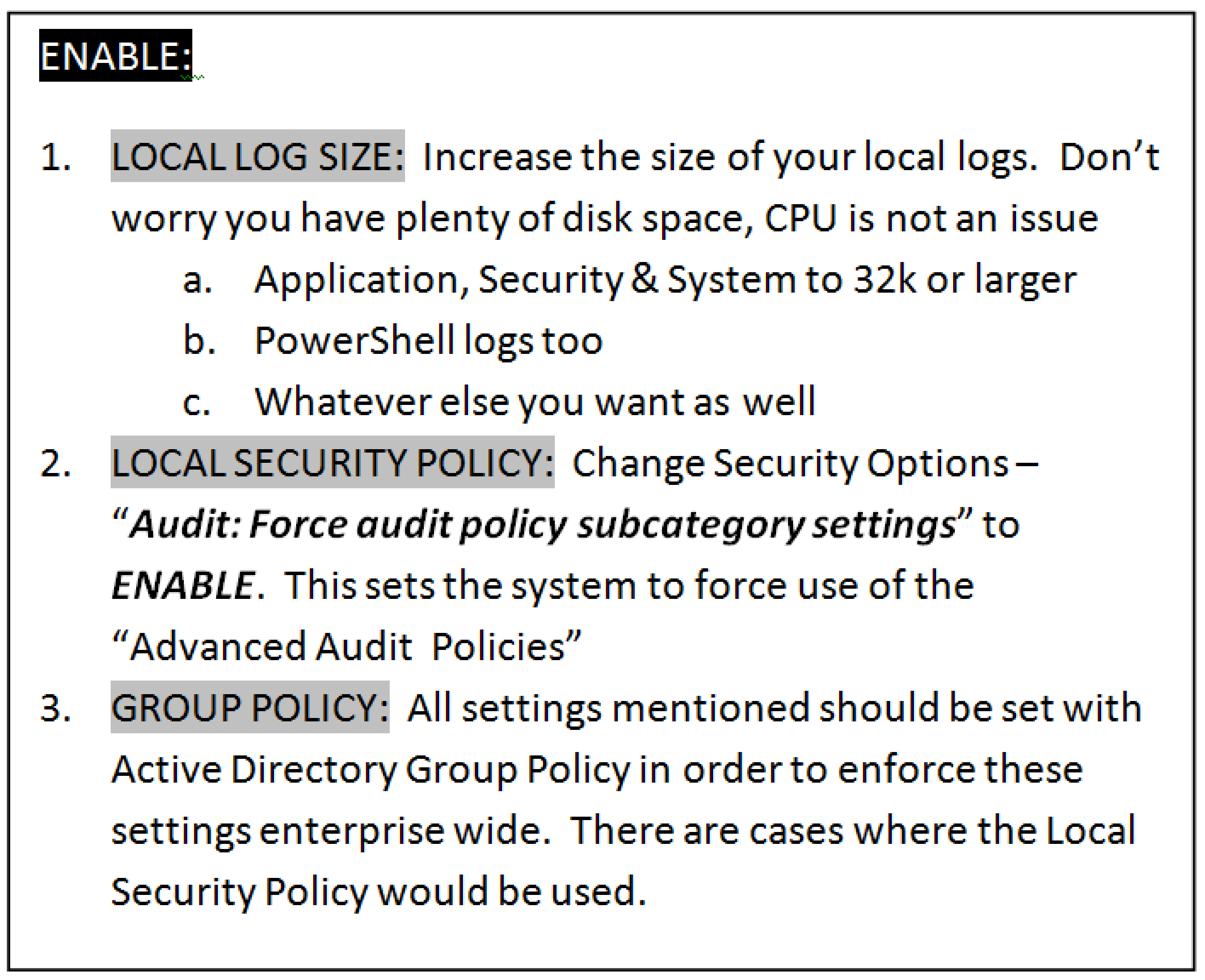
Get out your Cheat Sheets

ENABLE

Prepare

- Disk space !!!! Lots of it
  - Indexing will be your best friend
  - Meaning collect ONLY what you need, toss the rest
- Most likely you have big enough disks locally
  - Collect as much as you can
  - Windows will roll a Security log in 2 hours or less, minutes if you log Windows Firewall
- So where are the Windows Logs?
  - C:\Windows\System32\winevt\Logs

Enable



ENABLE:

1. LOCAL LOG SIZE: Increase the size of your local logs. Don’t worry you have plenty of disk space, CPU is not an issue
   a. Application, Security & System to 32k or larger
   b. PowerShell logs too
   c. Whatever else you want as well
2. LOCAL SECURITY POLICY: Change Security Options – “***Audit: Force audit policy subcategory settings***” to ***ENABLE***. This sets the system to force use of the “Advanced Audit Policies”
3. GROUP POLICY: All settings mentioned should be set with Active Directory Group Policy in order to enforce these settings enterprise wide. There are cases where the Local Security Policy would be used.

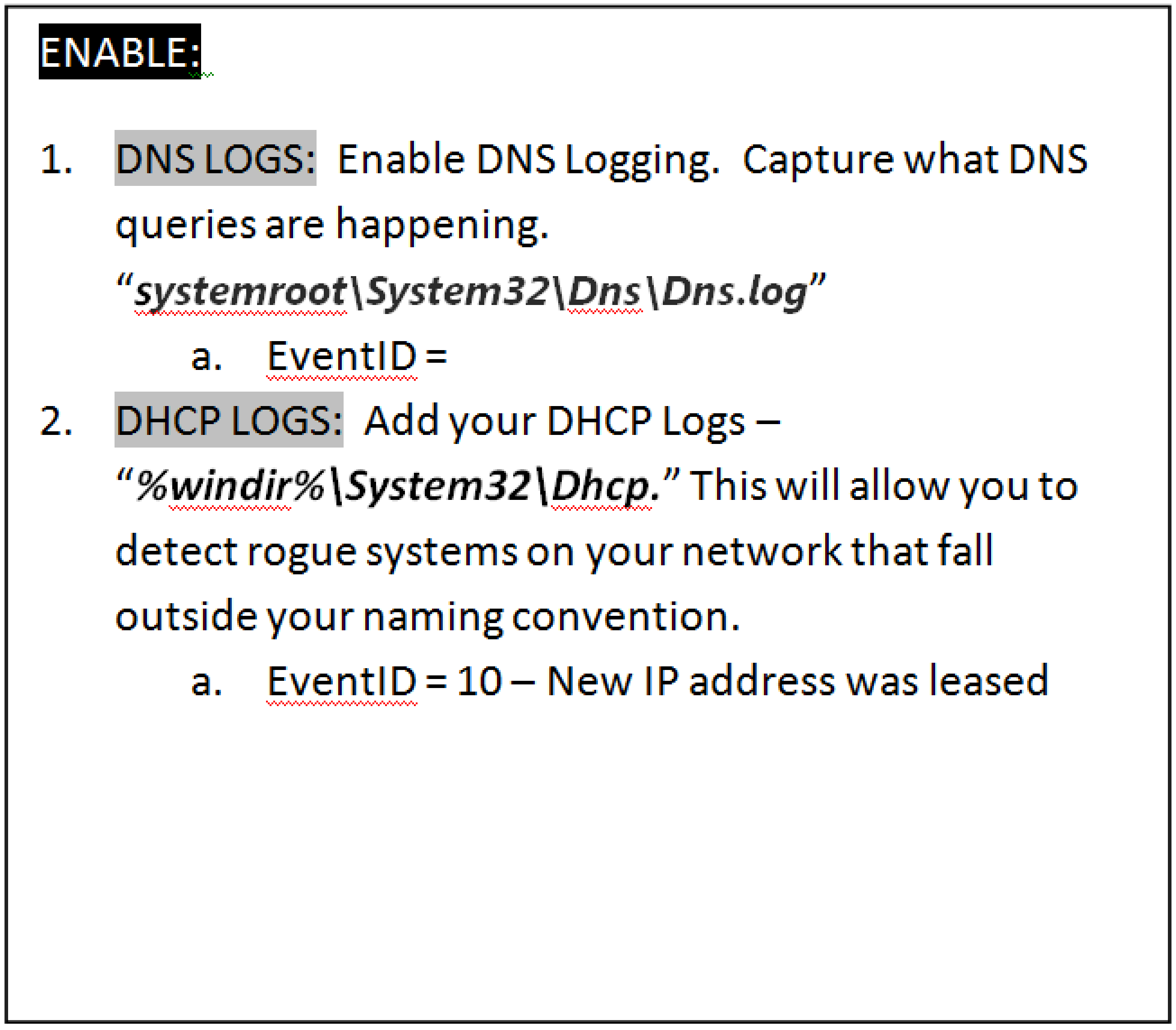
Let’s change some settings

- Open Event Viewer and follow along

- Open up the Local Security

DNS & DHCP

Enable



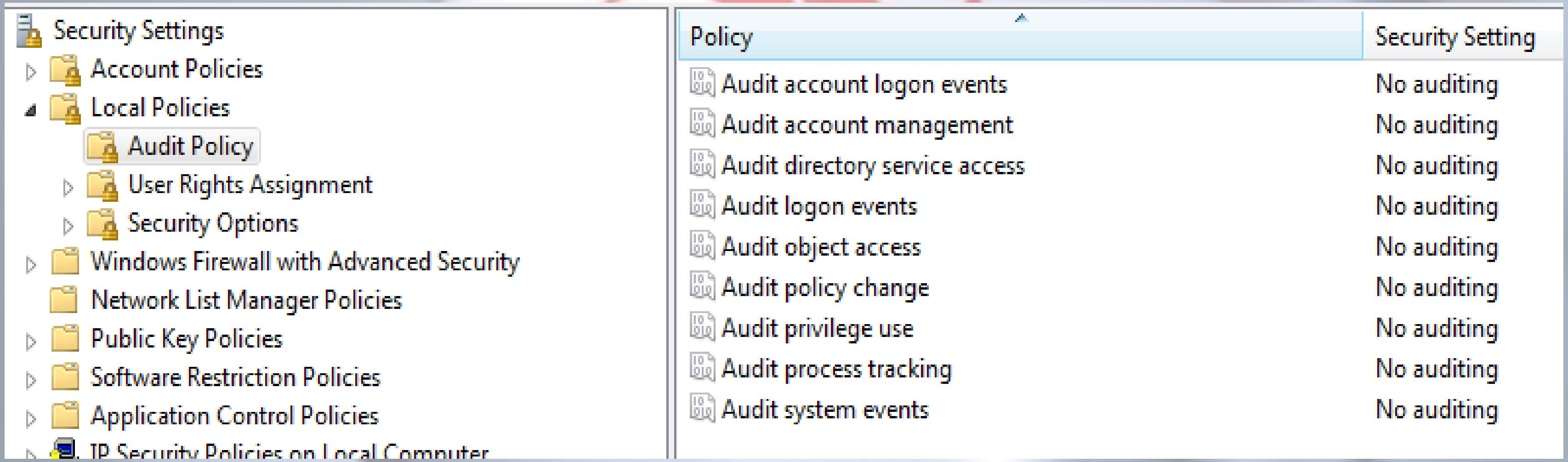
ENABLE:

1. DNS LOGS: Enable DNS Logging. Capture what DNS queries are happening. "*systemroot\System32\Dns\Dns.log*"
   a. EventID =
2. DHCP LOGS: Add your DHCP Logs – "*%windir%\System32\Dhcp.*" This will allow you to detect rogue systems on your network that fall outside your naming convention.
   a. EventID = 10 – New IP address was leased

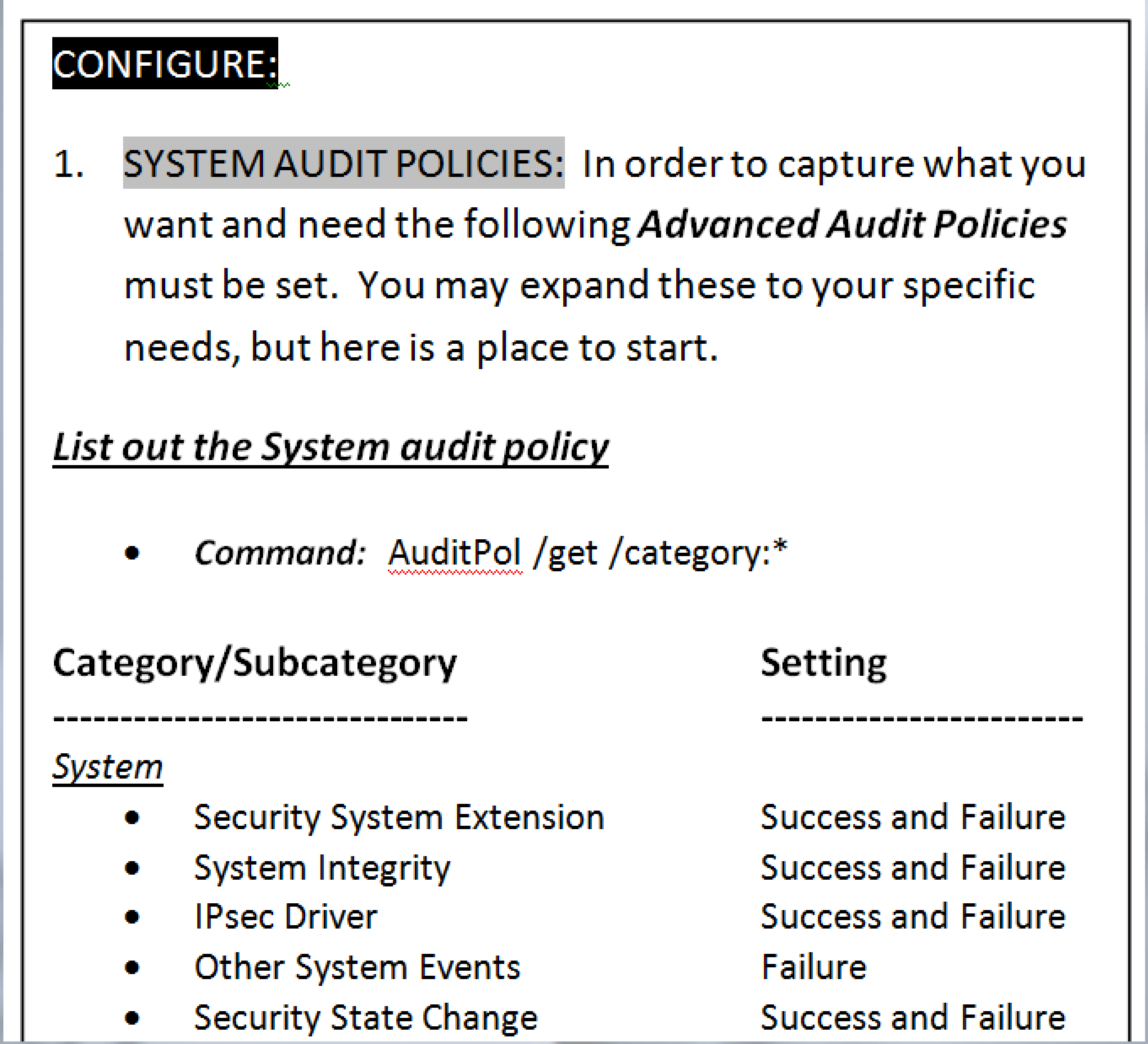
CONFIGURE

Did I say Windows SUCKS by default?

- Legacy Audit Settings


Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing



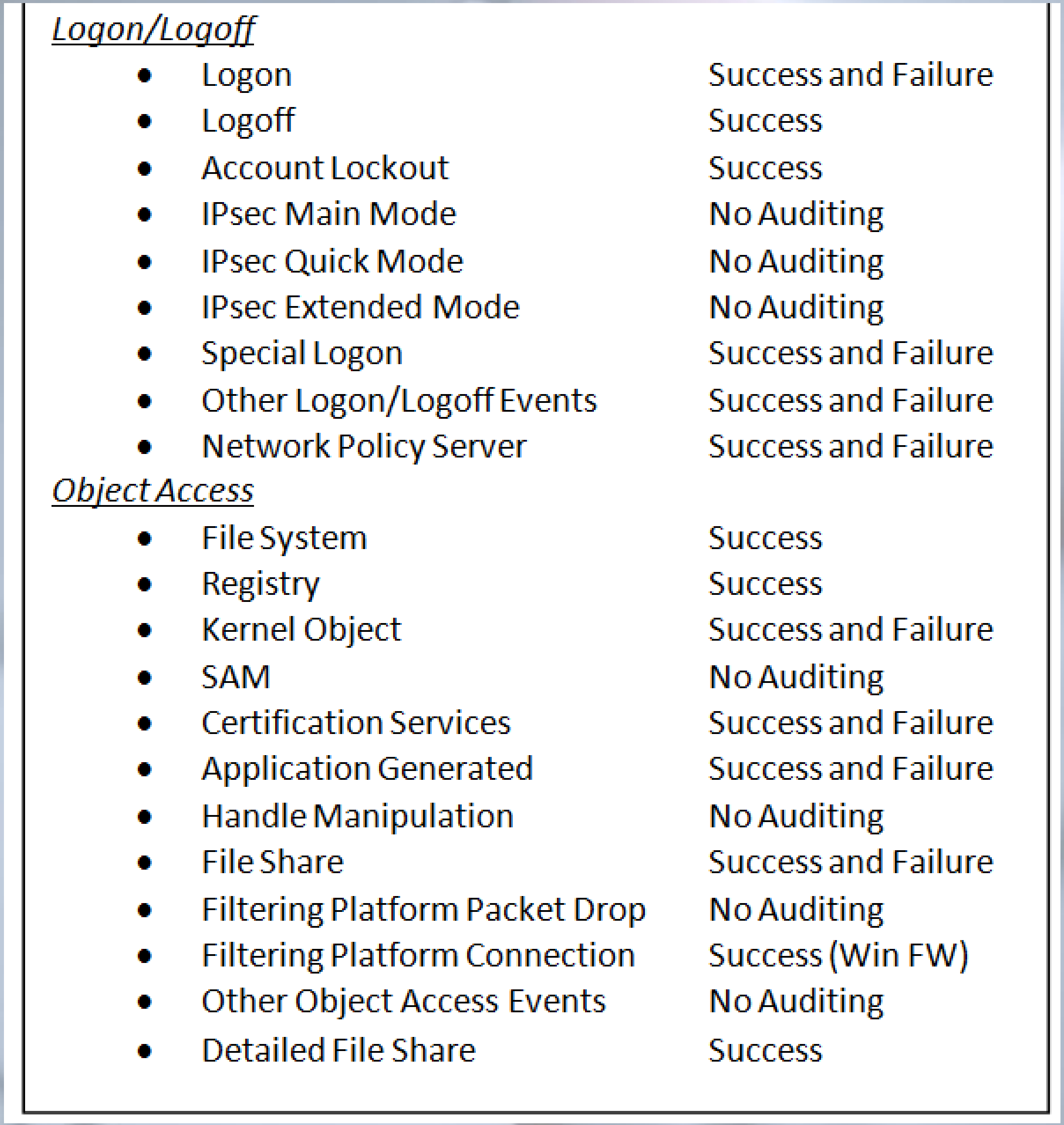
CONFIGURE:

1. SYSTEM AUDIT POLICIES: In order to capture what you want and need the following ***Advanced Audit Policies*** must be set. You may expand these to your specific needs, but here is a place to start.

