Cuckoo Sandbox and Dynamic Malware Analysis

Google Images

Slides: https://github.com/lehuff/BSides_Philly

Presentation by:
Lane Huff
lhuff@secure-innovations.net
Twitter: @skankinmonkey

Secure Innovations

… Or am I "Cuckoo for Malware?"

Agenda

- Who am I?
- What is Dynamic Malware Analysis?
- What is Static Malware Analysis?
- Cuckoo Overview
- Hiding from Malware
- Looking at Malware

Who am I?

Lane Huff

- Security Engineer at Secure Innovations
- Blog Author & Podcast Participant with Primal Security
- Open Source Contributor
- World Traveler
- Twitter: @skankinmonkey

Secure Innovations

What is Dynamic Malware Analysis?

It is Testing and Evaluating Programs in Real Time

- Running an executable
- Loading a DLL
- Opening a document
- Playing audio/video
- Opening a zip file

...and much More!

But wait! …

… Let's back up a little first!

Secure Innovations

Static Analysis

- **Static Analysis** is analyzing a file at rest
  - It can be any of the files previously mentioned
  - Memory Dumps (Volatility)
  - Network Data (tcpdump/Wireshark)
- Executables use debuggers
  - IDAPro
  - OllyDBG
  - Immunity

Static Analysis

- File Metadata
  - Reported file/MIME-type
  - MD5/SHA values
  - Version
  - Company Name
  - Application Name

...lots of information

Static Analysis

CompanyName	_PDMNeO
Comments	·l5ll.lwu
ProductName	L4w YLRvnkt
ProductVersion	5.4.6l3.4788
FileDescription	¯72l6b[
OriginalFilename	¯72t6b¯.exe

LegalCopyright	Copyright (C) 2005-2014 QhEznb PIaRjJCa6JY

Static Analysis

- Signing Certificates
  - Is the file signed?
  - Who signed it?
  - Indicator of CA compromise?

Static Analysis

'Spymel' Is Latest Example Of Attackers Using Signed Malware

Presents an Authenticode digital signature

md5_fingerprint: 73c27cdff2b041c8c2d35e749e86847c8
cn: SBO INVEST
sha1_fingerprint: 3a8412582563f43dd28aa1f31cdd0d0c6d78fd60
sn: 207789172986866458848936819203273666484

The highly obfuscated spyware dubbed Spymel is digitally signed with a certificate that was originally issued by certificate authority DigiCert to an entity named SBO Invest. DigiCert has since revoked the certificate but a newer version of Spymel has surfaced using another certificate issued to SBO Invest, Zscaler said.

http://www.darkreading.com/vulnerabilities---threats/spymel-is-latest-example-of-attackers-using-signed-malware-/d/d-id/1323805

Static Analysis

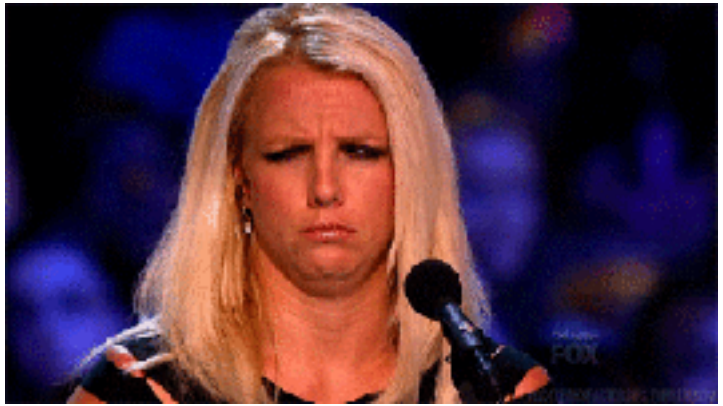
PDB Path c:\Documents and Settings\Administrator\My Documents\Visual Studio 2008\Projects\testing\Release\WindowsSecurityService.pdb

- Development environment
  - Compile time
  - Original filename
  - Development environment
  - Host system remnants
    - Paths
    - System language

Static Analysis

Reported Checksum	0x00000000
Actual Checksum	0x0000784
Minimum OS Version	4.0
Compile Time	1992-06-19 18:22:17