List out the System audit policy

- ***Command:*** AuditPol /get /category:*

Category/Subcategory	**Setting**
System	
• Security System Extension	Success and Failure
• System Integrity	Success and Failure
• IPsec Driver	Success and Failure
• Other System Events	Failure
• Security State Change	Success and Failure

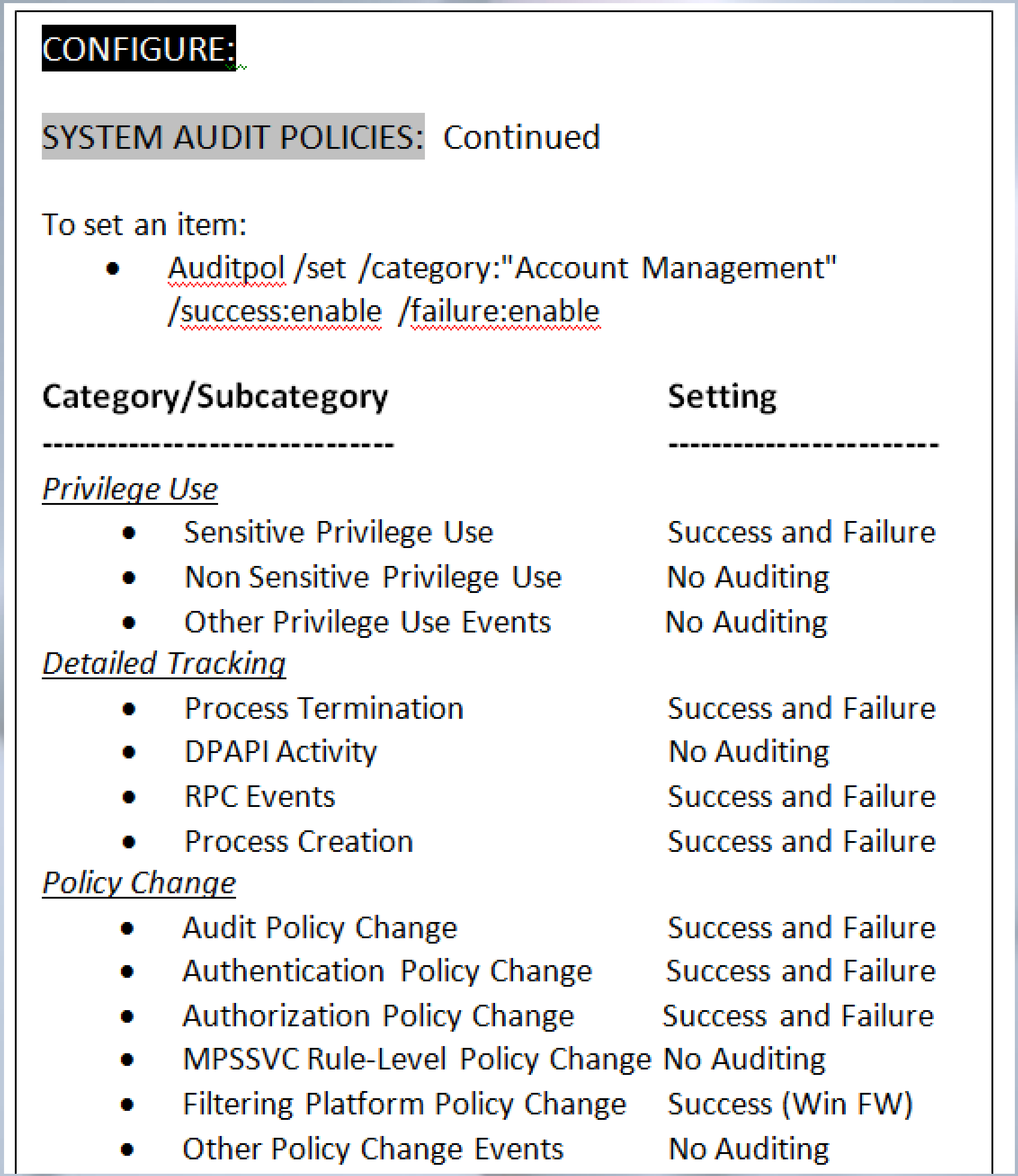


Logon/Logoff

Logon	Success and Failure
Logoff	Success
Account Lockout	Success
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success and Failure
Other Logon/Logoff Events	Success and Failure
Network Policy Server	Success and Failure

Object Access

File System	Success
Registry	Success
Kernel Object	Success and Failure
SAM	No Auditing
Certification Services	Success and Failure
Application Generated	Success and Failure
Handle Manipulation	No Auditing
File Share	Success and Failure
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	Success (Win FW)
Other Object Access Events	No Auditing
Detailed File Share	Success



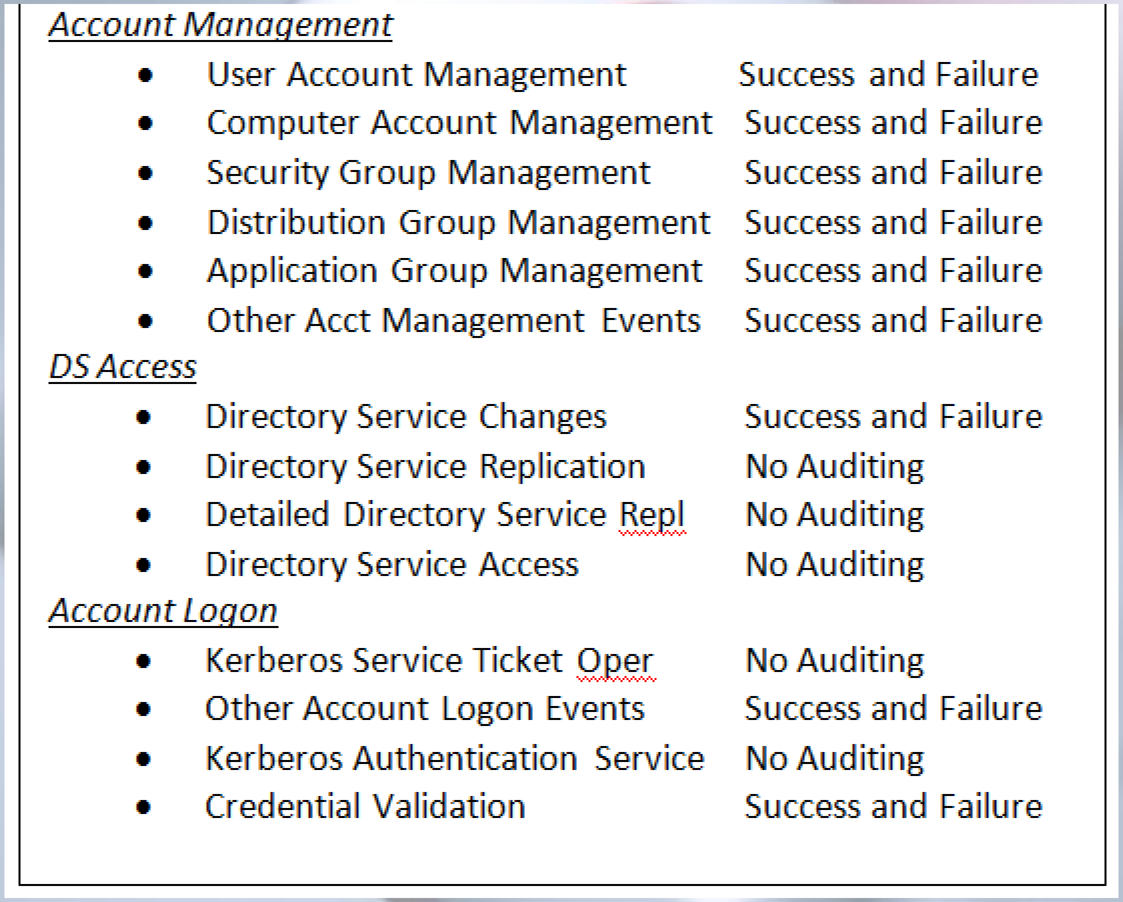
CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

To set an item:

-
  ```
  Auditpol /set /category:"Account Management"
  /success:enable /failure:enable
  ```

Category/Subcategory	Setting
Privilege Use	
• Sensitive Privilege Use	Success and Failure
• Non Sensitive Privilege Use	No Auditing
• Other Privilege Use Events	No Auditing
Detailed Tracking	
• Process Termination	Success and Failure
• DPAPI Activity	No Auditing
• RPC Events	Success and Failure
• Process Creation	Success and Failure
Policy Change	
• Audit Policy Change	Success and Failure
• Authentication Policy Change	Success and Failure
• Authorization Policy Change	Success and Failure
• MPSSVC Rule-Level Policy Change	No Auditing
• Filtering Platform Policy Change	Success (Win FW)
• Other Policy Change Events	No Auditing



Account Management

User Account Management	Success and Failure
Computer Account Management	Success and Failure
Security Group Management	Success and Failure
Distribution Group Management	Success and Failure
Application Group Management	Success and Failure
Other Acct Management Events	Success and Failure

DS Access

Directory Service Changes	Success and Failure
Directory Service Replication	No Auditing
Detailed Directory Service Repl	No Auditing
Directory Service Access	No Auditing

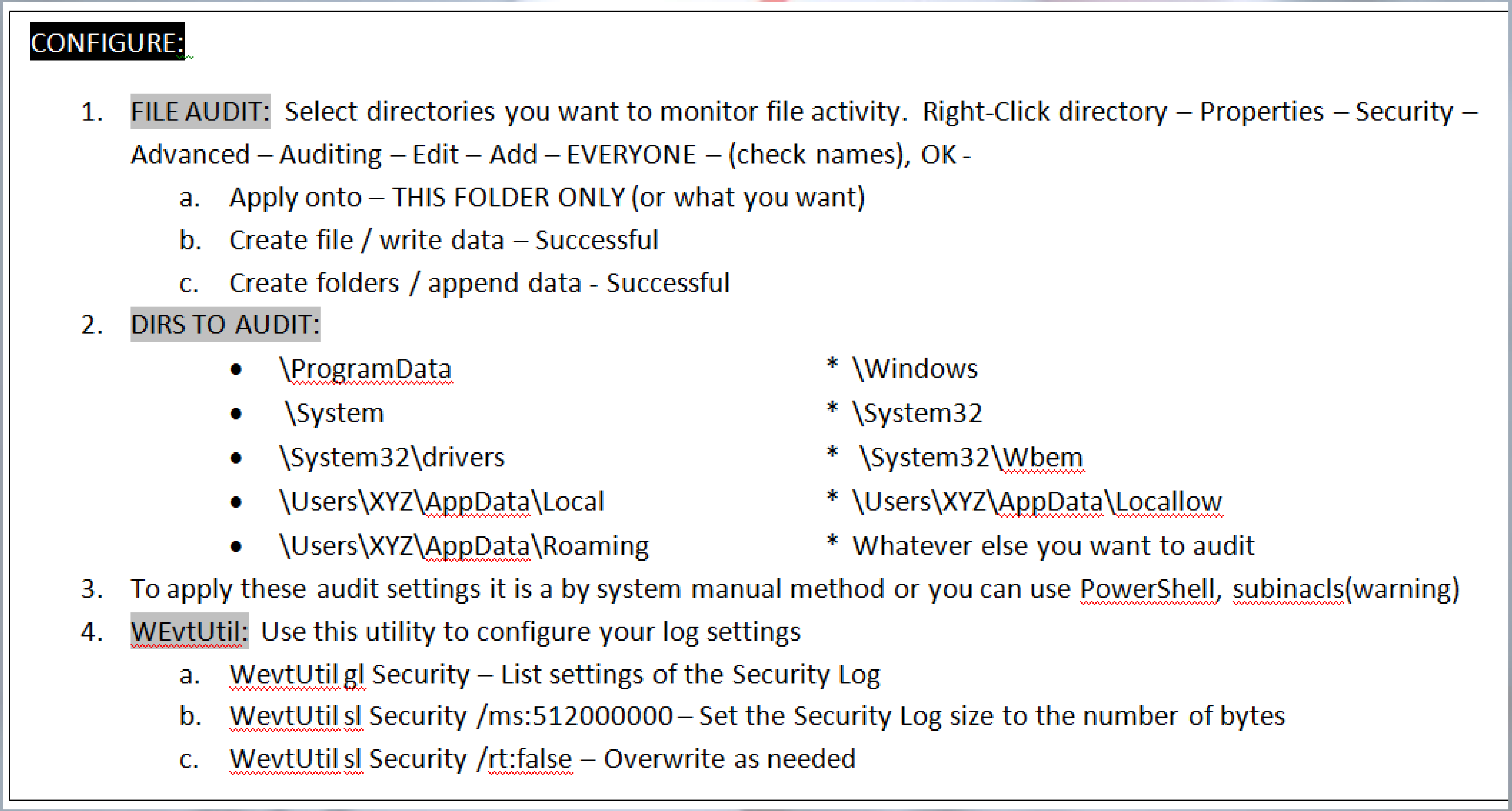
Account Logon

Kerberos Service Ticket Oper	No Auditing
Other Account Logon Events	Success and Failure
Kerberos Authentication Service	No Auditing
Credential Validation	Success and Failure

AuditPol

- I have a script for you…
- Data\Scripts
  - Set_Audit_Pol.cmd
- Open it up and take a look
- Adjust as necessary

File Auditing



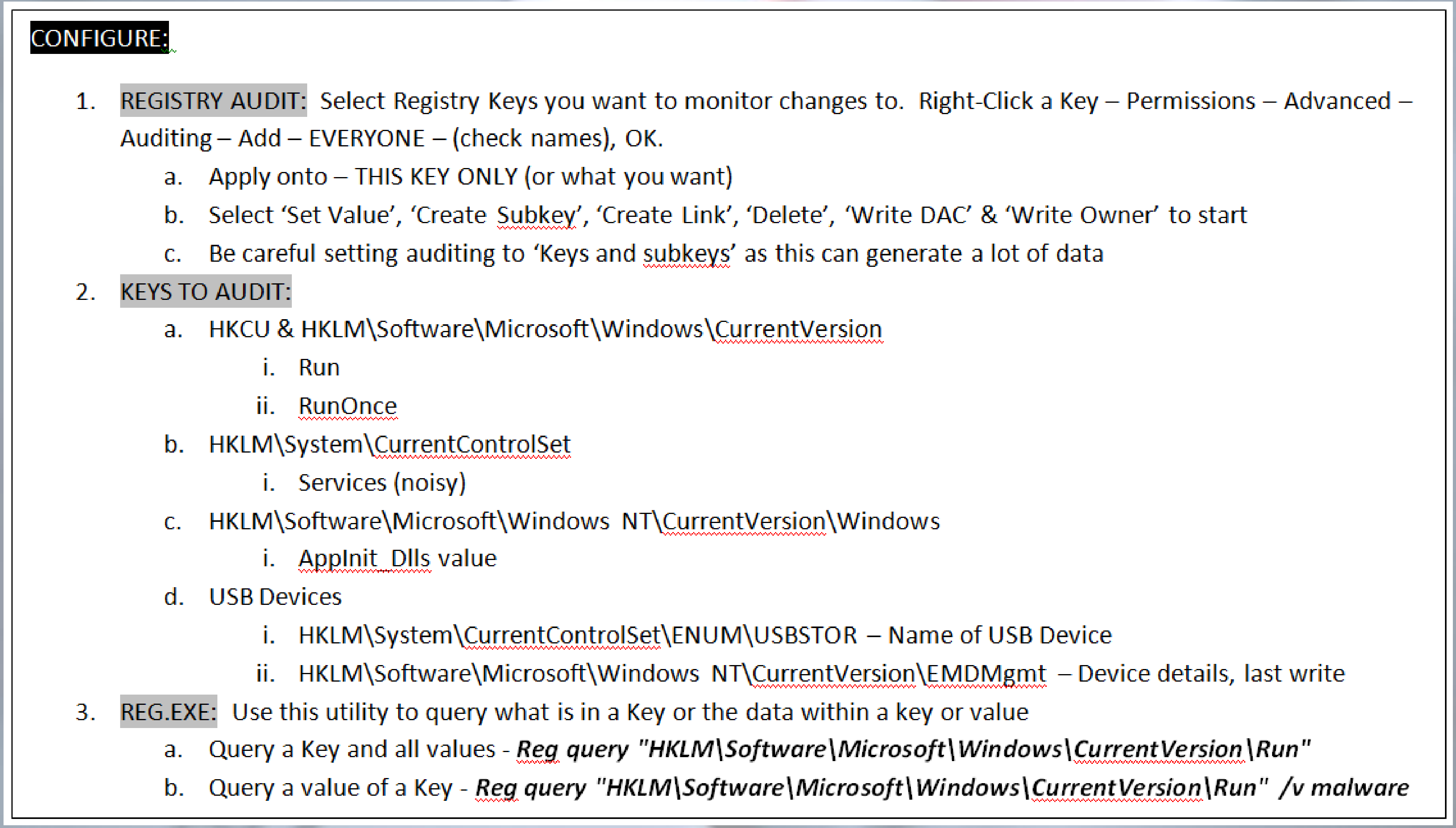
CONFIGURE:

1. FILE AUDIT: Select directories you want to monitor file activity. Right-Click directory – Properties – Security – Advanced – Auditing – Edit – Add – EVERYONE – (check names), OK -
    a. Apply onto – THIS FOLDER ONLY (or what you want)
    b. Create file / write data – Successful
    c. Create folders / append data - Successful
2. DIRS TO AUDIT:
    - \ProgramData
    - \System
    - \System32\drivers
    - \Users\XYZ\AppData\Local
    - \Users\XYZ\AppData\Roaming
    * \Windows
    * \System32
    * \System32\Wbem
    * \Users\XYZ\AppData\Locallow
    * Whatever else you want to audit
3. To apply these audit settings it is a by system manual method or you can use PowerShell, subinacls(warning)
4. WEvtUtil: Use this utility to configure your log settings
    a. WevtUtil gl Security – List settings of the Security Log
    b. WevtUtil sl Security /ms:512000000 – Set the Security Log size to the number of bytes
    c. WevtUtil sl Security /rt:false – Overwrite as needed

File Auditing

- Lets set some File Auditing
- Explorer…
- PowerShell command line
- Some Windows utilities

Registry Auditing



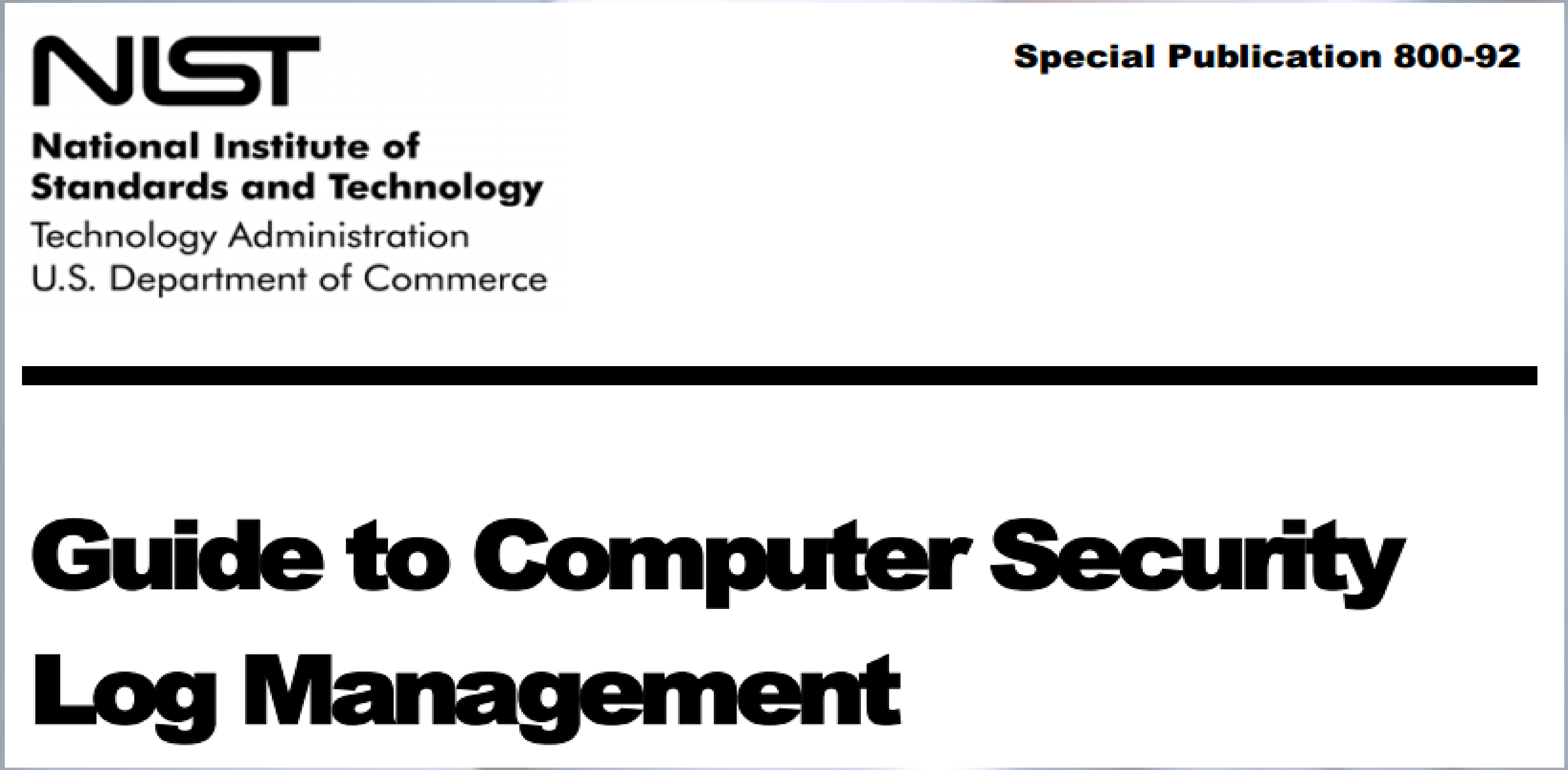
CONFIGURE:

1. REGISTRY AUDIT: Select Registry Keys you want to monitor changes to. Right-Click a Key – Permissions – Advanced – Auditing – Add – EVERYONE – (check names), OK.
   a. Apply onto – THIS KEY ONLY (or what you want)
   b. Select 'Set Value', 'Create Subkey', 'Create Link', 'Delete', 'Write DAC' & 'Write Owner' to start
   c. Be careful setting auditing to 'Keys and subkeys' as this can generate a lot of data
2. KEYS TO AUDIT:
   a. HKCU & HKLM\Software\Microsoft\Windows\CurrentVersion
      i. Run
      ii. RunOnce
   b. HKLM\System\CurrentControlSet
      i. Services (noisy)
   c. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows
      i. AppInit_Dlls value
   d. USB Devices
      i. HKLM\System\CurrentControlSet\ENUM\USBSTOR – Name of USB Device
      ii. HKLM\Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt – Device details, last write
3. REG.EXE: Use this utility to query what is in a Key or the data within a key or value
   a. Query a Key and all values - ***Reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"***
   b. Query a value of a Key - ***Reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v malware***

Registry Auditing

- Lets set some Registry Auditing
- RegEdt32…
- PowerShell command line
- Some Windows utilities

Like to read?



NIST

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-92

Guide to Computer Security Log Management

- Lacks the details we are now discussing

Legacy Windows (XP, 2003)

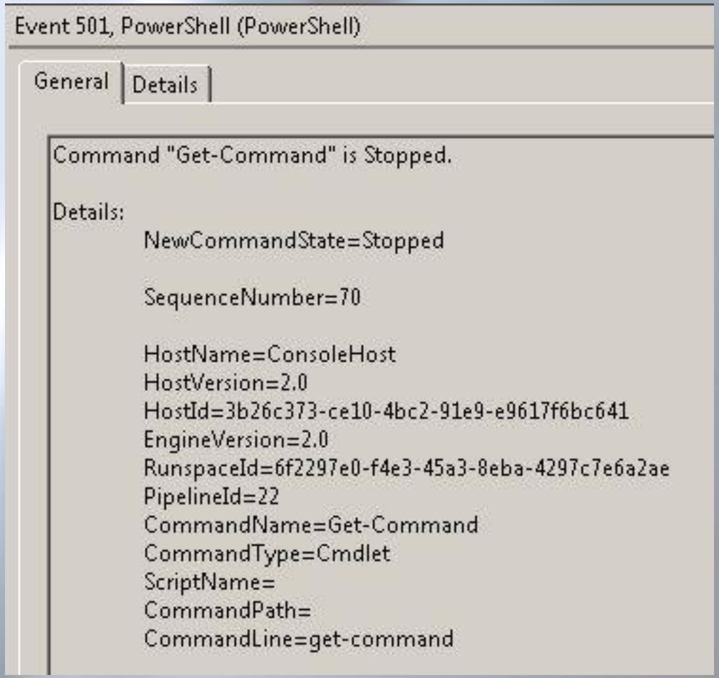
DISA STIG Auditing Policies Recommendation for Legacy Systems (XP, 2003 and earlier)

Audit Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success , Failure
Audit object access	Failure
Audit policy change	Success
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success

Me thinks this is missing something…

Powershell

- It’s nice to know Powershell executed, but we REALLY want to see what was executed
- Again, Windows SUCKS by default
- Details on setting PowerShell Preference variables
  - http://technet.microsoft.com/en-us/library/hh847796.aspx
- Run this command on each computer
  - $LogCommandHealthEvent = $true
  - $LogCommandLifecycleEvent = $true
- Splunk - Inputs.conf
  - # Windows platform specific input processor
  - [WinEventLog://Windows PowerShell]
  - disabled = 0



```
Command "Get-Command" is Stopped.

Details:
	NewCommandState=Stopped

	SequenceNumber=70

	HostName=ConsoleHost
	HostVersion=2.0
	HostId=3b26c373-ce10-4bc2-91e9-e9617f6bc641
	EngineVersion=2.0
	RunspaceId=6f2297e0-f4e3-45a3-8eba-4297c7e6a2ae
	PipelineId=22
	CommandName=Get-Command
	CommandType=Cmdlet
	ScriptName=
	CommandPath=
	CommandLine=get-command
```

Powershell Command Line

File System Security PowerShell Module 2.0 http://gallery.technet.microsoft.com/scriptcenter/1abd77a5-9c0b-4a2b-acef-90dbb2b84e85.

```
Get-Item C:\Windows | Add-Audit -Account "NT Authority\Everyone" -AccessRights
Delete -AppliesTo ThisFolderSubfoldersAndFiles
```

http://gallery.technet.microsoft.com/scriptcenter/1abd77a5-9c0b-4a2b-acef-90dbb2b84e85

The old iCacls or subinacls used to do it in Win XP and earlier…

Command Line basics for auditing

- https://chapters.theiia.org/lansing/Documents/Command%20Line%20Basics%20for%20IT%20Auditors.pdf

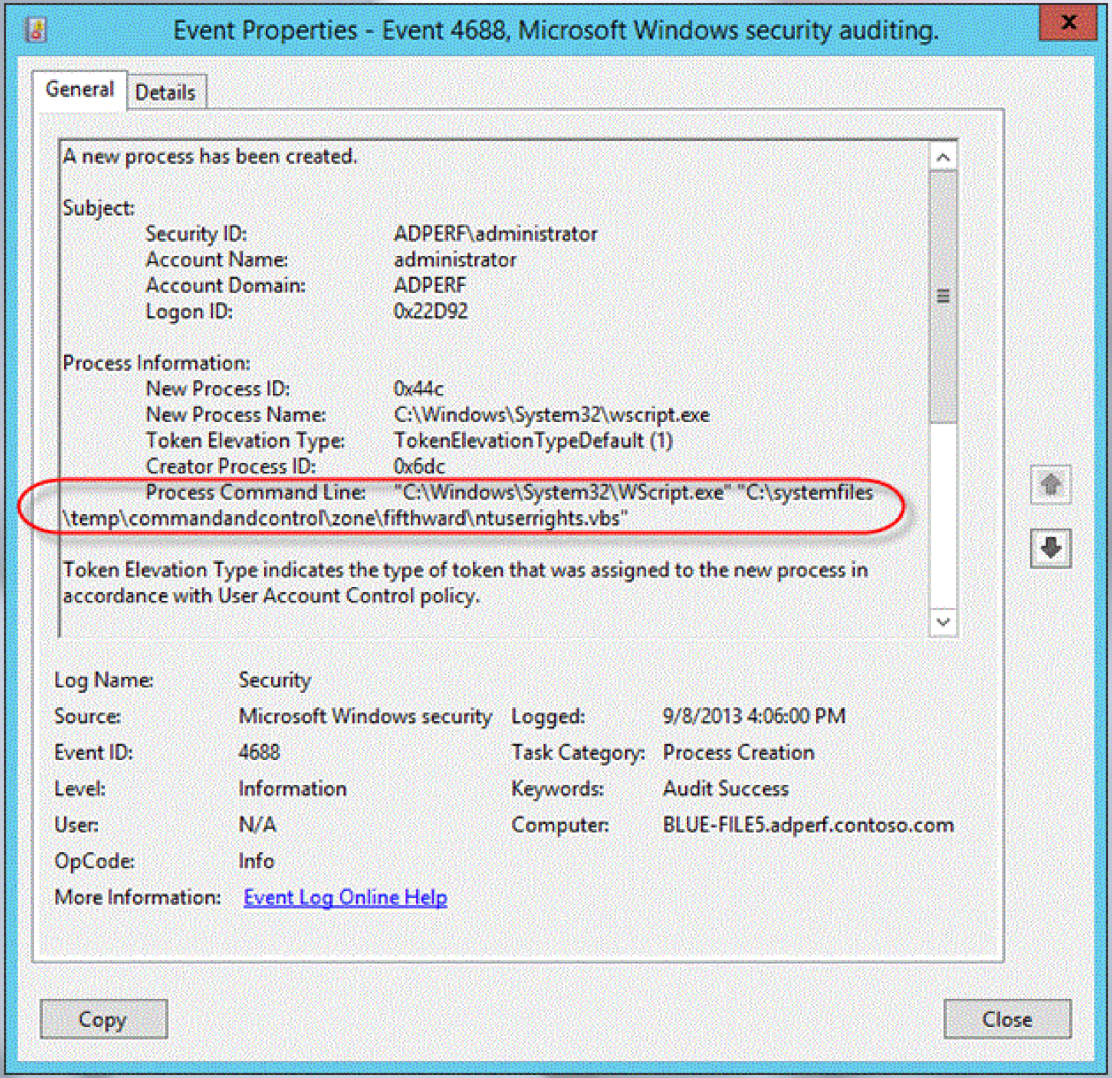
How to Gather logs with Powershell

- http://blogs.technet.com/b/heyscriptingguy/archive/2011/01/24/use-powershell-cmdlet-to-filter-event-log-for-easy-parsing.aspx

Windows 8.1

- It’s nice to know cmd.exe executed, but we REALLY want to see what was executed. It would be better if we could see what was executed with svchost.exe!
- Again, Windows SUCKS by default, even Windows 8.1
  - I do think this is the K3wlest feature in Windows 8.1
- Set GPO
  - Administrative Templates\System\Audit Process Creation
  - "Include command line in process creation events“
  - http://technet.microsoft.com/en-us/library/dn535776.aspx
- Registry Key
  - Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit\ProcessCreationIncludeCmdLine_Enabled to DWORD - 1

Windows 8.1 CMD line details!



Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details

```
A new process has been created.

Subject:
        Security ID:            ADPERF\administrator
        Account Name:           administrator
        Account Domain:         ADPERF
        Logon ID:               0x22D92

Process Information:
        New Process ID:         0x44c
        New Process Name:       C:\Windows\System32\wscript.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x6dc
        Process Command Line:   "C:\Windows\System32\WScript.exe" "C:\systemfiles
\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in
accordance with User Account Control policy.
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/8/2013 4:06:00 PM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	BLUE-FILE5.adperf.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

GATHER

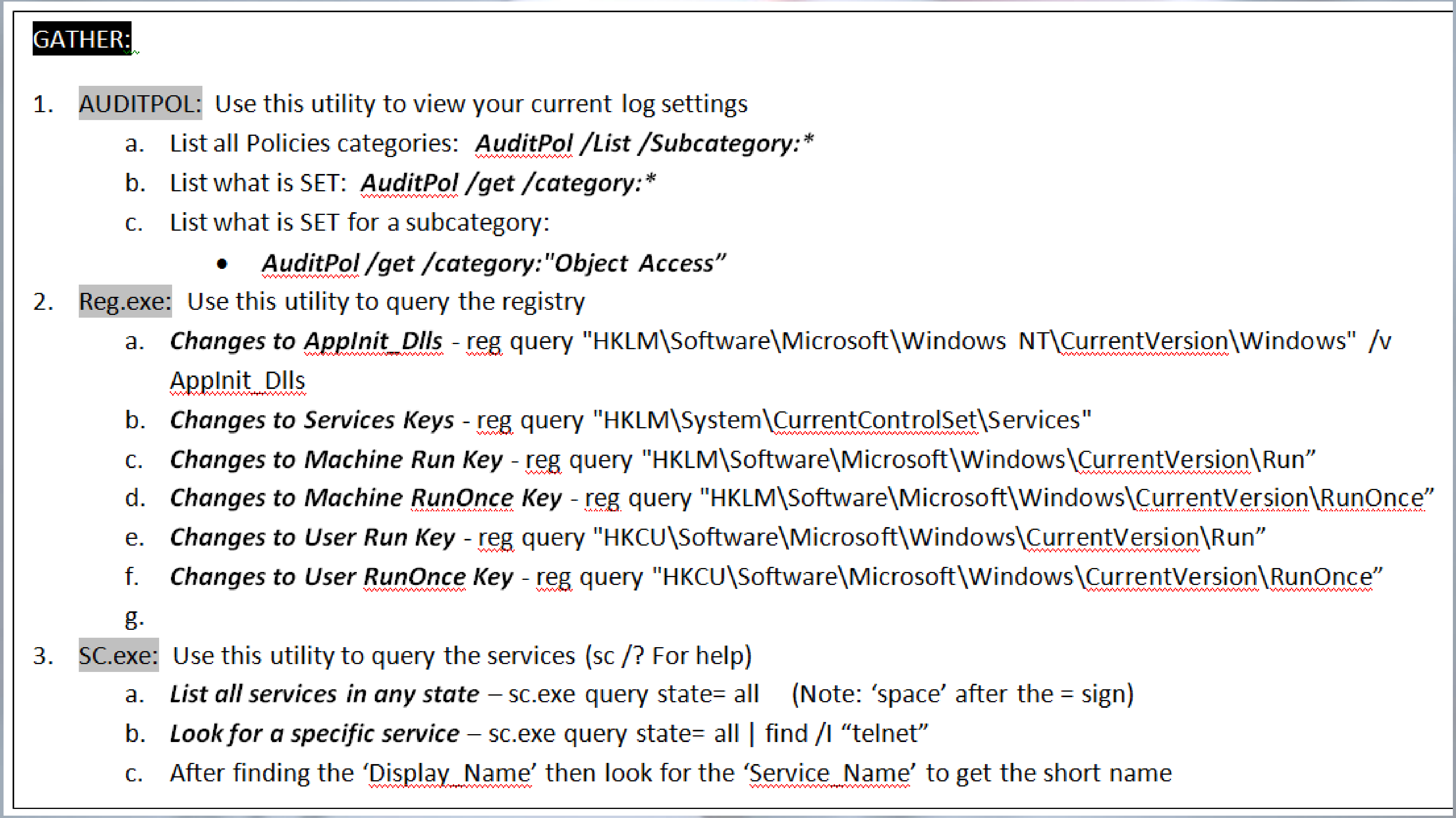
Windows Event Utility

WEvtUtil.exe – Command line tool to view logs.

- Help - WEvtUtil /?

/c:<count>	Return a specified count of event log entries. If omitted, you'll get everything.	/c:5
/rd:<True|False>	Reverse Direction. By default entries are returned oldest first. When set to True you'll get newest entries first.	/rd:true
/f:<Text|XML|RenderedXML>	The default output format is XML. Set this to Text; easier to read output.	/f:text
/r:<computername>	Specify the name of a remote computer.	/r:server01
/u:<username>	The user account to connect to the remote system	/u:Best1_usr
/p:<password>	The user account password to connect to the remote system	/p:BreachMe

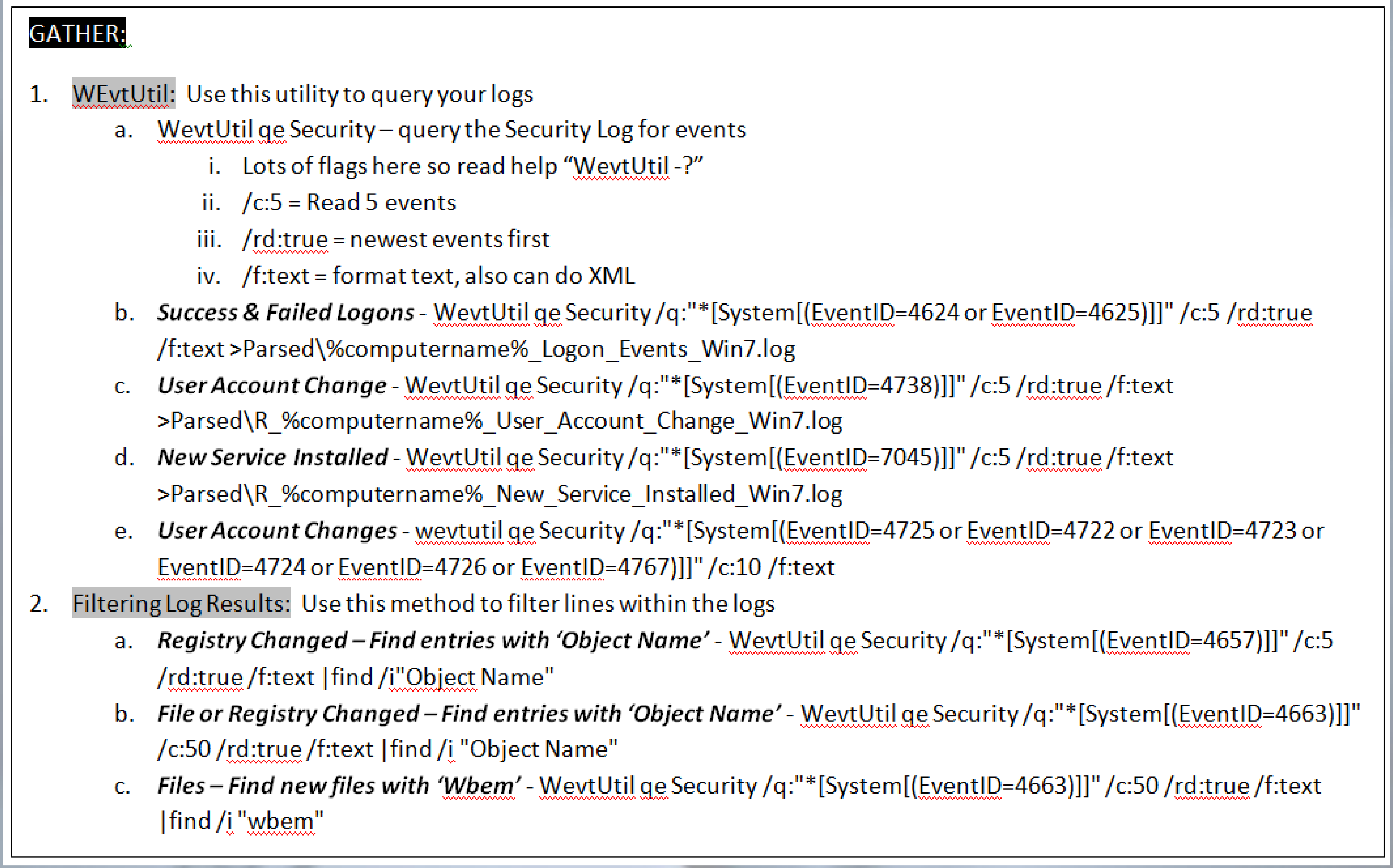
Let’s take a look



GATHER:

1. AUDITPOL: Use this utility to view your current log settings
   a. List all Policies categories: ***AuditPol /List /Subcategory:****
   b. List what is SET: ***AuditPol /get /category:****
   c. List what is SET for a subcategory:
      - ***AuditPol /get /category:"Object Access”***
2. Reg.exe: Use this utility to query the registry
   a. ***Changes to AppInit_Dlls*** - reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_Dlls
   b. ***Changes to Services Keys*** - reg query "HKLM\System\CurrentControlSet\Services"
   c. ***Changes to Machine Run Key*** - reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run”
   d. ***Changes to Machine RunOnce Key*** - reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce”
   e. ***Changes to User Run Key*** - reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run”
   f. ***Changes to User RunOnce Key*** - reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce”
   g.
3. SC.exe: Use this utility to query the services (sc /? For help)
   a. ***List all services in any state*** – sc.exe query state= all (Note: ‘space’ after the = sign)
   b. ***Look for a specific service*** – sc.exe query state= all | find /I “telnet”
   c. After finding the ‘Display_Name’ then look for the ‘Service_Name’ to get the short name

Let’s Play



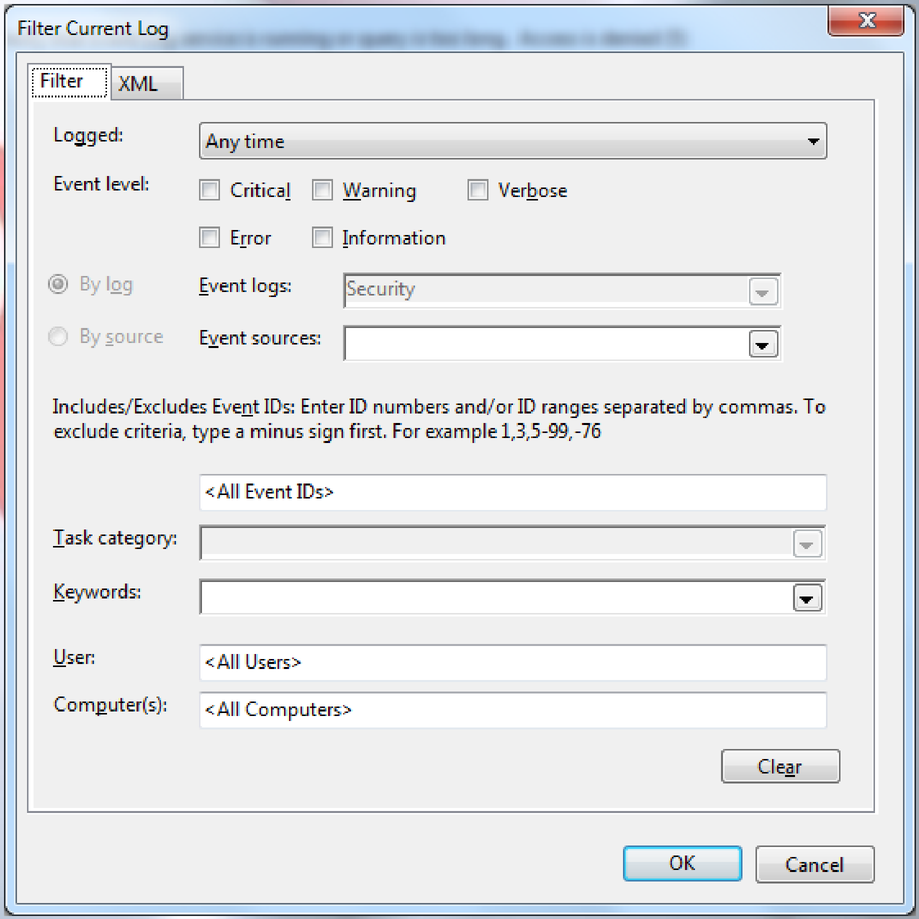
GATHER:

1. WEvtUtil: Use this utility to query your logs
    - a. WevtUtil qe Security – query the Security Log for events
        - i. Lots of flags here so read help “WevtUtil -?”
        - ii. /c:5 = Read 5 events
        - iii. /rd:true = newest events first
        - iv. /f:text = format text, also can do XML
    - b. ***Success & Failed Logons*** - WevtUtil qe Security /q:"*[System[(EventID=4624 or EventID=4625)]]" /c:5 /rd:true /f:text >Parsed\%computername%_Logon_Events_Win7.log
    - c. ***User Account Change*** - WevtUtil qe Security /q:"*[System[(EventID=4738)]]" /c:5 /rd:true /f:text >Parsed\R_%computername%_User_Account_Change_Win7.log
    - d. ***New Service Installed*** - WevtUtil qe Security /q:"*[System[(EventID=7045)]]" /c:5 /rd:true /f:text >Parsed\R_%computername%_New_Service_Installed_Win7.log
    - e. ***User Account Changes*** - wevtutil qe Security /q:"*[System[(EventID=4725 or EventID=4722 or EventID=4723 or EventID=4724 or EventID=4726 or EventID=4767)]]" /c:10 /f:text
2. Filtering Log Results: Use this method to filter lines within the logs
    - a. ***Registry Changed – Find entries with ‘Object Name’*** - WevtUtil qe Security /q:"*[System[(EventID=4657)]]" /c:5 /rd:true /f:text |find /i"Object Name"
    - b. ***File or Registry Changed – Find entries with ‘Object Name’*** - WevtUtil qe Security /q:"*[System[(EventID=4663)]]" /c:50 /rd:true /f:text |find /i "Object Name"
    - c. ***Files – Find new files with ‘Wbem’*** - WevtUtil qe Security /q:"*[System[(EventID=4663)]]" /c:50 /rd:true /f:text |find /i "wbem"

Let’s Look at Event Viewer

- Filter Current Log

- Use XML tab to feed your command line



Filter Current Log

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

● By log — Event logs: Security

○ By source — Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Windows Event Utility

- You can use the Event Log “Filter Current Log” to build a query and by viewing the XML copy and paste into the command line or save the XML results and execute at the command line.
- wevtutil qe Login_query.txt /sq:true /c:50

- Using WEvtUtil
  - http://www.petri.co.il/command-line-event-log.htm

What to monitor for

1. Administrator/Root/Guest login attempts
2. C$ logins workstations
3. C$ logins servers
4. Net.exe use, Net1.exe
5. Cscript.exe, PSExec.exe
6. IPConfig, NetStat
7. Database alerts
8. Disabled Acct login attempts
9. DNS Names surfing out from servers not in known list
10. FTP from servers and workstations
11. Group membership changes
12. Certain share accessed
13. Systems without logging agents of various kinds
14. OWA logins
15. RDP logins
16. Services installed servers, workstations noisy
17. Success logins for certain accounts
18. Suspicious files being executed
19. VPN logins
20. Unknown processes

Go Ahead and execute these on your system

- Open a command prompt and execute the following:
  - Net view
  - IPConfig
  - You have already connected to the Server share
  - RDP to the server
  - Add a user to your system
  - Change a user membership
  - Execute some utilities you have

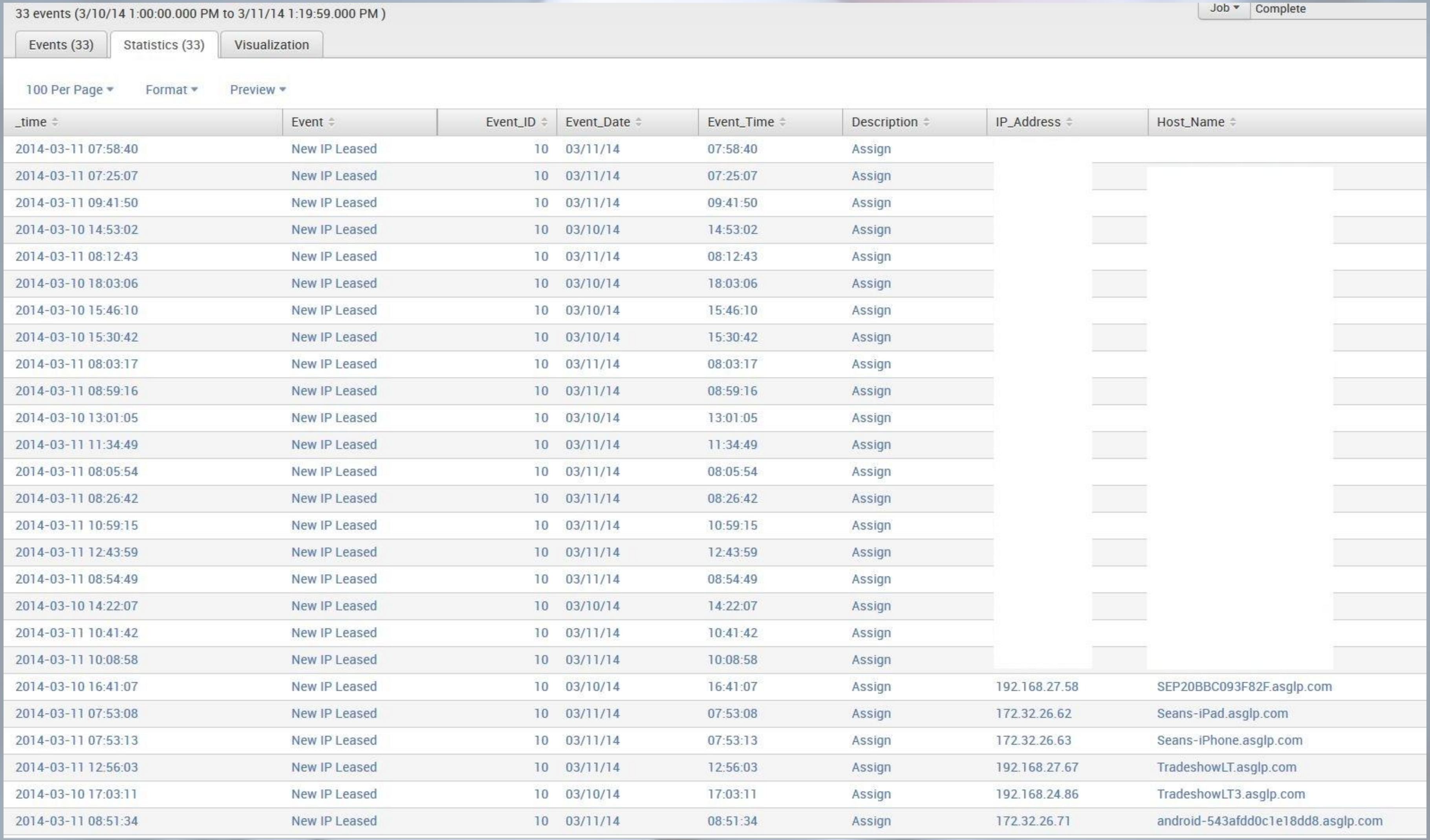
DHCP

- Lab
- Look at a Sample DHCP Log

- What you are looking for:

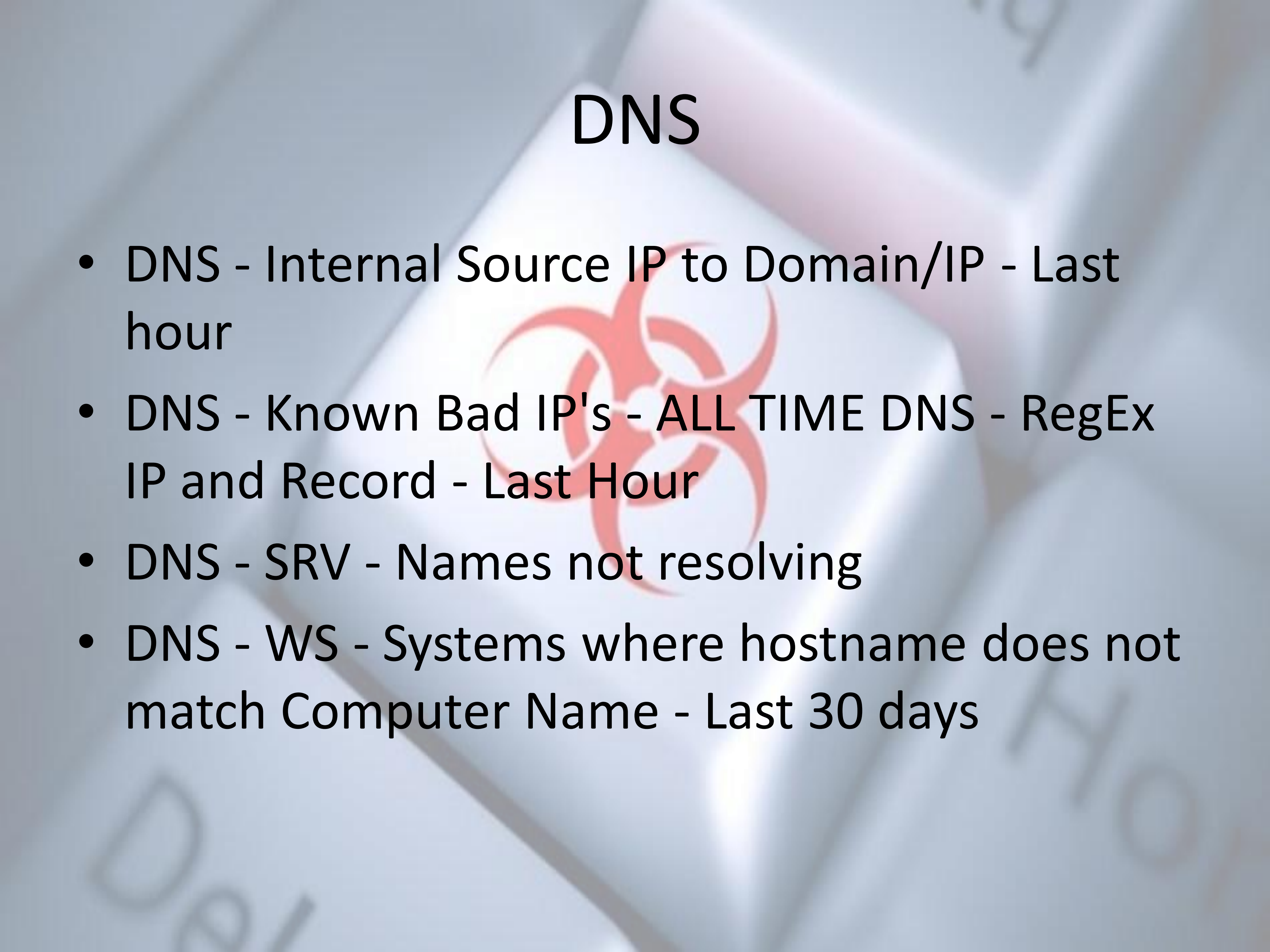
```
ID   Date               Message  IP                      System Name                MAC
10,02/17/14,10:53:24,Assign,10.1.2.3,US6575496-7001.domain.us.boo.hack.com,A44E31118A40,,538664179,0,,,
```

DHCP Logs



33 events (3/10/14 1:00:00.000 PM to 3/11/14 1:19:59.000 PM)

_time	Event	Event_ID	Event_Date	Event_Time	Description	IP_Address	Host_Name
2014-03-11 07:58:40	New IP Leased	10	03/11/14	07:58:40	Assign	[redacted]	[redacted]
2014-03-11 07:25:07	New IP Leased	10	03/11/14	07:25:07	Assign	[redacted]	[redacted]
2014-03-11 09:41:50	New IP Leased	10	03/11/14	09:41:50	Assign	[redacted]	[redacted]
2014-03-10 14:53:02	New IP Leased	10	03/10/14	14:53:02	Assign	[redacted]	[redacted]
2014-03-11 08:12:43	New IP Leased	10	03/11/14	08:12:43	Assign	[redacted]	[redacted]
2014-03-10 18:03:06	New IP Leased	10	03/10/14	18:03:06	Assign	[redacted]	[redacted]
2014-03-10 15:46:10	New IP Leased	10	03/10/14	15:46:10	Assign	[redacted]	[redacted]
2014-03-10 15:30:42	New IP Leased	10	03/10/14	15:30:42	Assign	[redacted]	[redacted]
2014-03-11 08:03:17	New IP Leased	10	03/11/14	08:03:17	Assign	[redacted]	[redacted]
2014-03-11 08:59:16	New IP Leased	10	03/11/14	08:59:16	Assign	[redacted]	[redacted]
2014-03-10 13:01:05	New IP Leased	10	03/10/14	13:01:05	Assign	[redacted]	[redacted]
2014-03-11 11:34:49	New IP Leased	10	03/11/14	11:34:49	Assign	[redacted]	[redacted]
2014-03-11 08:05:54	New IP Leased	10	03/11/14	08:05:54	Assign	[redacted]	[redacted]
2014-03-11 08:26:42	New IP Leased	10	03/11/14	08:26:42	Assign	[redacted]	[redacted]
2014-03-11 10:59:15	New IP Leased	10	03/11/14	10:59:15	Assign	[redacted]	[redacted]
2014-03-11 12:43:59	New IP Leased	10	03/11/14	12:43:59	Assign	[redacted]	[redacted]