Windows NT 4.0 RTM: July 31, 1996



Static Analysis

- Compression/Obfuscation Tools
  - .NET Obfuscators
  - ‘Weird’ variable names

Static Analysis

```
SmartAssembly.SmartUsageWithUI.ConfirmFeatureUsageReportingForm.resources
SmartAssembly.SmartUsageWithUI.Resources.current.png
SmartAssembly.SmartUsageWithUI.Resources.data.png
SmartAssembly.SmartUsageWithUI.Resources.error.png
SmartAssembly.SmartUsageWithUI.Resources.error16.png
SmartAssembly.SmartUsageWithUI.Resources.network.png
SmartAssembly.SmartUsageWithUI.Resources.ok.png
SmartAssembly.SmartUsageWithUI.Resources.{logo}.png
SmartAssembly.SmartUsageWithUI.Resources.warning16.png
SmartAssembly.SmartUsageWithUI.Resources.default.ico
```

```
"Powered by SmartAssembly 6.8.0.121
Ghttp://www.smartassembly.com/webservices/UploadReportLog.n/GetServerURL
@http://www.smartassembly.com/webservices/Reporting/UploadReport2
```

Static Analysis

```
Sub AuLoOpen()
    VNAUWQD = "1,213k1,12 hj1kh21"
    HuhdDww
End Sub
Sub Workbook_Open()
    HuhdDww
End Sub
Sub HuhdDww()
    LiqUachi
End Sub
Sub LiqUachi()
Dim bbgd As Boolean, sss As Integer, YGIW As String
sss = -55 + 54
HYII = "I" & "IM"
HYTE = HYTE & "P"
bbgd = False
On Error Resume Next
Dim WOIEW As String
TTGDFW = LyhJb(3 + 90 + sss)
DBDDW = Environ(HYII) & TTGDIW
JIEKR = " " & "mp" & ""
FFDRRF = "" & " r--"
LQwDO = DBDDW

FFFNNNF = LQwDO + "nj12h" + FFDRRF
SSHHDD = DBDDW & "dhaj" & FFDRRF
WOIEW = DBDDW & "" & "y1" & JIEKR
```

```
HHgGvvv (TTNHHF)
HHgGvvv (SS-HDJ)

Module7 Tyryka (7)
BH.ASD = Chr(102 + 8)
Set yyGvvGgv = CreateObject("  & '' & 'W' & '' & "o" & "d." & "Application  & BHJASJ)
yyGvvGgv.Visible = bbgd
yyGvvGgv.Documents.Open (  FNNH)
Module1  yryka (8)
HYJASGT   Module1.Draw(mCTFW)
Module1 Tyryka (3)
yyGvvGgv.Qu..
Set yyGvvGgv   Nothing
End Sub
Public Function LyhJb(wwww As Integer)
    LyhJb = Chr(wwww)
End Function
Public Function  HgGvvv(fffe As String)
    ActiveDocument.SaveAs FileName:=fffe, FileFormat:=3
End Function
Sub Auto_Open()
    LiqUachi
End Sub
```

… But what does the program actually do?

Google Images

(Re)introducing Dynamic Analysis — *Why?!*

- Obfuscation/Compression/ Encryption Techniques may mask true intentions of a file.
- Malware authors don't want to make analysis easy!

Secure Innovations

(Re)introducing Dynamic Analysis

Some options for dynamic analysis:

- ➢Run on your System!
- ➢Run on a VM
- ➢Run on an Isolated (Physical) System

**None of these options are ideal or easy to work with and are not very 'dynamic.'*

Cuckoo Sandbox

- Malware Analysis Platform
  - WinXP (x86), Windows 7 (x86, x86_64 (beta))
  - Linux (beta)
  - Android (beta)
- Sandbox Architecture
  - VirtualBox
  - KVM
  - VMWare Workstation
  - VMWare ESXi
  - XenServer
  - Bare Metal

Cuckoo Sandbox (cont.)

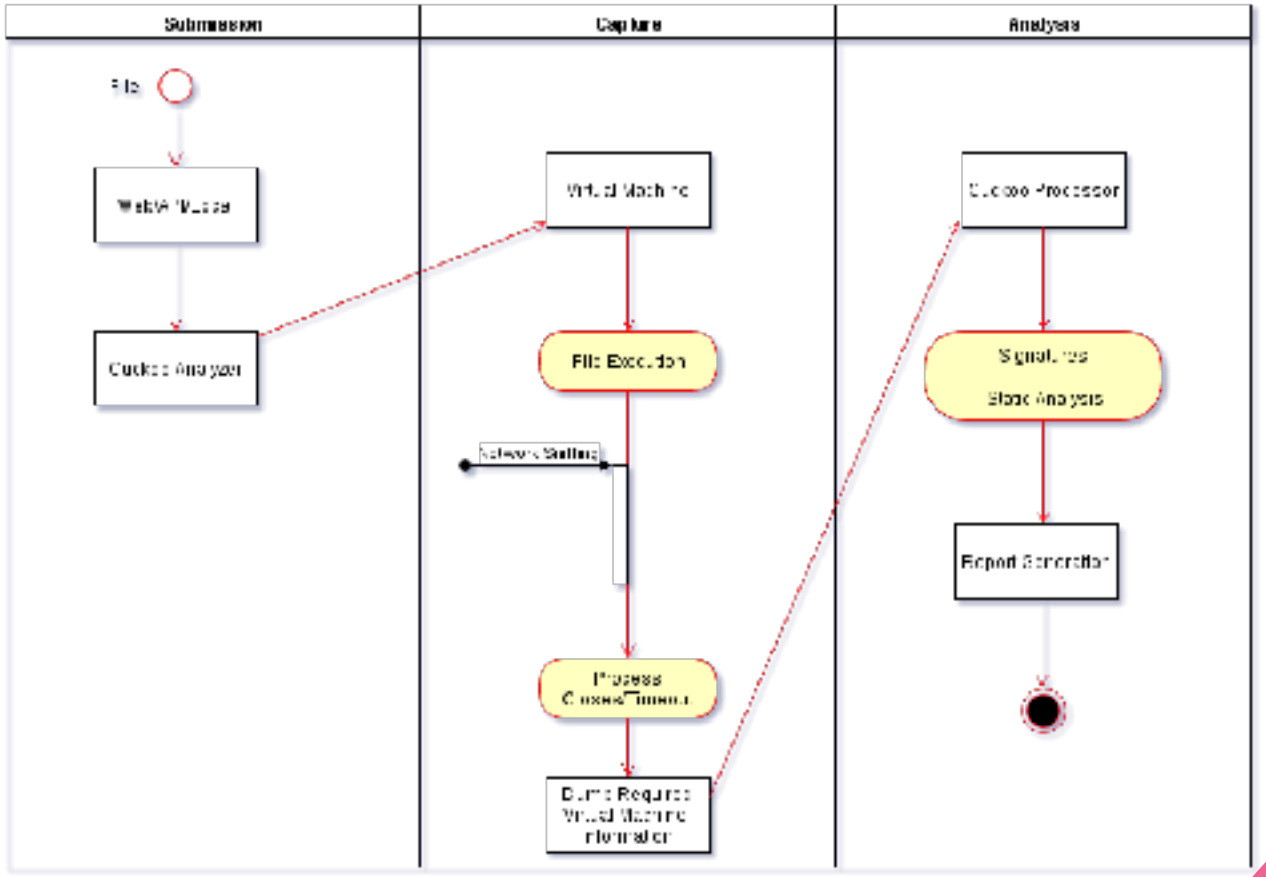
- Registry Analysis
- Process Analysis
- Network Analysis
- Memory Analysis*
- Kernel Analysis
- Dropped File Analysis
  - … and Static Analysis!

*Using Volatility

Architecture Challenges

- Nesting Cuckoo
  - 32-bit
  - Resource competition
- Flat is more scalable
  - ...but harder to manage (ESX)
- Consider your goal!
  - Personal deployment?
  - Enterprise?
  - Sharing with friends?

How does it work?



To summarize…

Step 1:

➢Submit a file

To summarize…

Step 1:

- ➢ Submit a file

Step 2:

- ➢ Cuckoo sends file to a VM for execution

To summarize…

Step 1:

➢Submit a file

Step 2:

➢Cuckoo sends file to a VM for execution

Step 3:

➢Cuckoo performs analysis on the returned information

To summarize…

Step 1:

➢Submit a file

Step 2:

➢Cuckoo sends file to a VM for execution

Step 3:

➢Cuckoo performs analysis on the returned information

Step 4:

➢ Reports are generated

Cuckoo Distributions

- Main Distribution:
  https://www.cuckoosandbox.org/

- Brad Spengler's 1.2 Fork (Spender-Sandbox):
  https://github.com/spender-sandbox/cuckoo-modified

Cuckoo Forks Unique Features

Cuckoo 1.2

- 32-bit Windows Analysis only
- Good documentation
- Community Signatures (*not actively maintained anymore*)
- Stable!
- Old (March 2015)
- Execution graph