2014-03-11 08:54:49	New IP Leased	10	03/11/14	08:54:49	Assign	[redacted]	[redacted]
2014-03-10 14:22:07	New IP Leased	10	03/10/14	14:22:07	Assign	[redacted]	[redacted]
2014-03-11 10:41:42	New IP Leased	10	03/11/14	10:41:42	Assign	[redacted]	[redacted]
2014-03-11 10:08:58	New IP Leased	10	03/11/14	10:08:58	Assign	[redacted]	[redacted]
2014-03-10 16:41:07	New IP Leased	10	03/10/14	16:41:07	Assign	192.168.27.58	SEP20BBC093F82F.asglp.com
2014-03-11 07:53:08	New IP Leased	10	03/11/14	07:53:08	Assign	172.32.26.62	Seans-iPad.asglp.com
2014-03-11 07:53:13	New IP Leased	10	03/11/14	07:53:13	Assign	172.32.26.63	Seans-iPhone.asglp.com
2014-03-11 12:56:03	New IP Leased	10	03/11/14	12:56:03	Assign	192.168.27.67	TradeshowLT.asglp.com
2014-03-10 17:03:11	New IP Leased	10	03/10/14	17:03:11	Assign	192.168.24.86	TradeshowLT3.asglp.com
2014-03-11 08:51:34	New IP Leased	10	03/11/14	08:51:34	Assign	172.32.26.71	android-543afdd0c1e18dd8.asglp.com



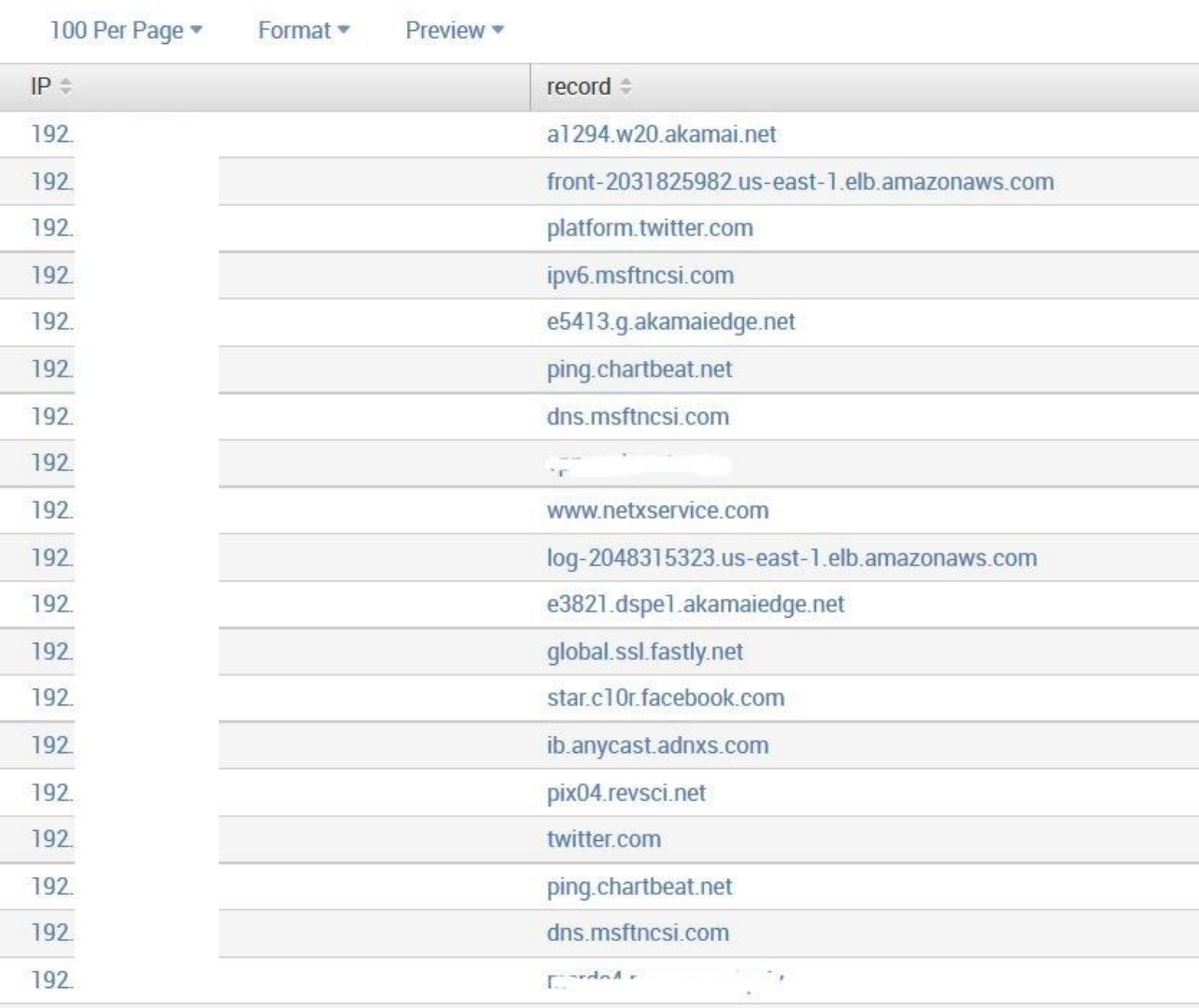
DNS

- DNS - Internal Source IP to Domain/IP - Last hour
- DNS - Known Bad IP's - ALL TIME DNS - RegEx IP and Record - Last Hour
- DNS - SRV - Names not resolving
- DNS - WS - Systems where hostname does not match Computer Name - Last 30 days

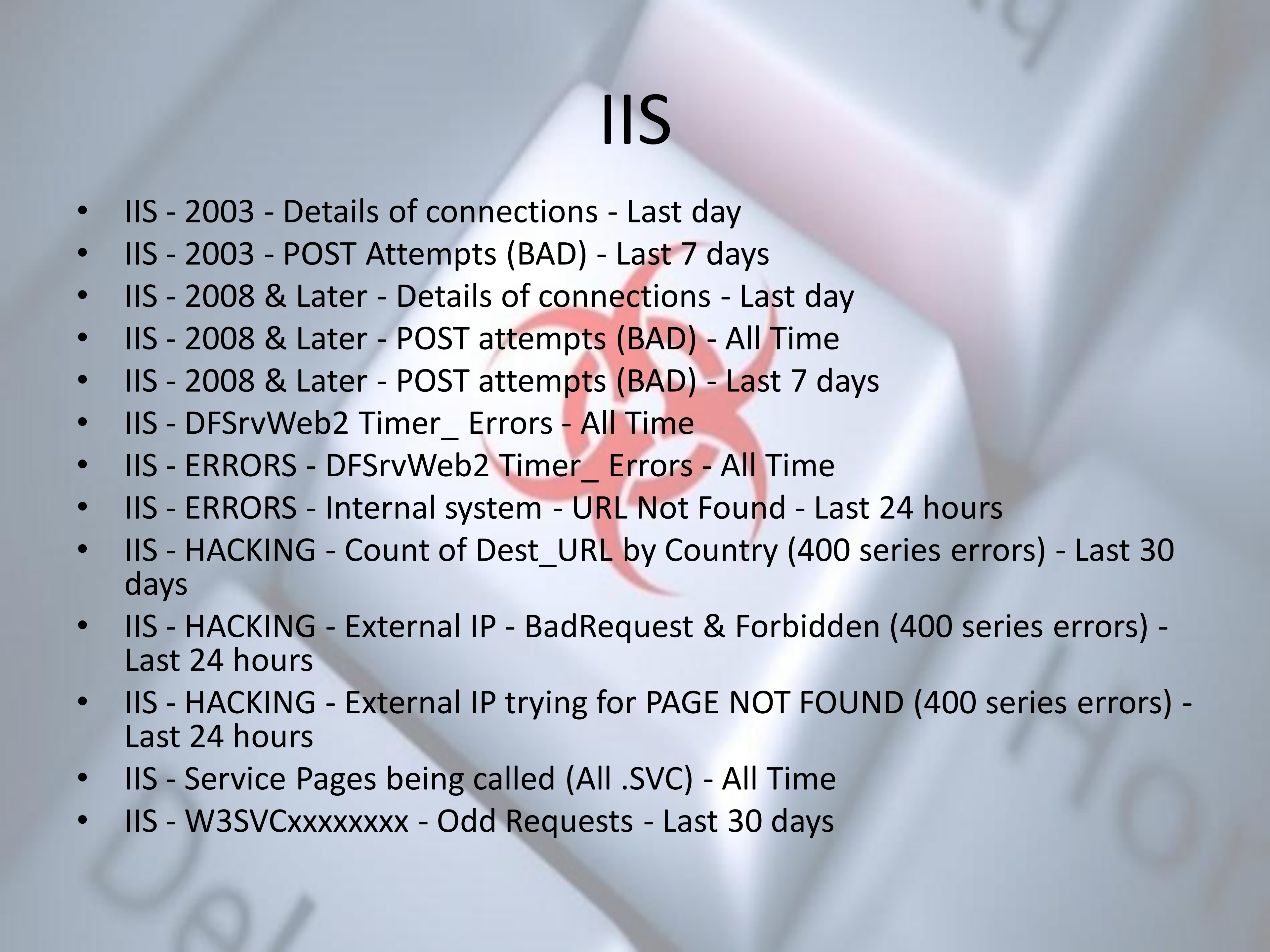
DNS Logs

- Lab
- Look at Sample DNS Log – Wht can you find ?

DNS Logs



IP	record
192.[redacted]	a1294.w20.akamai.net
192.[redacted]	front-2031825982.us-east-1.elb.amazonaws.com
192.[redacted]	platform.twitter.com
192.[redacted]	ipv6.msftncsi.com
192.[redacted]	e5413.g.akamaiedge.net
192.[redacted]	ping.chartbeat.net
192.[redacted]	dns.msftncsi.com
192.[redacted]	[redacted]
192.[redacted]	www.netxservice.com
192.[redacted]	log-2048315323.us-east-1.elb.amazonaws.com
192.[redacted]	e3821.dspe1.akamaiedge.net
192.[redacted]	global.ssl.fastly.net
192.[redacted]	star.c10r.facebook.com
192.[redacted]	ib.anycast.adnxs.com
192.[redacted]	pix04.revsci.net
192.[redacted]	twitter.com
192.[redacted]	ping.chartbeat.net
192.[redacted]	dns.msftncsi.com
192.[redacted]	[redacted]

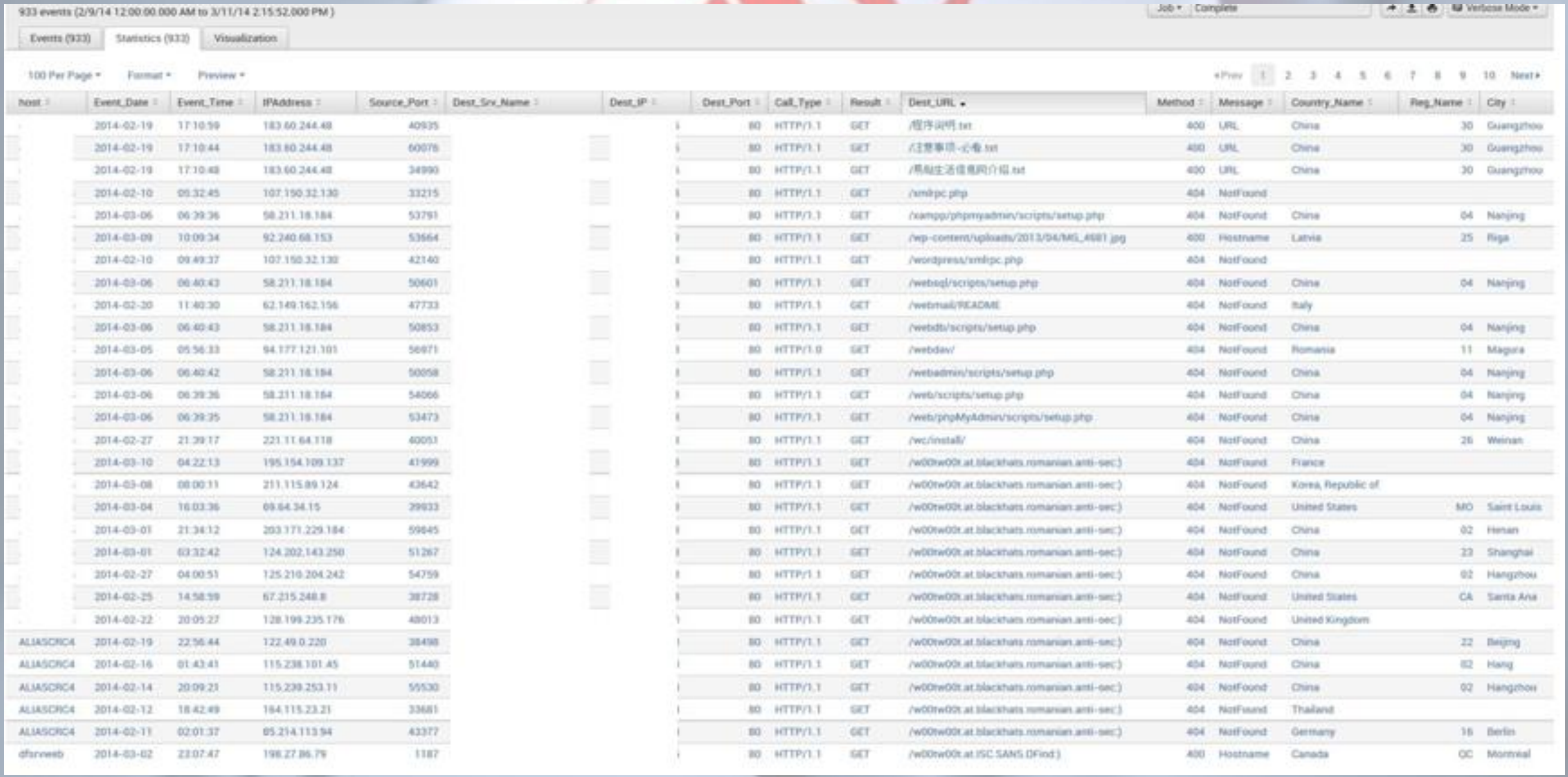


IIS

- IIS - 2003 - Details of connections - Last day
- IIS - 2003 - POST Attempts (BAD) - Last 7 days
- IIS - 2008 & Later - Details of connections - Last day
- IIS - 2008 & Later - POST attempts (BAD) - All Time
- IIS - 2008 & Later - POST attempts (BAD) - Last 7 days
- IIS - DFSrvWeb2 Timer_ Errors - All Time
- IIS - ERRORS - DFSrvWeb2 Timer_ Errors - All Time
- IIS - ERRORS - Internal system - URL Not Found - Last 24 hours
- IIS - HACKING - Count of Dest_URL by Country (400 series errors) - Last 30 days
- IIS - HACKING - External IP - BadRequest & Forbidden (400 series errors) - Last 24 hours
- IIS - HACKING - External IP trying for PAGE NOT FOUND (400 series errors) - Last 24 hours
- IIS - Service Pages being called (All .SVC) - All Time
- IIS - W3SVCxxxxxxxx - Odd Requests - Last 30 days

IIS Logs

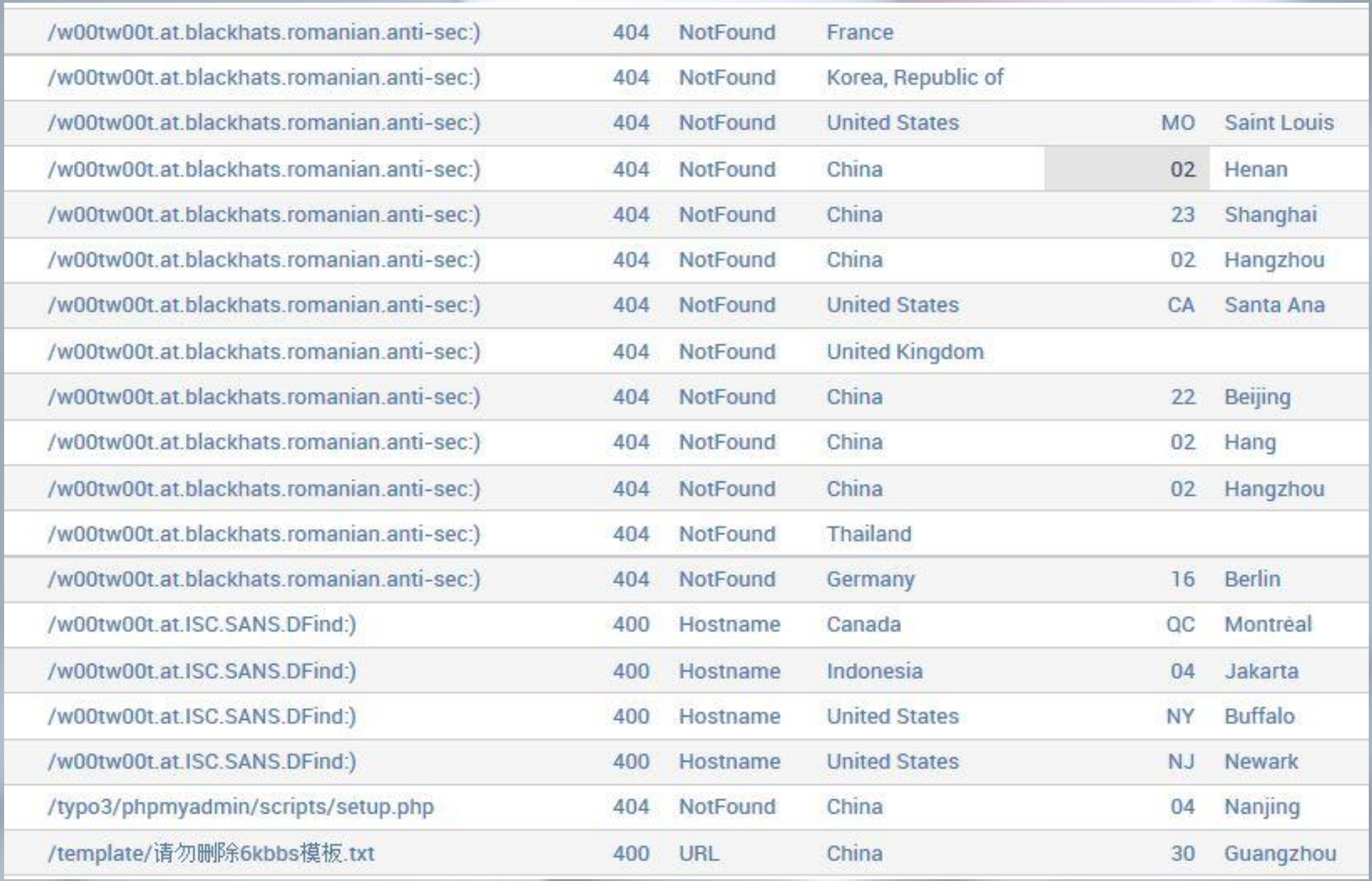
- Lab
- Look at a Sample IIS Log



933 events (2/9/14 12:00:00.000 AM to 3/11/14 2:15:52.000 PM)

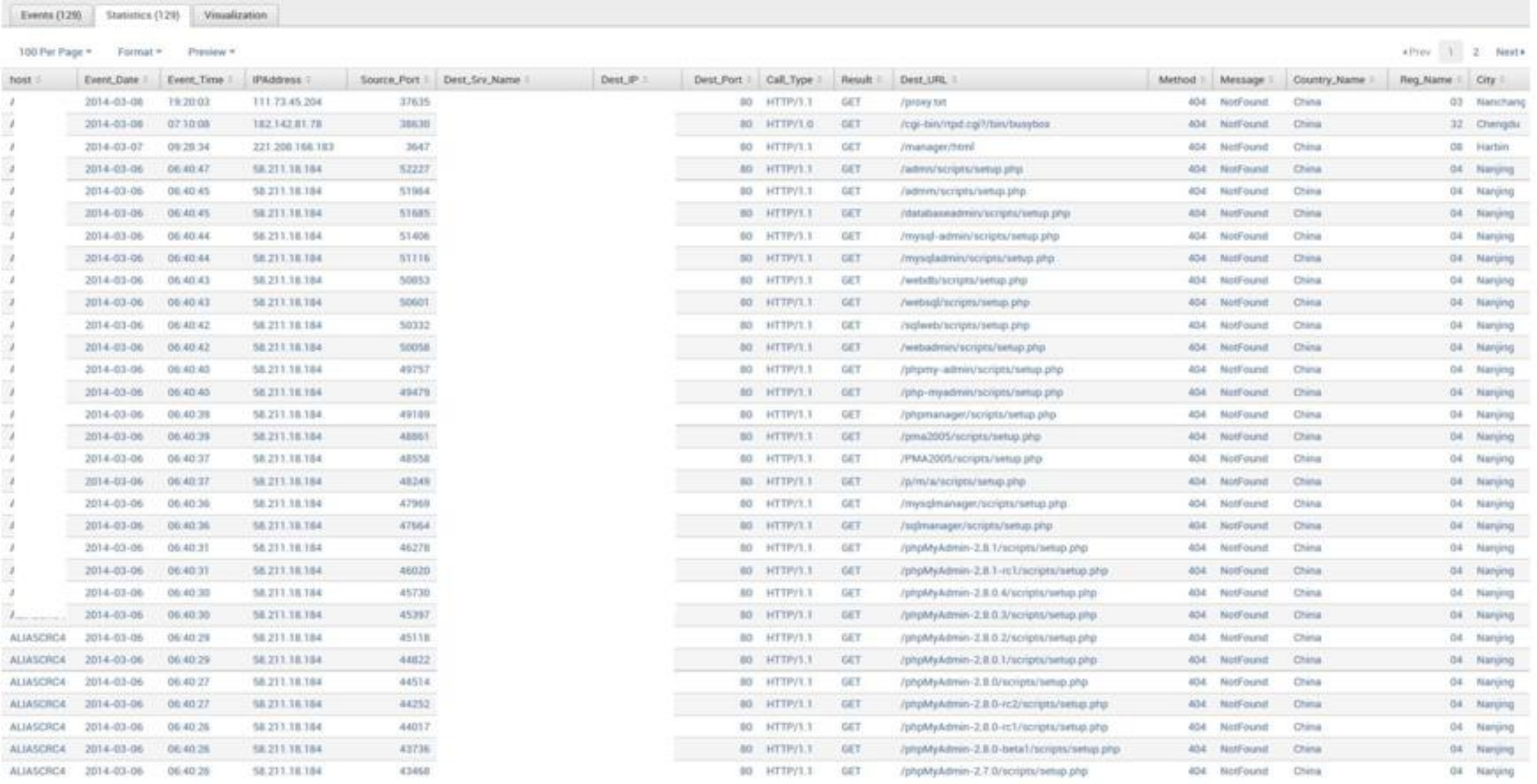
host	Event_Date	Event_Time	IPAddress	Source_Port	Dest_Srv_Name	Dest_IP	Dest_Port	Call_Type	Result	Dest_URL	Method	Message	Country_Name	Reg_Name	City
	2014-02-19	17:10:59	183.60.244.48	40935			80	HTTP/1.1	GET	/程序说明.txt	400	URL	China	30	Guangzhou
	2014-02-19	17:10:44	183.60.244.48	60076			80	HTTP/1.1	GET	/注意事项-必看.txt	400	URL	China	30	Guangzhou
	2014-02-19	17:10:48	183.60.244.48	34990			80	HTTP/1.1	GET	/易贴生活信息网介绍.txt	400	URL	China	30	Guangzhou
	2014-02-10	05:32:45	107.150.32.130	33215			80	HTTP/1.1	GET	/xmlrpc.php	404	NotFound			
	2014-03-06	06:39:36	58.211.18.184	53791			80	HTTP/1.1	GET	/xampp/phpmyadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-03-09	10:09:34	92.240.68.153	53664			80	HTTP/1.1	GET	/wp-content/uploads/2013/04/IMG_4681.jpg	400	Hostname	Latvia	25	Riga
	2014-02-10	09:49:37	107.150.32.130	42140			80	HTTP/1.1	GET	/wordpress/xmlrpc.php	404	NotFound			
	2014-03-06	06:40:43	58.211.18.184	50601			80	HTTP/1.1	GET	/websql/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-02-20	11:40:30	62.149.162.156	47733			80	HTTP/1.1	GET	/webmail/README	404	NotFound	Italy		
	2014-03-06	06:40:43	58.211.18.184	50853			80	HTTP/1.1	GET	/webdb/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-03-05	05:56:33	94.177.121.101	56871			80	HTTP/1.0	GET	/webdav/	404	NotFound	Romania	11	Magura
	2014-03-06	06:40:42	58.211.18.184	50058			80	HTTP/1.1	GET	/webadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-03-06	06:39:36	58.211.18.184	54066			80	HTTP/1.1	GET	/web/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-03-06	06:39:35	58.211.18.184	53473			80	HTTP/1.1	GET	/web/phpMyAdmin/scripts/setup.php	404	NotFound	China	04	Nanjing
	2014-02-27	21:39:17	221.11.64.118	40051			80	HTTP/1.1	GET	/wc/install/	404	NotFound	China	26	Weinan
	2014-03-10	04:22:13	195.154.109.137	41999			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	France		
	2014-03-08	08:00:11	211.115.89.124	43642			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Korea, Republic of		
	2014-03-04	16:03:36	69.64.34.15	29933			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United States	MO	Saint Louis
	2014-03-01	21:34:12	203.171.229.184	59845			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Henan
	2014-03-01	03:32:42	124.202.143.250	51267			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	23	Shanghai
	2014-02-27	04:00:51	125.210.204.242	54759			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hangzhou
	2014-02-25	14:58:59	67.215.248.8	38728			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United States	CA	Santa Ana
	2014-02-22	20:05:27	128.199.235.176	48013			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United Kingdom		
ALIASCRC4	2014-02-19	22:56:44	122.49.0.220	38498			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	22	Beijing
ALIASCRC4	2014-02-16	01:43:41	115.238.101.45	51440			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hang
ALIASCRC4	2014-02-14	20:09:21	115.239.253.11	55530			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hangzhou
ALIASCRC4	2014-02-12	18:42:49	184.115.23.21	33681			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Thailand		
ALIASCRC4	2014-02-11	02:01:37	85.214.113.94	43377			80	HTTP/1.1	GET	/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Germany	16	Berlin
dfsrvweb	2014-03-02	23:07:47	198.27.86.79	1187			80	HTTP/1.1	GET	/w00tw00t.at.ISC.SANS.DFind:)	400	Hostname	Canada	QC	Montreal

IIS Logs – w00t w00t



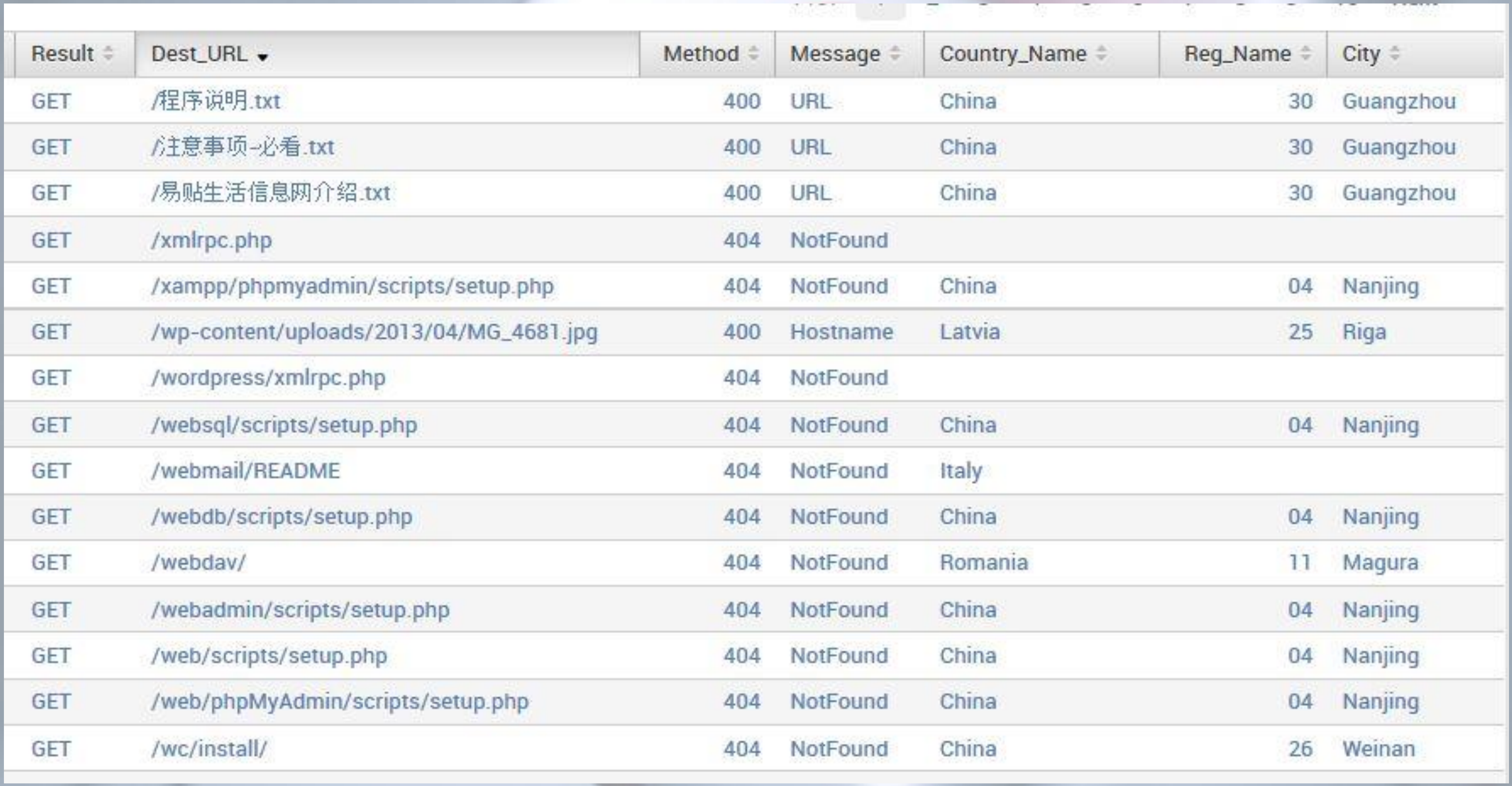
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	France		
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Korea, Republic of		
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United States	MO	Saint Louis
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Henan
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	23	Shanghai
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hangzhou
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United States	CA	Santa Ana
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	United Kingdom		
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	22	Beijing
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hang
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	China	02	Hangzhou
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Thailand		
/w00tw00t.at.blackhats.romanian.anti-sec:)	404	NotFound	Germany	16	Berlin
/w00tw00t.at.ISC.SANS.DFind:)	400	Hostname	Canada	QC	Montréal
/w00tw00t.at.ISC.SANS.DFind:)	400	Hostname	Indonesia	04	Jakarta
/w00tw00t.at.ISC.SANS.DFind:)	400	Hostname	United States	NY	Buffalo
/w00tw00t.at.ISC.SANS.DFind:)	400	Hostname	United States	NJ	Newark
/typo3/phpmyadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
/template/请勿删除6kbbs模板.txt	400	URL	China	30	Guangzhou

IIS Logs



host	Event_Date	Event_Time	IPAddress	Source_Port	Dest_Srv_Name	Dest_IP	Dest_Port	Call_Type	Result	Dest_URL	Method	Message	Country_Name	Reg_Name	City