Cuckoo Features

Cuckoo 2.0 RC2

- 32/64-bit Windows support
- Android/OSX/Linux support *(no documentation yet)*
- Import/Export reports
- Maintained set of Community Signatures
- Suricata/Snort Integration
- MITM support for Encrypted Traffic
- Malware Scoring support *(very bad right now)*
- Sandbox Baselining *(memory-only)*

Cuckoo Forks Unique Features

Spender Sandbox

All the Features of 1.2 plus …

- ➢32/64-bit Windows support
- ➢Normalized Registry Names
- ➢Service monitoring
- ➢Better signatures *(and maintained!)*
- ➢Per-Analysis commenting
- ➢Better at evading Anti-Sandbox and Anti-VM tools
- ➢Malware Scoring *(pretty good)*
- ➢Very stable and good documentation

… and more! (regular updates to Git.)

Comparison

Feature	2.0 RC2	Spender
32/64bit Windows 7	✓	✓
Android/OSX/Unix	✓	x
Community Signatures	✓	✓
Suricata/Snort Integration	✓	✓
Normalized Registry Keys	x	✓
Commenting	x	✓
Scoring	✓	✓
Baselining	✓	x

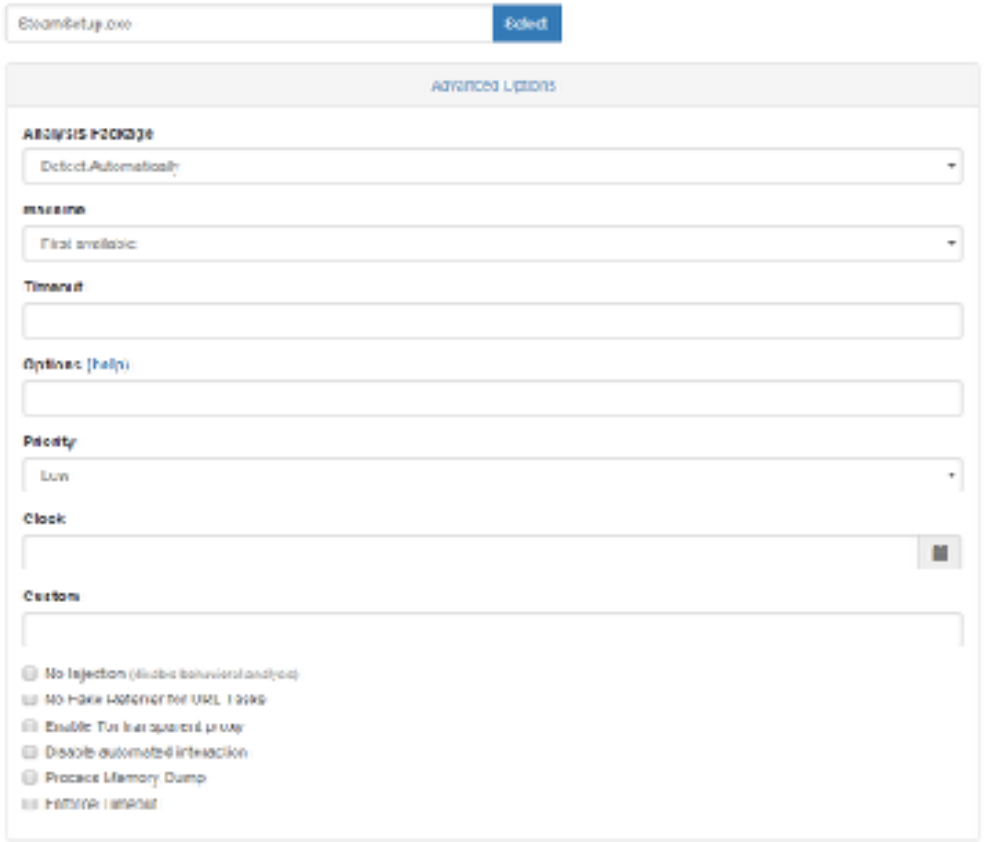
Analysis Packages

- (Java) applet
- bin(ary data)
- Cp1 (control panel applets)
- Dll
- Doc (Word)
- Exe
- Generic (via cmd.exe)
- HTML
- IE (for URL)

… Automatic Detection (usually)