[redacted]	2014-03-08	19:20:03	111.73.45.204	37635			80	HTTP/1.1	GET	/proxy.txt	404	NotFound	China	03	Nanchang
[redacted]	2014-03-08	07:10:08	182.142.81.78	38630			80	HTTP/1.0	GET	/cgi-bin/rtpd.cgi?/bin/busybox	404	NotFound	China	32	Chengdu
[redacted]	2014-03-07	09:28:34	221.208.166.183	3647			80	HTTP/1.1	GET	/manager/html	404	NotFound	China	08	Harbin
[redacted]	2014-03-06	06:40:47	58.211.18.184	52227			80	HTTP/1.1	GET	/admin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:45	58.211.18.184	51964			80	HTTP/1.1	GET	/admm/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:45	58.211.18.184	51685			80	HTTP/1.1	GET	/databaseadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:44	58.211.18.184	51406			80	HTTP/1.1	GET	/mysql-admin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:44	58.211.18.184	51116			80	HTTP/1.1	GET	/mysqladmin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:43	58.211.18.184	50853			80	HTTP/1.1	GET	/webdb/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:43	58.211.18.184	50601			80	HTTP/1.1	GET	/websql/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:42	58.211.18.184	50332			80	HTTP/1.1	GET	/sqlweb/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:42	58.211.18.184	50058			80	HTTP/1.1	GET	/webadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:40	58.211.18.184	49757			80	HTTP/1.1	GET	/phpmy-admin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:40	58.211.18.184	49479			80	HTTP/1.1	GET	/php-myadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:39	58.211.18.184	49189			80	HTTP/1.1	GET	/phpmanager/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:39	58.211.18.184	48861			80	HTTP/1.1	GET	/pma2005/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:37	58.211.18.184	48558			80	HTTP/1.1	GET	/PMA2005/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:37	58.211.18.184	48249			80	HTTP/1.1	GET	/p/m/a/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:36	58.211.18.184	47969			80	HTTP/1.1	GET	/mysqlmanager/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:36	58.211.18.184	47664			80	HTTP/1.1	GET	/sqlmanager/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:31	58.211.18.184	46278			80	HTTP/1.1	GET	/phpMyAdmin-2.8.1/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:31	58.211.18.184	46020			80	HTTP/1.1	GET	/phpMyAdmin-2.8.1-rc1/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:30	58.211.18.184	45730			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0.4/scripts/setup.php	404	NotFound	China	04	Nanjing
[redacted]	2014-03-06	06:40:30	58.211.18.184	45397			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0.3/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:29	58.211.18.184	45118			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0.2/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:29	58.211.18.184	44822			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0.1/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:27	58.211.18.184	44514			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:27	58.211.18.184	44252			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0-rc2/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:26	58.211.18.184	44017			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0-rc1/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:26	58.211.18.184	43736			80	HTTP/1.1	GET	/phpMyAdmin-2.8.0-beta1/scripts/setup.php	404	NotFound	China	04	Nanjing
ALIASCRC4	2014-03-06	06:40:26	58.211.18.184	43468			80	HTTP/1.1	GET	/phpMyAdmin-2.7.0/scripts/setup.php	404	NotFound	China	04	Nanjing

IIS Logs – China Calling

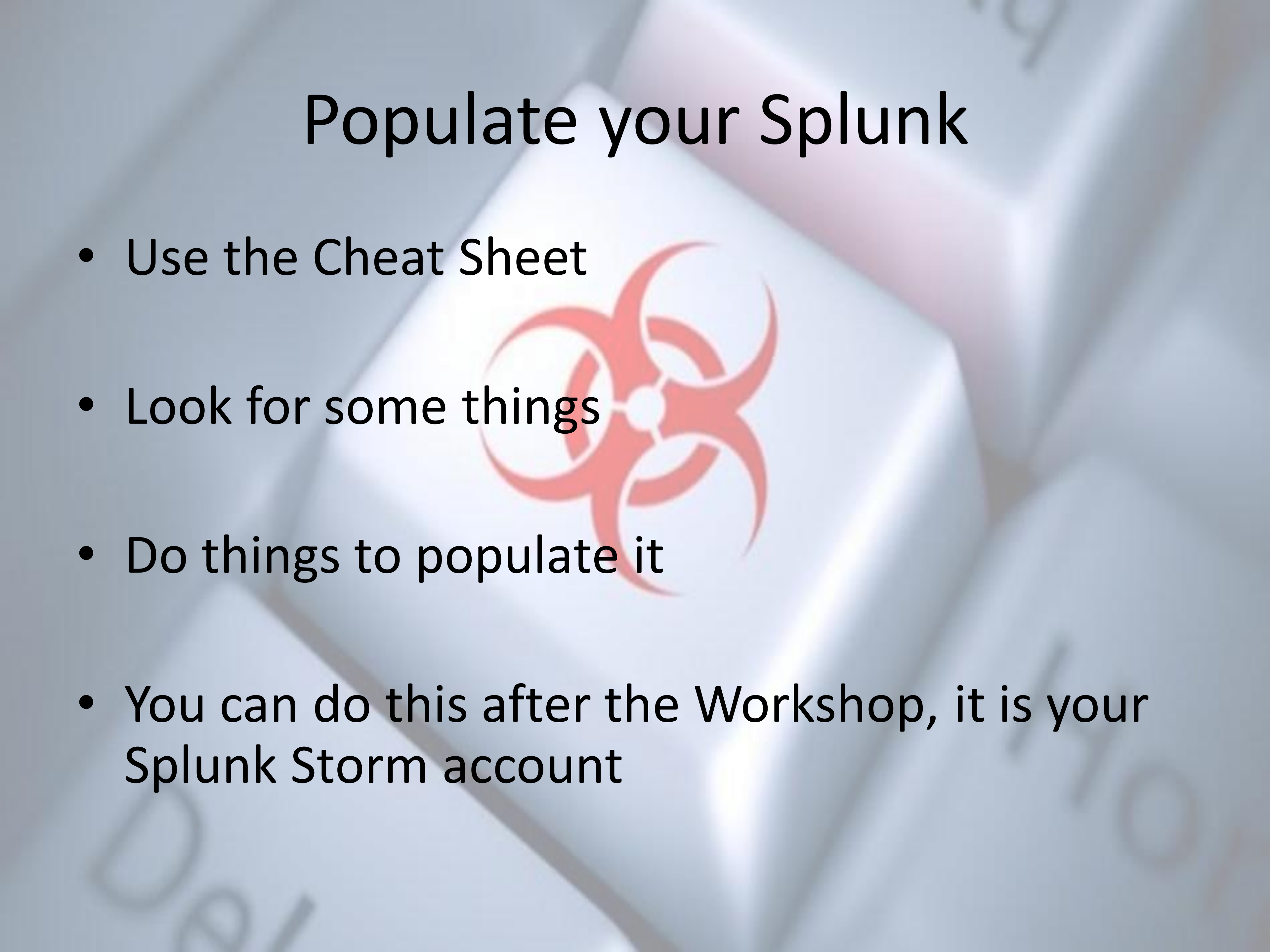


Result	Dest_URL	Method	Message	Country_Name	Reg_Name	City
GET	/程序说明.txt	400	URL	China	30	Guangzhou
GET	/注意事项-必看.txt	400	URL	China	30	Guangzhou
GET	/易贴生活信息网介绍.txt	400	URL	China	30	Guangzhou
GET	/xmlrpc.php	404	NotFound			
GET	/xampp/phpmyadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/wp-content/uploads/2013/04/MG_4681.jpg	400	Hostname	Latvia	25	Riga
GET	/wordpress/xmlrpc.php	404	NotFound			
GET	/websql/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/webmail/README	404	NotFound	Italy		
GET	/webdb/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/webdav/	404	NotFound	Romania	11	Magura
GET	/webadmin/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/web/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/web/phpMyAdmin/scripts/setup.php	404	NotFound	China	04	Nanjing
GET	/wc/install/	404	NotFound	China	26	Weinan

HARVEST

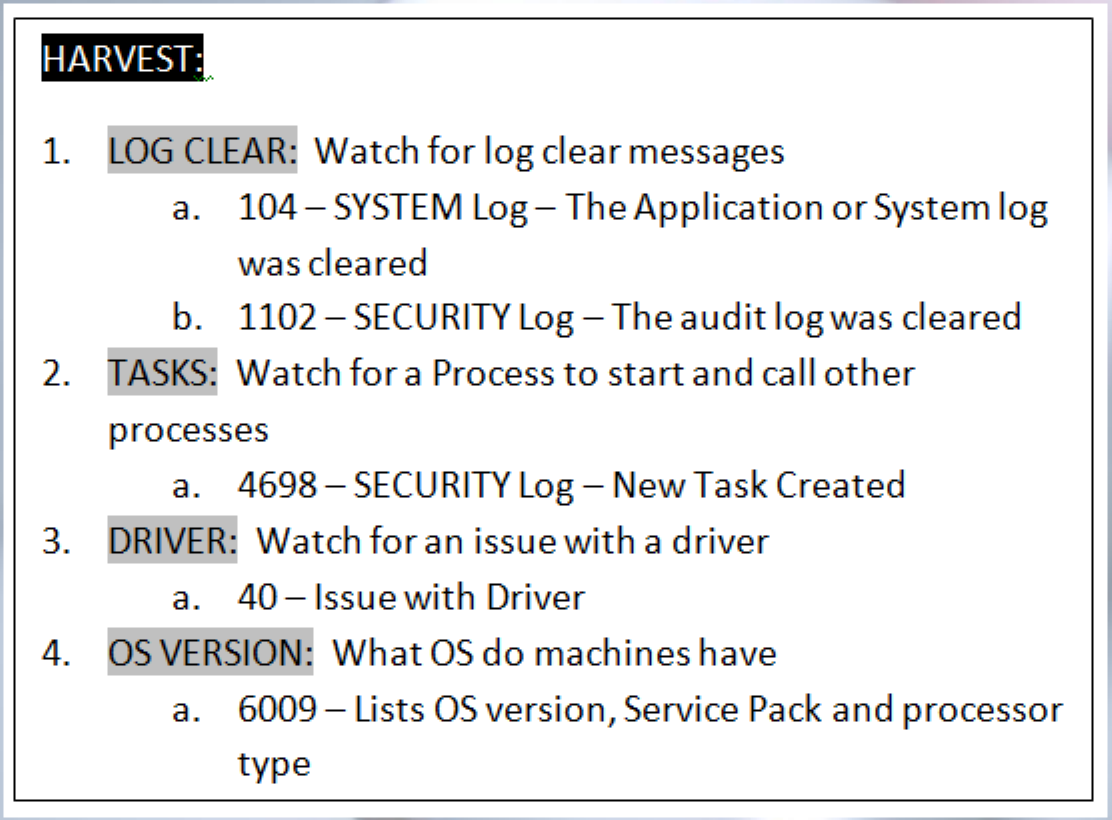
- Time for some Splunkage
- Let’s see what you can find
- First let’s look at a populated Splunk setup
- Open your Splunk Storm console

Populate your Splunk



- Use the Cheat Sheet
- Look for some things
- Do things to populate it
- You can do this after the Workshop, it is your Splunk Storm account

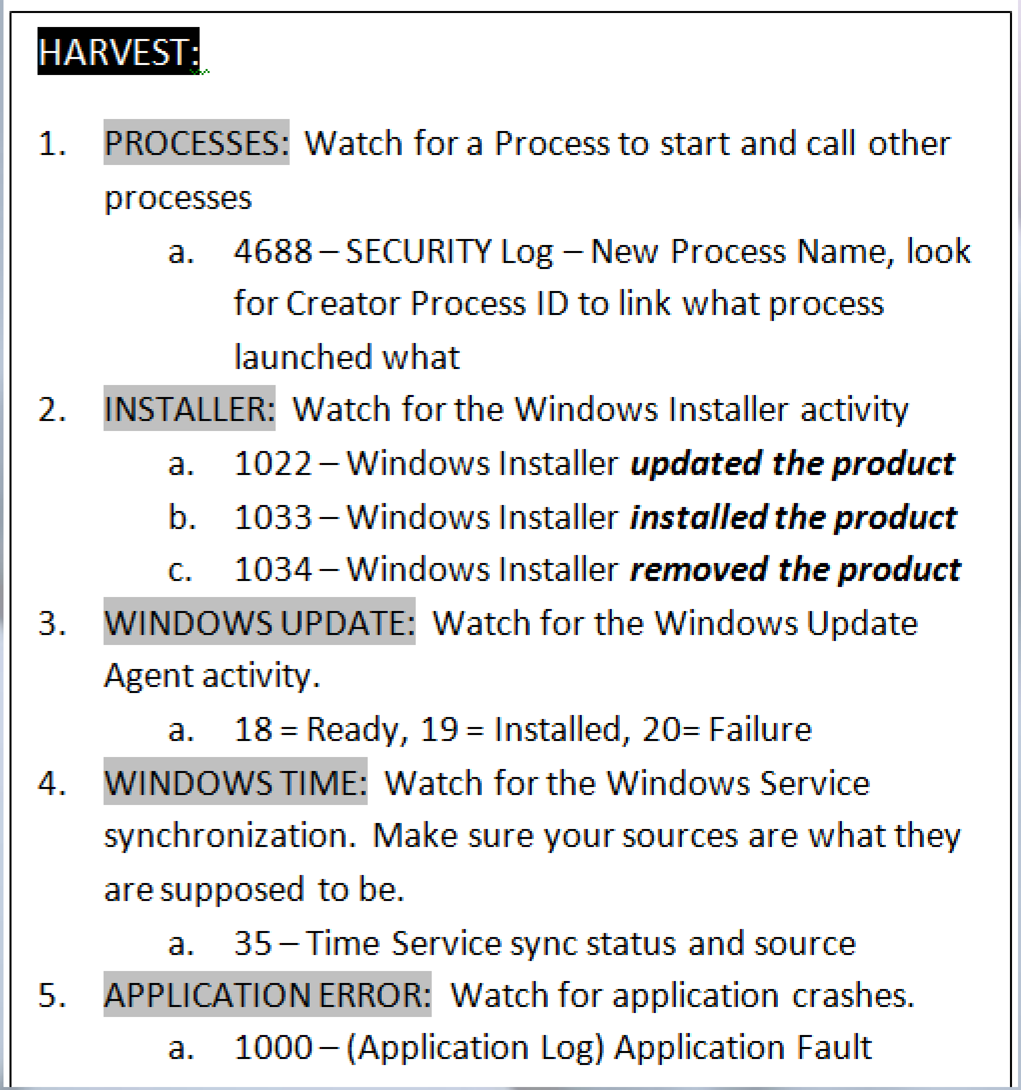
Log Clear, Tasks, Drivers, OS Version



HARVEST:

1. LOG CLEAR: Watch for log clear messages
   a. 104 – SYSTEM Log – The Application or System log was cleared
   b. 1102 – SECURITY Log – The audit log was cleared
2. TASKS: Watch for a Process to start and call other processes
   a. 4698 – SECURITY Log – New Task Created
3. DRIVER: Watch for an issue with a driver
   a. 40 – Issue with Driver
4. OS VERSION: What OS do machines have
   a. 6009 – Lists OS version, Service Pack and processor type

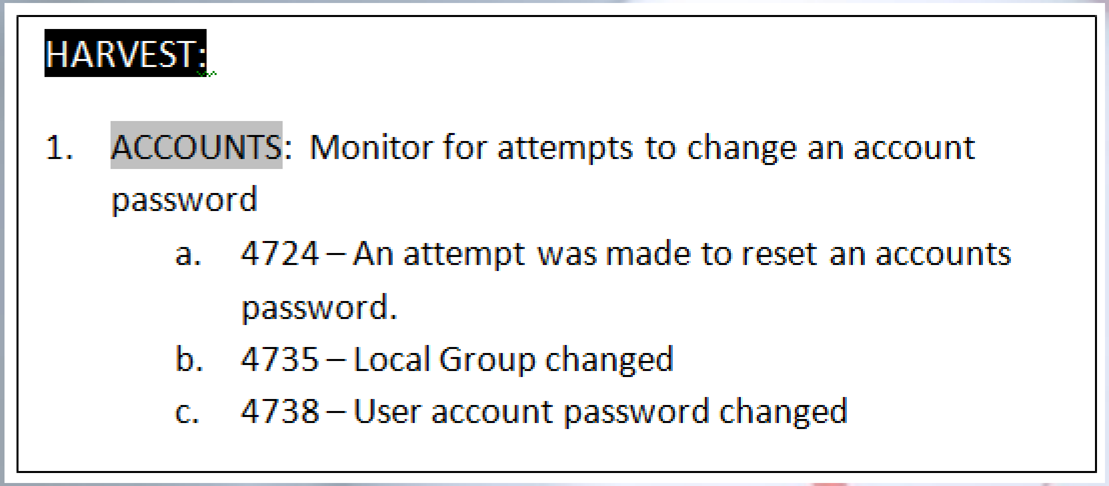
Processes, Installer, Windows Update, Windows Time, Application Errros



HARVEST:

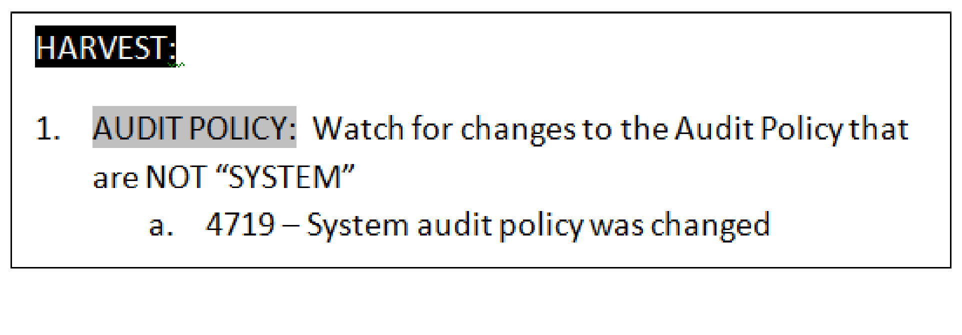
1. PROCESSES: Watch for a Process to start and call other processes
   a. 4688 – SECURITY Log – New Process Name, look for Creator Process ID to link what process launched what
2. INSTALLER: Watch for the Windows Installer activity
   a. 1022 – Windows Installer ***updated the product***
   b. 1033 – Windows Installer ***installed the product***
   c. 1034 – Windows Installer ***removed the product***
3. WINDOWS UPDATE: Watch for the Windows Update Agent activity.
   a. 18 = Ready, 19 = Installed, 20= Failure
4. WINDOWS TIME: Watch for the Windows Service synchronization. Make sure your sources are what they are supposed to be.
   a. 35 – Time Service sync status and source
5. APPLICATION ERROR: Watch for application crashes.
   a. 1000 – (Application Log) Application Fault

Accounts, Audit Policy, AppLocker



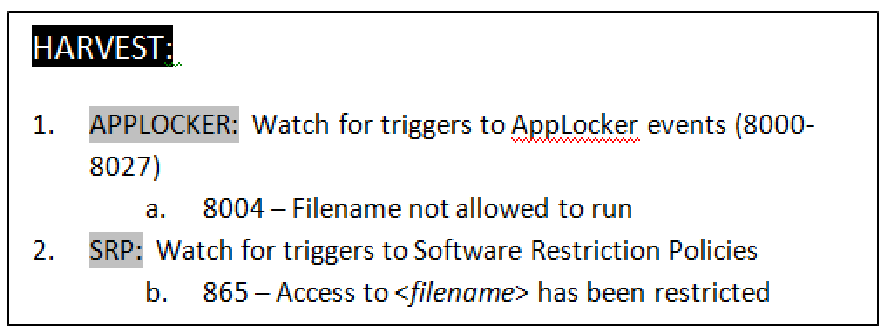
HARVEST:

1. ACCOUNTS: Monitor for attempts to change an account password
   a. 4724 – An attempt was made to reset an accounts password.
   b. 4735 – Local Group changed
   c. 4738 – User account password changed



HARVEST:

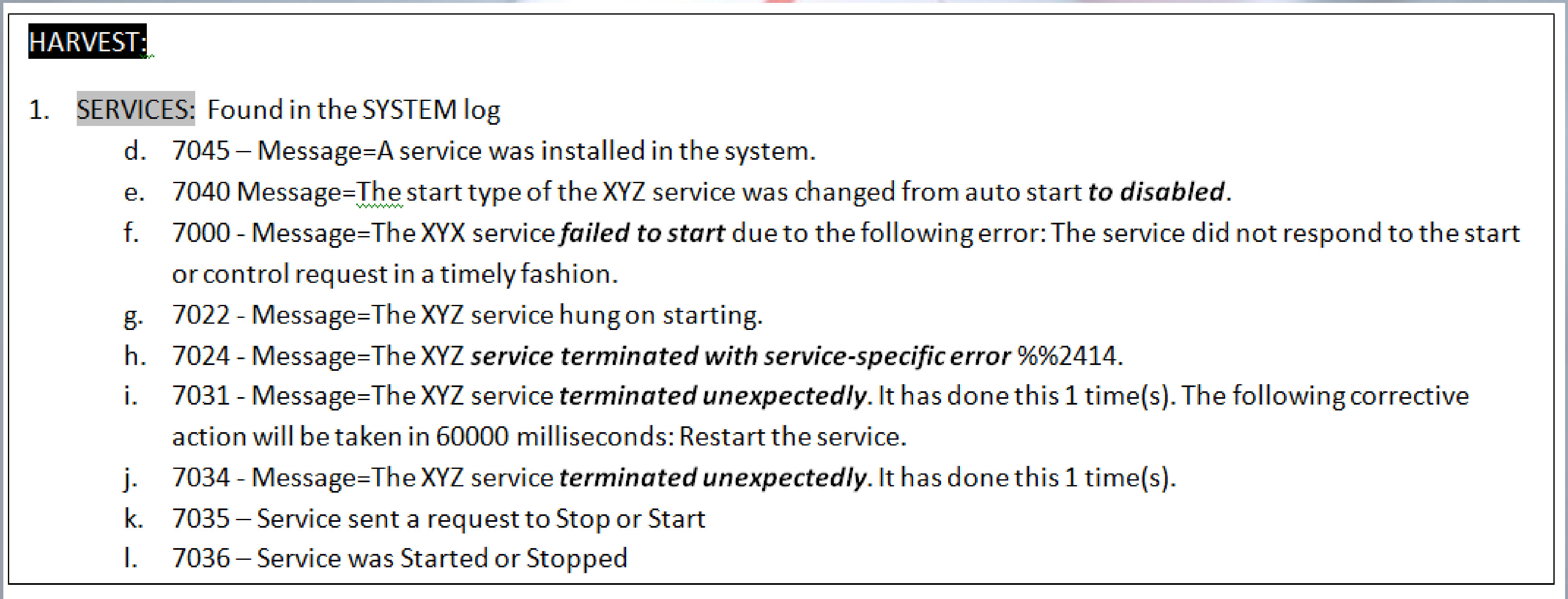
1. AUDIT POLICY: Watch for changes to the Audit Policy that are NOT "SYSTEM"
   a. 4719 – System audit policy was changed



HARVEST:

1. APPLOCKER: Watch for triggers to AppLocker events (8000-8027)
   a. 8004 – Filename not allowed to run
2. SRP: Watch for triggers to Software Restriction Policies
   b. 865 – Access to <*filename*> has been restricted

Services



HARVEST:

1. SERVICES: Found in the SYSTEM log

    d. 7045 – Message=A service was installed in the system.

    e. 7040 Message=The start type of the XYZ service was changed from auto start ***to disabled***.

    f. 7000 - Message=The XYX service ***failed to start*** due to the following error: The service did not respond to the start or control request in a timely fashion.

    g. 7022 - Message=The XYZ service hung on starting.

    h. 7024 - Message=The XYZ ***service terminated with service-specific error*** %%2414.

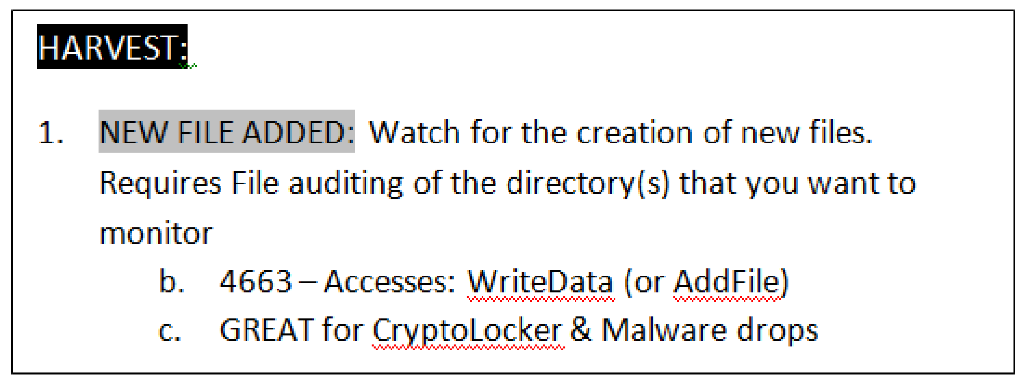
    i. 7031 - Message=The XYZ service ***terminated unexpectedly***. It has done this 1 time(s). The following corrective action will be taken in 60000 milliseconds: Restart the service.

    j. 7034 - Message=The XYZ service ***terminated unexpectedly***. It has done this 1 time(s).

    k. 7035 – Service sent a request to Stop or Start