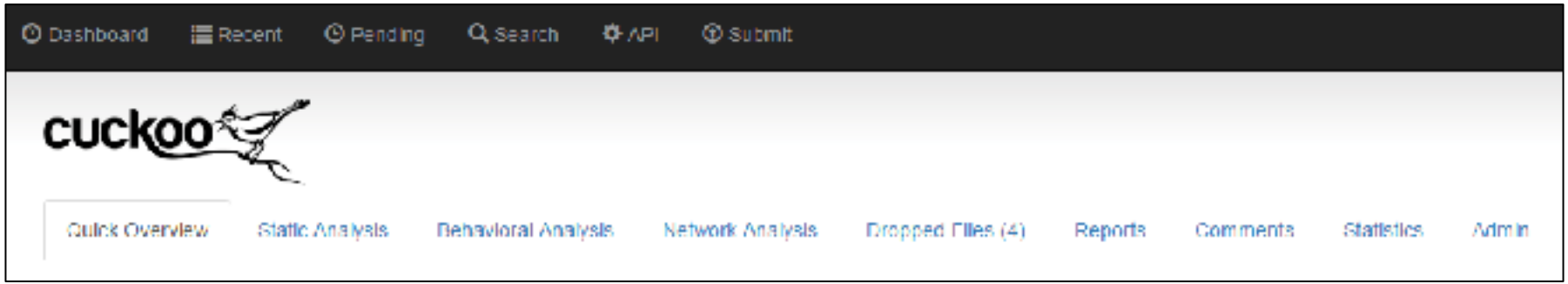
- Jar
- MSI
- PDG
- PPT
- PS1 (Powershell)
- Vbs (VBScript)
- Xls (Excel)
- Zip

Submission Options



- Package Selection
- Machine Selection
- Override Timeout Value
- Set Clock Options (Spender-Only)
- Disable VM-Interaction
- Memory Analysis

Overview Page



- File Details
  - SSDEEP
  - Yara
- Signatures
  - Community based
  - Customizable
  - Severity
- Network Traffic (DNS/Host)
- File/Process/Registry activity

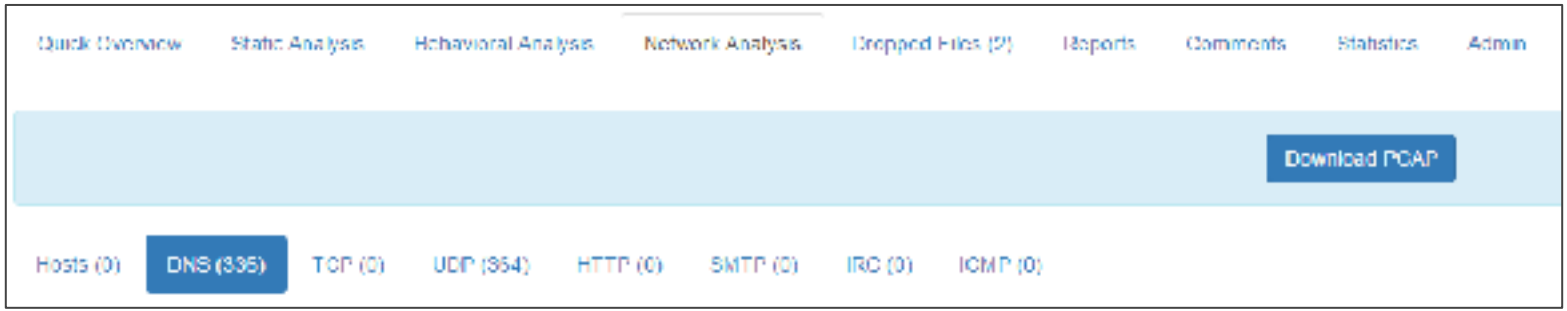
Static Analysis Page

- PE Information
  - Reported/Actual Checksum
  - Compile Time
- Version Information
  - File metadata (author, etc)
- Memory Sections
  - Virtual Size/Raw Size
- Imports
  - Kernel, other system calls
- Strings
- Antivirus (VirusTotal)

Behavioral Analysis Page

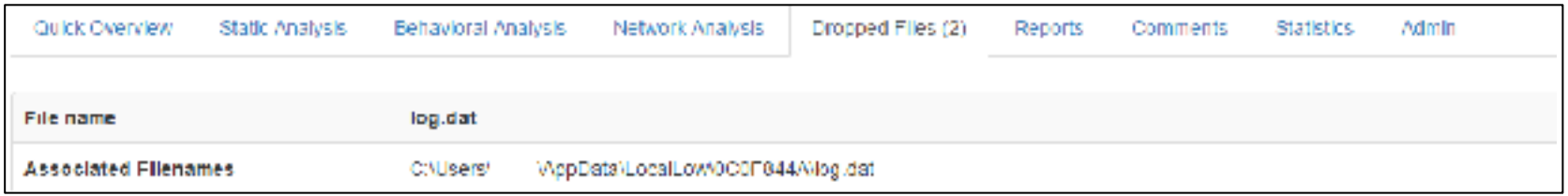
- Process Tree
  - Useful for viewing execution flow
- Per process ‘action’ breakdown