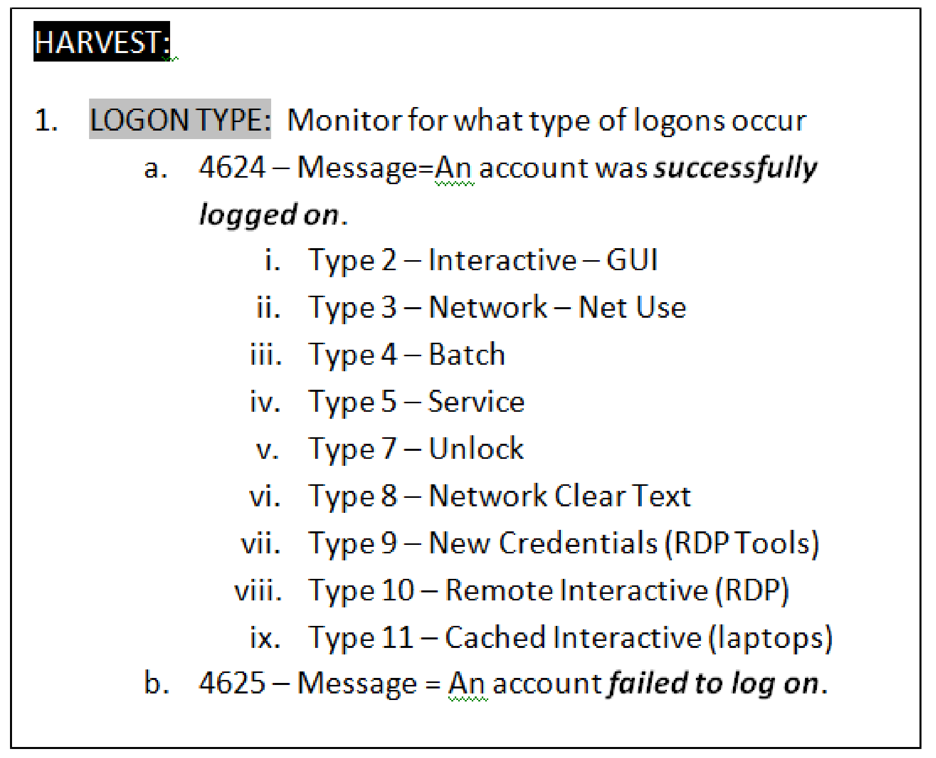
    l. 7036 – Service was Started or Stopped

New Files Added, Logon Type



HARVEST:

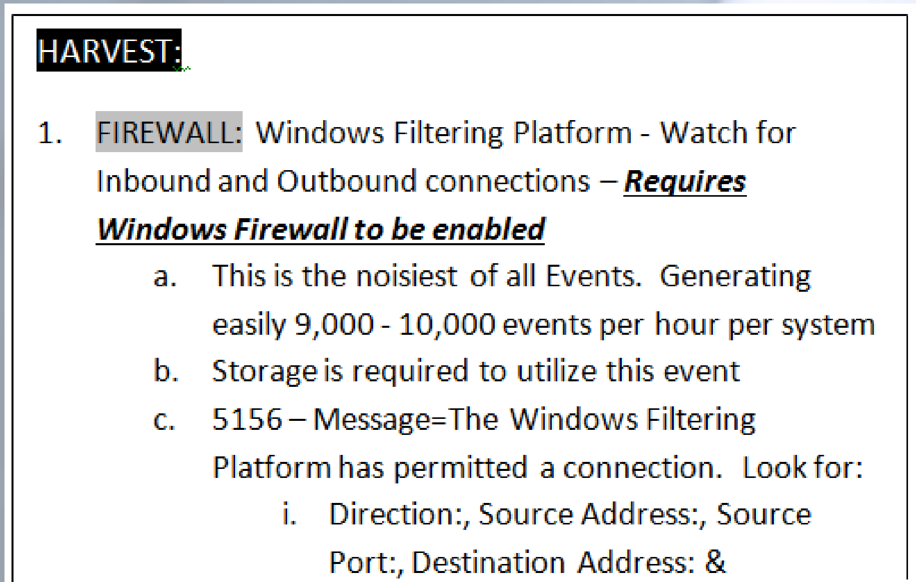
1. NEW FILE ADDED: Watch for the creation of new files. Requires File auditing of the directory(s) that you want to monitor
    b. 4663 – Accesses: WriteData (or AddFile)
    c. GREAT for CryptoLocker & Malware drops



HARVEST:

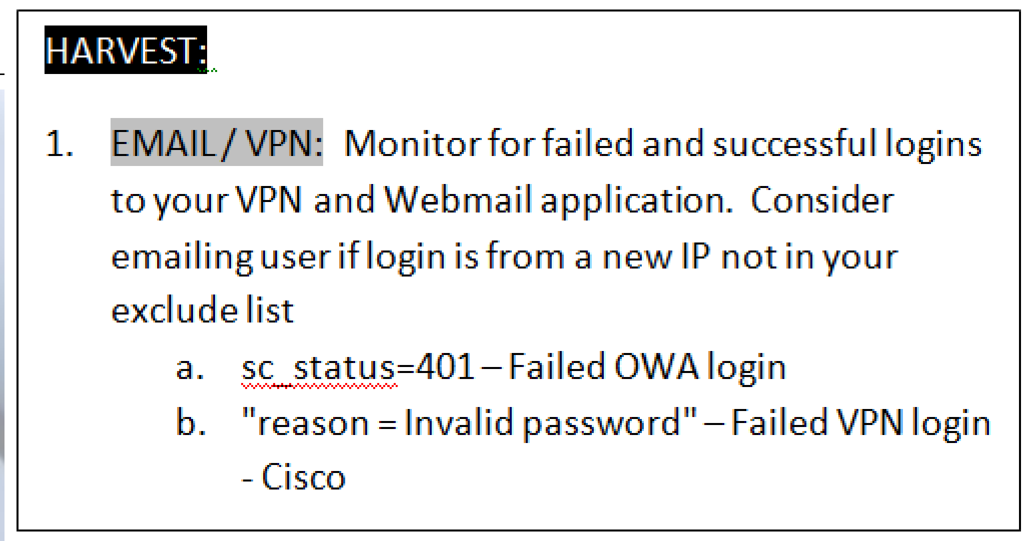
1. LOGON TYPE: Monitor for what type of logons occur
    a. 4624 – Message=An account was ***successfully logged on***.
        i. Type 2 – Interactive – GUI
        ii. Type 3 – Network – Net Use
        iii. Type 4 – Batch
        iv. Type 5 – Service
        v. Type 7 – Unlock
        vi. Type 8 – Network Clear Text
        vii. Type 9 – New Credentials (RDP Tools)
        viii. Type 10 – Remote Interactive (RDP)
        ix. Type 11 – Cached Interactive (laptops)
    b. 4625 – Message = An account ***failed to log on***.

Windows Firewall, Email/VPN



HARVEST:

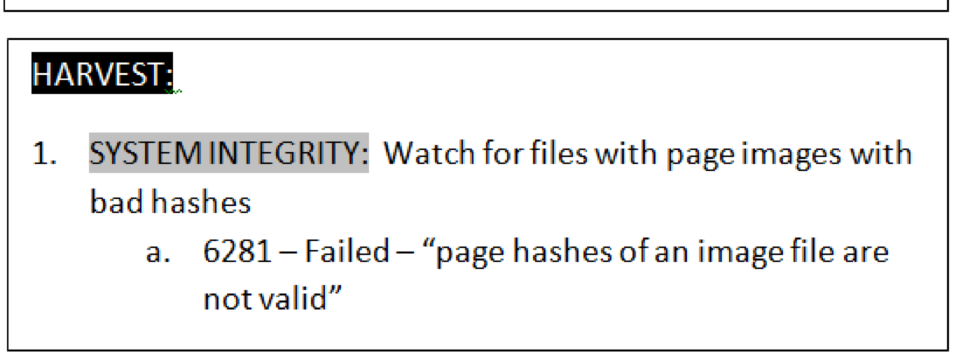
1. FIREWALL: Windows Filtering Platform - Watch for Inbound and Outbound connections – ***Requires Windows Firewall to be enabled***
   a. This is the noisiest of all Events. Generating easily 9,000 - 10,000 events per hour per system
   b. Storage is required to utilize this event
   c. 5156 – Message=The Windows Filtering Platform has permitted a connection. Look for:
      i. Direction:, Source Address:, Source Port:, Destination Address: & Destination Port:



HARVEST:

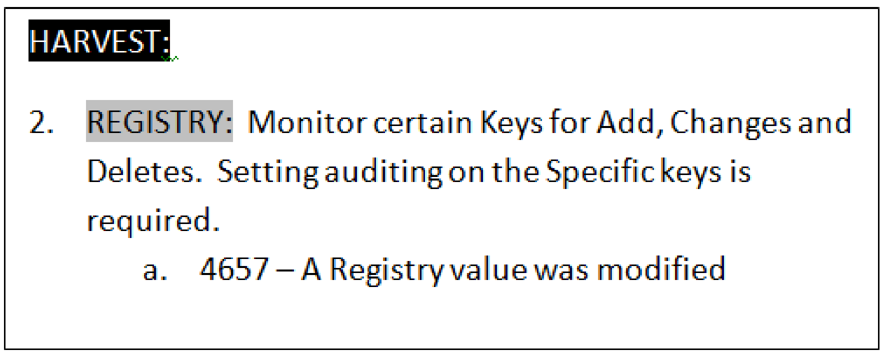
1. EMAIL / VPN: Monitor for failed and successful logins to your VPN and Webmail application. Consider emailing user if login is from a new IP not in your exclude list
   a. sc_status=401 – Failed OWA login
   b. "reason = Invalid password" – Failed VPN login - Cisco

System Integrity, Registry



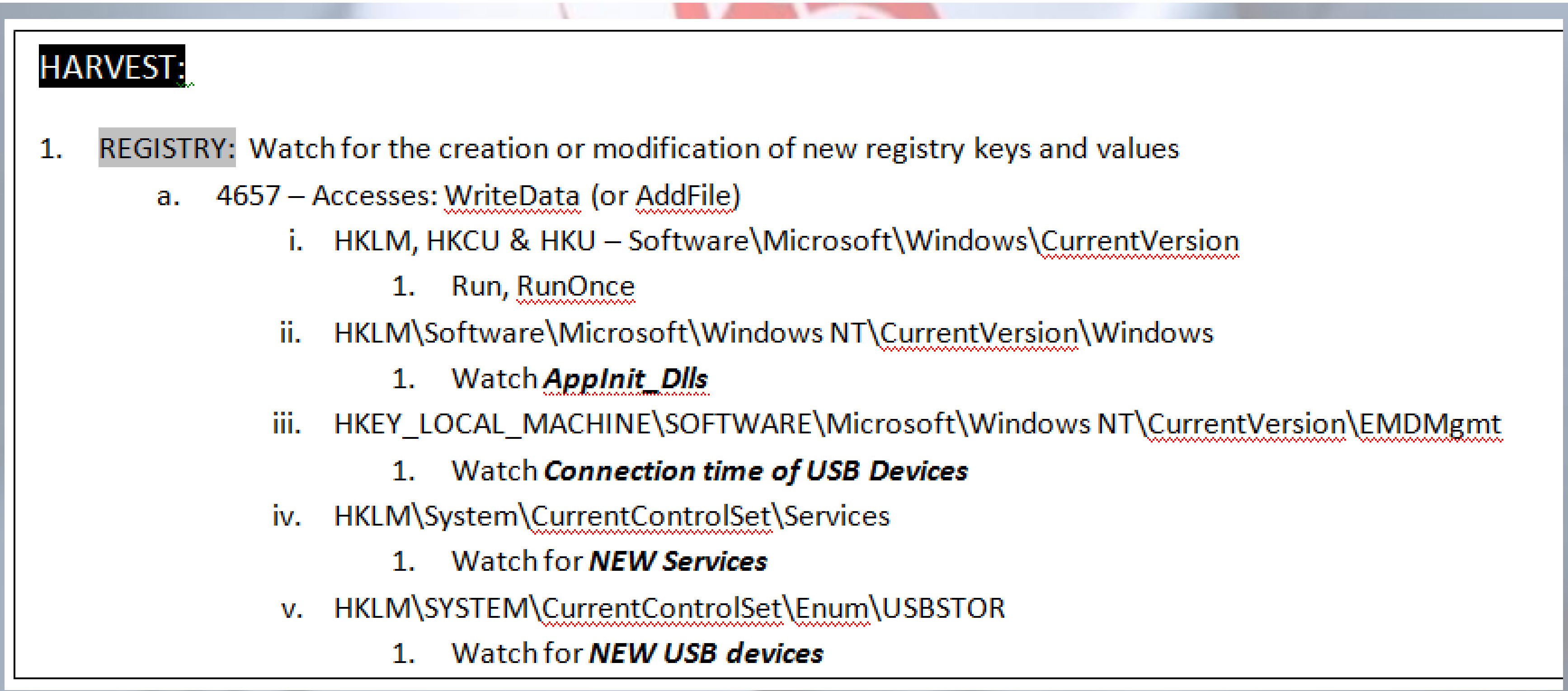
HARVEST:

1. SYSTEM INTEGRITY: Watch for files with page images with bad hashes
   a. 6281 – Failed – "page hashes of an image file are not valid"



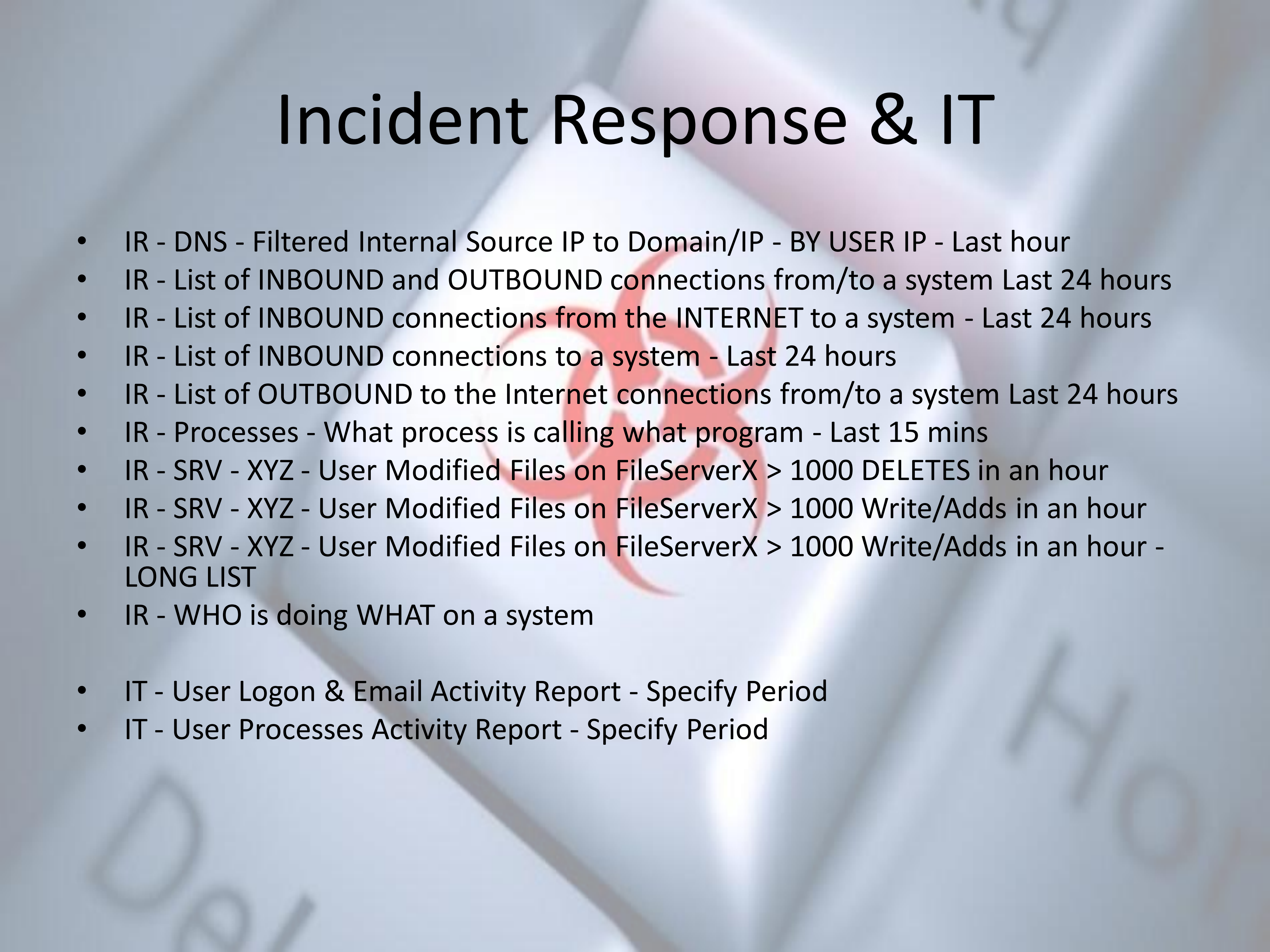
HARVEST:

2. REGISTRY: Monitor certain Keys for Add, Changes and Deletes. Setting auditing on the Specific keys is required.
   a. 4657 – A Registry value was modified



HARVEST:

1. REGISTRY: Watch for the creation or modification of new registry keys and values
   a. 4657 – Accesses: WriteData (or AddFile)
      i. HKLM, HKCU & HKU – Software\Microsoft\Windows\CurrentVersion
         1. Run, RunOnce
      ii. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows
         1. Watch ***AppInit_Dlls***
      iii. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
         1. Watch ***Connection time of USB Devices***
      iv. HKLM\System\CurrentControlSet\Services
         1. Watch for ***NEW Services***
      v. HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
         1. Watch for ***NEW USB devices***

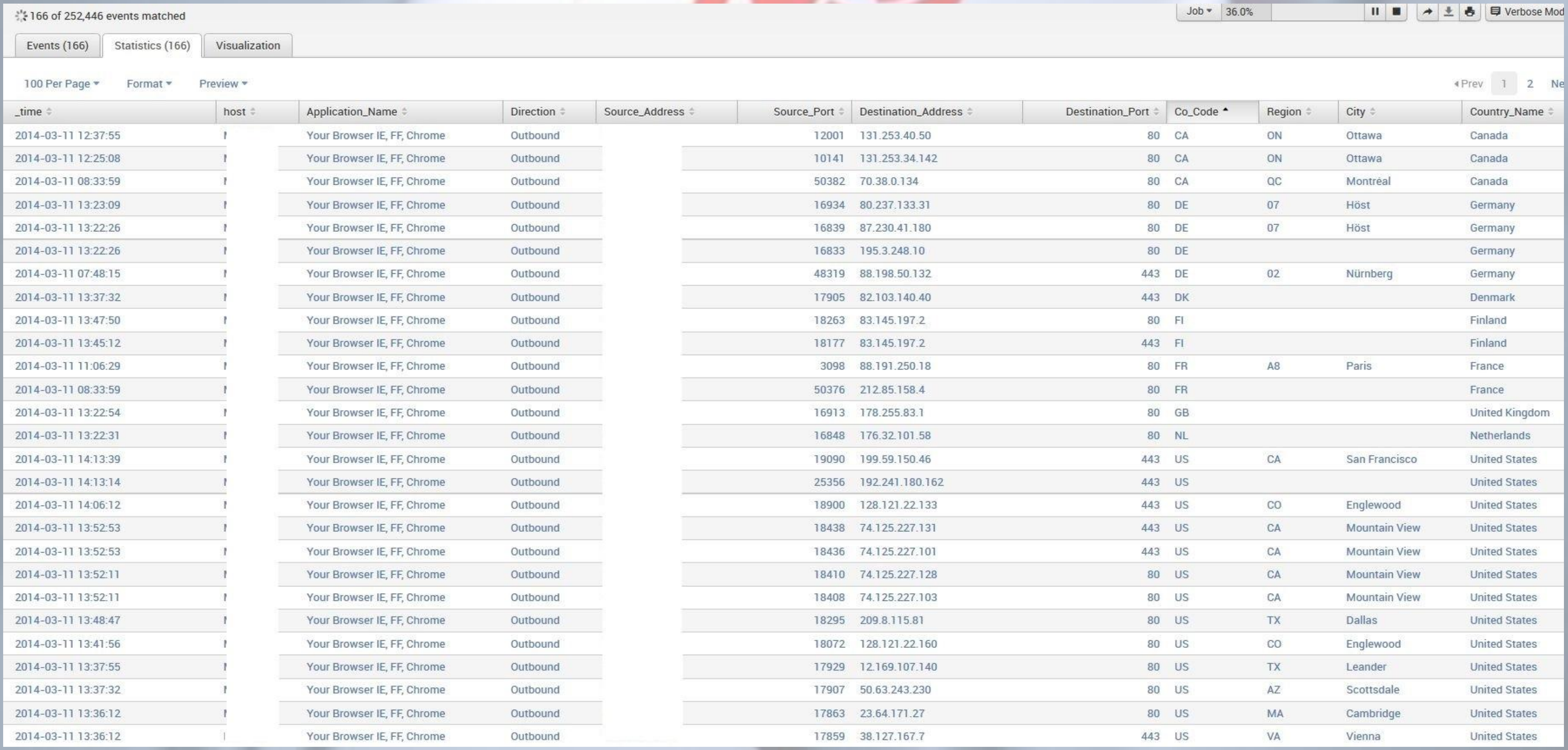


Incident Response & IT

- IR - DNS - Filtered Internal Source IP to Domain/IP - BY USER IP - Last hour
- IR - List of INBOUND and OUTBOUND connections from/to a system Last 24 hours
- IR - List of INBOUND connections from the INTERNET to a system - Last 24 hours
- IR - List of INBOUND connections to a system - Last 24 hours
- IR - List of OUTBOUND to the Internet connections from/to a system Last 24 hours
- IR - Processes - What process is calling what program - Last 15 mins
- IR - SRV - XYZ - User Modified Files on FileServerX > 1000 DELETES in an hour
- IR - SRV - XYZ - User Modified Files on FileServerX > 1000 Write/Adds in an hour
- IR - SRV - XYZ - User Modified Files on FileServerX > 1000 Write/Adds in an hour - LONG LIST
- IR - WHO is doing WHAT on a system

- IT - User Logon & Email Activity Report - Specify Period
- IT - User Processes Activity Report - Specify Period

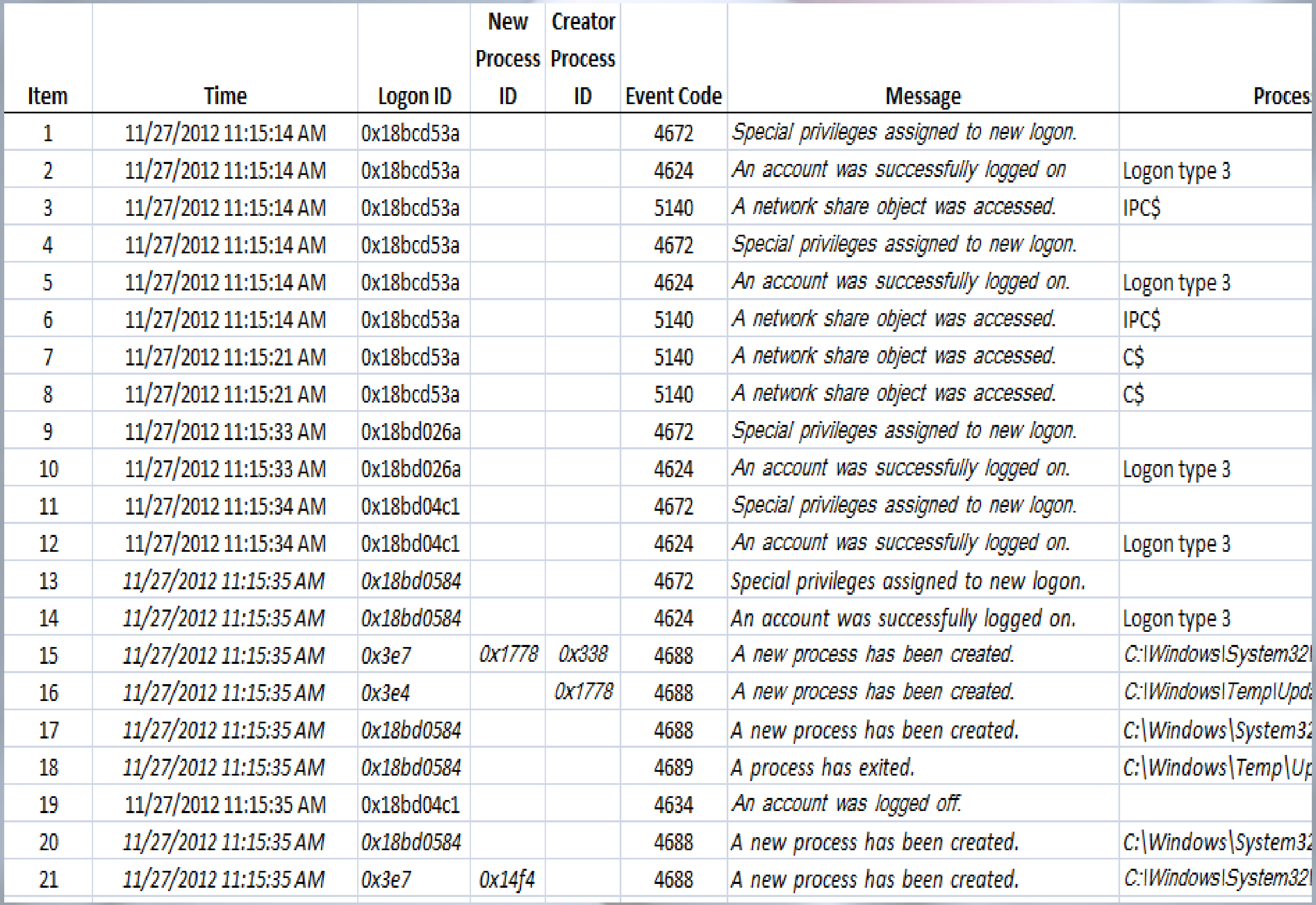
Where did they go?



166 of 252,446 events matched

_time	host	Application_Name	Direction	Source_Address	Source_Port	Destination_Address	Destination_Port	Co_Code	Region	City	Country_Name
2014-03-11 12:37:55	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	12001	131.253.40.50	80	CA	ON	Ottawa	Canada
2014-03-11 12:25:08	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	10141	131.253.34.142	80	CA	ON	Ottawa	Canada
2014-03-11 08:33:59	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	50382	70.38.0.134	80	CA	QC	Montréal	Canada
2014-03-11 13:23:09	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	16934	80.237.133.31	80	DE	07	Höst	Germany
2014-03-11 13:22:26	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	16839	87.230.41.180	80	DE	07	Höst	Germany
2014-03-11 13:22:26	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	16833	195.3.248.10	80	DE			Germany
2014-03-11 07:48:15	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	48319	88.198.50.132	443	DE	02	Nürnberg	Germany
2014-03-11 13:37:32	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	17905	82.103.140.40	443	DK			Denmark
2014-03-11 13:47:50	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18263	83.145.197.2	80	FI			Finland
2014-03-11 13:45:12	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18177	83.145.197.2	443	FI			Finland
2014-03-11 11:06:29	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	3098	88.191.250.18	80	FR	A8	Paris	France
2014-03-11 08:33:59	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	50376	212.85.158.4	80	FR			France
2014-03-11 13:22:54	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	16913	178.255.83.1	80	GB			United Kingdom
2014-03-11 13:22:31	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	16848	176.32.101.58	80	NL			Netherlands
2014-03-11 14:13:39	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	19090	199.59.150.46	443	US	CA	San Francisco	United States
2014-03-11 14:13:14	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	25356	192.241.180.162	443	US			United States
2014-03-11 14:06:12	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18900	128.121.22.133	443	US	CO	Englewood	United States
2014-03-11 13:52:53	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18438	74.125.227.131	443	US	CA	Mountain View	United States
2014-03-11 13:52:53	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18436	74.125.227.101	443	US	CA	Mountain View	United States
2014-03-11 13:52:11	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18410	74.125.227.128	80	US	CA	Mountain View	United States
2014-03-11 13:52:11	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18408	74.125.227.103	80	US	CA	Mountain View	United States
2014-03-11 13:48:47	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18295	209.8.115.81	80	US	TX	Dallas	United States
2014-03-11 13:41:56	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	18072	128.121.22.160	80	US	CO	Englewood	United States
2014-03-11 13:37:55	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	17929	12.169.107.140	80	US	TX	Leander	United States
2014-03-11 13:37:32	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	17907	50.63.243.230	80	US	AZ	Scottsdale	United States
2014-03-11 13:36:12	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	17863	23.64.171.27	80	US	MA	Cambridge	United States
2014-03-11 13:36:12	[redacted]	Your Browser IE, FF, Chrome	Outbound	[redacted]	17859	38.127.167.7	443	US	VA	Vienna	United States

Event - Spreadsheet



Item	Time	Logon ID	New Process ID	Creator Process ID	Event Code	Message	Proces
1	11/27/2012 11:15:14 AM	0x18bcd53a			4672	*Special privileges assigned to new logon.*	
2	11/27/2012 11:15:14 AM	0x18bcd53a			4624	*An account was successfully logged on*	Logon type 3
3	11/27/2012 11:15:14 AM	0x18bcd53a			5140	*A network share object was accessed.*	IPC$
4	11/27/2012 11:15:14 AM	0x18bcd53a			4672	*Special privileges assigned to new logon.*	
5	11/27/2012 11:15:14 AM	0x18bcd53a			4624	*An account was successfully logged on.*	Logon type 3
6	11/27/2012 11:15:14 AM	0x18bcd53a			5140	*A network share object was accessed.*	IPC$
7	11/27/2012 11:15:21 AM	0x18bcd53a			5140	*A network share object was accessed.*	C$
8	11/27/2012 11:15:21 AM	0x18bcd53a			5140	*A network share object was accessed.*	C$
9	11/27/2012 11:15:33 AM	0x18bd026a			4672	*Special privileges assigned to new logon.*	
10	11/27/2012 11:15:33 AM	0x18bd026a			4624	*An account was successfully logged on.*	Logon type 3
11	11/27/2012 11:15:34 AM	0x18bd04c1			4672	*Special privileges assigned to new logon.*	
12	11/27/2012 11:15:34 AM	0x18bd04c1			4624	*An account was successfully logged on.*	Logon type 3
13	*11/27/2012 11:15:35 AM*	*0x18bd0584*			4672	Special privileges assigned to new logon.	
14	*11/27/2012 11:15:35 AM*	*0x18bd0584*			4624	An account was successfully logged on.	Logon type 3
15	*11/27/2012 11:15:35 AM*	*0x3e7*	*0x1778*	*0x338*	4688	*A new process has been created.*	*C:\Windows\System32\*
16	*11/27/2012 11:15:35 AM*	*0x3e4*		*0x1778*	4688	*A new process has been created.*	*C:\Windows\Temp\Upd*
17	*11/27/2012 11:15:35 AM*	*0x18bd0584*			4688	*A new process has been created.*	C:\Windows\System32
18	*11/27/2012 11:15:35 AM*	*0x18bd0584*			4689	*A process has exited.*	C:\Windows\Temp\Up
19	11/27/2012 11:15:35 AM	0x18bd04c1			4634	*An account was logged off.*	
20	*11/27/2012 11:15:35 AM*	*0x18bd0584*			4688	*A new process has been created.*	C:\Windows\System32
21	*11/27/2012 11:15:35 AM*	*0x3e7*	*0x14f4*		4688	*A new process has been created.*	*C:\Windows\System32\*

Monitor Accounts

- Account - Attempt to change Account Password - Last 24 hours
- Account - Domain Connection issue - Last 24 hours
- Account - Failed Guest and Administrator Logins - Last 24 hours
- Account - Local Group changed - Last 30 days
- Account - Logon Type by Count - Last 24 hours
- Account - Logon by Type 8 - CLEAR TEXT Login - Last 24 hours
- Account - Logon by Type 10 - RDP Login - Last 24 hours
- Account - Logon by Type - Last 15 mins
- Account - SRV - Successful Logins of NON-User Accounts - Last hour
- Account - User Account Attempted Password Change - Last 7 days
- Account - User Account DELETED - Last 7 days
- Account - User Account ENABLED - Last 7 days
- Account - User Account Locked Out - Last 24 hours
- Account - User Account Password changed - Last 7 days
- Account - User Account UNLOCKED - Last 7 days
- Account - User Account password reset - last 7 days
- Account - User Account was DISABLED - Last 30 days
- Account - User failed to logon - Last 24 hours
- Account - User locked out of domain - Last 24 hours
- Account - User successfully logged on - Last hour
- Account - User successfully logged on - NOT Exchange - Last hour
- Account - User successfully logged on Exchange - Last hour
- Account - WS/SRV - Account failed to logon - Last 24 hours
- Account - WS/SRV - Account login with explicit credentials - Last 24 hours
- Account - WS/SRV - User added to group - Last 24 hours

Lots more

- Application Crash - Application Error - Last 24 hours
- Application Crash - Windows Error Reporting - Last hour
- Audit Policy - SRV - Audit Policy changed - Last 24 hours
- Audit Policy - WS - Audit Policy changed - Last 7 days
- Client - DC Issue with distant clients contacting a DC - Last 24 hours
- Commands - Registry related commands executed - Last hour
- Commands - SRV - CScript.exe executed - By Count - Last 30 days
- Commands - SRV - Net.exe Net1.exe used - By COUNT - Last 24 hours
- Commands - SRV - Net.exe Net1.exe used - Last 24 hours
- Commands - SRV - Schtasks and AT executed - Last 30 day
- Commands - Suspicious commands being executed - Last 24 hours
- Commands - WS - CScript.exe executed - By Count - Last 30 days
- Commands - WS - Net.exe Net1.exe used - Last 24 hours
- Commands - WS - Schtasks and AT executed - Last 30 day
- DNS - Internal Source IP to Domain/IP - Last hour
- DNS - Known Bad IP's - ALL TIME DNS - RegEx IP and Record - Last Hour
- DNS - SRV - Names not resolving
- DNS - WS - Systems where hostname does not match Computer Name - Last 30 days
- Driver - Issue with driver - last 24 hours

And more

- Exchange - Mail Server having issues
- Exchange - Successful Webmail Logon Count by IP
- Exchange - Successful Webmail logins
- Exchange - Failed Email delivery - Last hour
- Exchange - Failed Mobile device email login > 10 last hour
- Exchange - Failed OWA login last hour
- Exchange - Failed Email delivery - Last hour
- Exchange - Failed Mobile device email login > 10 last 24 hours
- Exchange - Failed Mobile device email login > 10 last hour
- Exchange - Failed OWA login last 24 hours
- Exchange - Failed OWA login last hour
- Executables - SRV - New File dropped in monitored locations - Last 30 days
- Executables - WS - New File dropped in monitored locations - Last 30 days
- GPO - Group Policy Failed - Last 7 days

Yet more

- Kerberos - List of Kerberos tickets - Last 24 hours
- Logs - SRV - Cleared - Last 7 days
- Logs - SRV - Logs low on events - Last 24 hours
- Logs - WS - Cleared - Last 7 days
- Logs - WS - Logs low on events - Last 24 hours
- SRV - Files Modified on ServerX - Last 4 hours
- NTFS - NTFS Error - Last 7 days
- OS Version - SRV - What OS, SP, CPU type - Last 30 days
- OS Version - WS - What OS, SP, CPU type - Last 30 days
- Firewall - Threats - Last Hour
- Firewall - Traffic - Last Hour
- Printing - Printer Failed - Last 30 days
- Privileged Object - SRV - Last 24 hours
- Privileged Object - WS - Last 24 hours
- Processes - SRV - New Process being launched - Last 60 mins
- Processes - WS - New Process being launched - Last 60 mins

Product, Registry & SNMP

- Product - SRV - Installation Started - Last Day
- Product - SRV - Installation Status All - Last Day
- Product - SRV - Installation Status OTHER - Last 30 Days
- Product - SRV - Windows Installer Status - Last Day
- Product - SRV - Windows Update - Last 24 hours
- Product - WS - Installation Started - Last Day
- Product - WS - Installation Status All - Last Day
- Product - WS - Installation Status OTHER - Last 30 Days
- Product - WS - Windows Installer Status - Last Day
- Product - WS - Windows Update - Last 24 hours
- Registry - Key Changed - Last 24 hours
- Registry - Key value Add, Change, Delete - Last 24 hours
- Registry - Run & RunOnce Key value Add, Change, Delete - Last 24 hours
- SNMP - SNMP Service Config updated - Last 7 days

Services & Shares

- Service - SRV - Issues with startup or failure - Last 24 hours
- Service - SRV - New SERVICE Installed - Last Hour
- Service - SRV - SERVICE state changed 'to disabled' - Last 24 hours
- Service - SRV - Service Failed to Start - last 7 days
- Service - State - Startup or Failure - Last 24 hours
- Service - WS - Issues with startup or failure - Last 24 hours
- Service - WS - New SERVICE Installed - Last Hour
- Service - WS - SERVICE state changed 'to disabled' - Last 24 hours
- Service - WS - Service Failed to Start - last 7 days

- Shares - WS - C$ Share being accessed - Last 24 hours
- Shares - WS - C$ or Admin$ Share accessed - Last 24 hours

And Finally

- System Integrity - SRV - File Hash are not valid - Last 24 hours
- System Integrity - WS - File Hash are not valid - Last 24 hours
- Tasks - New Task Scheduled - Last Hour
- Tasks - Task Scheduled Created, Changed or Deleted - Last Hour
- Time - SRV - Time Service sync details - Last 24 hours
- Time - SRV - When a system rebooted - last 24 hours
- Time - WS - Time Service sync details - Last 24 hours
- Time - WS - When a system rebooted - last 24 hours
- USB - Status of USB drives used - Last 7 days
- VPN - FAILED logins Last Hour VPN - Successful logins Last Hour
- WinRM - SRV - WinRM Service status - Last 30 days
- WinRM - WS - WinRM Service status - Last 30 days

Resources

- Our Website
  - www.MI2Security.com

- The Handout – Windows Logging Cheat Sheet

Questions?

- You can find us at:
- Michael@MI2Security.com

- @HackerHurricane
- @MI2Security
- www.MI2Security.com

- Yes – We do consulting ;-)