Network Analysis Page



- ➢Breakdown by Type of Traffic
  - Post-Analysis Lookup *(via VirusTotal)*
  - Can view Packet Information *(Useful for plaintext Data!)*
- ➢Downloadable PCAP File

Dropped Files Page



- List of Files Created during Execution of Submitted File
- Similar Information to Static Analysis Page
- Search VirusTotal for File
- Download Dropped File for Submission

Additional Pages

Reports

- Download generated reports for the analysis
  - JSON
  - HTML
  - Summary HTML
  - PDF
  - *..and more if set in reporting.conf*

Comments

- Per-analysis notes

Statistics

- Speed of Modules, Signatures, Reports

Admin

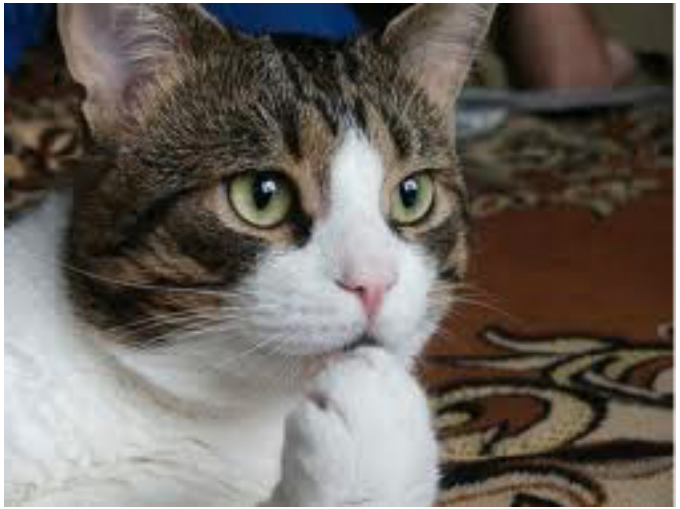
- Job ID
- Mongo DB ID
- Delete Job

Let's change gears again!

Secure Innovations

Malware authors are smart.
They know we're looking for them!

What are some methods used to detect analysis?



Indicators for Sandbox/Analysis

- Process Names
- Registry Entries
- Device Names
- MAC Addresses
- Default System Settings
- IP Addresses
- Auto-Start Entries
- Start Menu Items
- Date/Time

(This list is always growing and methods are being changed.)

Detection Countermeasures

- Manually Sanitize:
  - VM-Related Registry Keys
  - Device Names
- Change MAC address to a ‘Physical’ Device Address
- Don’t Install VMWare Tools/VirtualBox Additions
- Make your System Look ‘Used’
  - Install Applications
  - Use the Browser Some
  - Multiple Users on a System
- More than 1 CPU
- More than 2GB of RAM

Detection Countermeasures

VMCloak

- Automated Virtual Machine Generation and Cloaking for Cuckoo Sandbox
- Can install Various Versions of Windows (XP, 7, 8, 10) and OSX
  - Can add Optional Applications on top of installation
    - Adobe
    - .NET
    - Office
    - *...and more!*
- Applies a Set of Configuration Options to Avoid VM/Sandbox Detection
- Can automatically add the VM to your Cuckoo install
- More info: http://jbremer.org/vmcloak3/
- Download: https://github.com/jbremer/vmcloak

Verify your Anti-Anti-Countermeasures!

PAFish (Paranoid Fish)

- Executable which emulates Anti-Analysis/Sandbox Techniques
- Submit to your Sandbox and View Results to see where your VM lacks
- Not updated often, but still useful
- Download: https://github.com/a0rtega/pafish

One Last Note on VMs

Malware Behaves Differently in Different Environments *(Shocking!)*

- ➢ Thorough analysis requires multiple environments for testing
- ➢ Different software loads (Adobe 9, 10, WinZip, 7Zip, etc.)
- ➢ Different versions of Internet Explorer; Other Web Browsers
- ➢ Try with and without EMET

Microsoft provides some useful images for testing different browsers:

https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

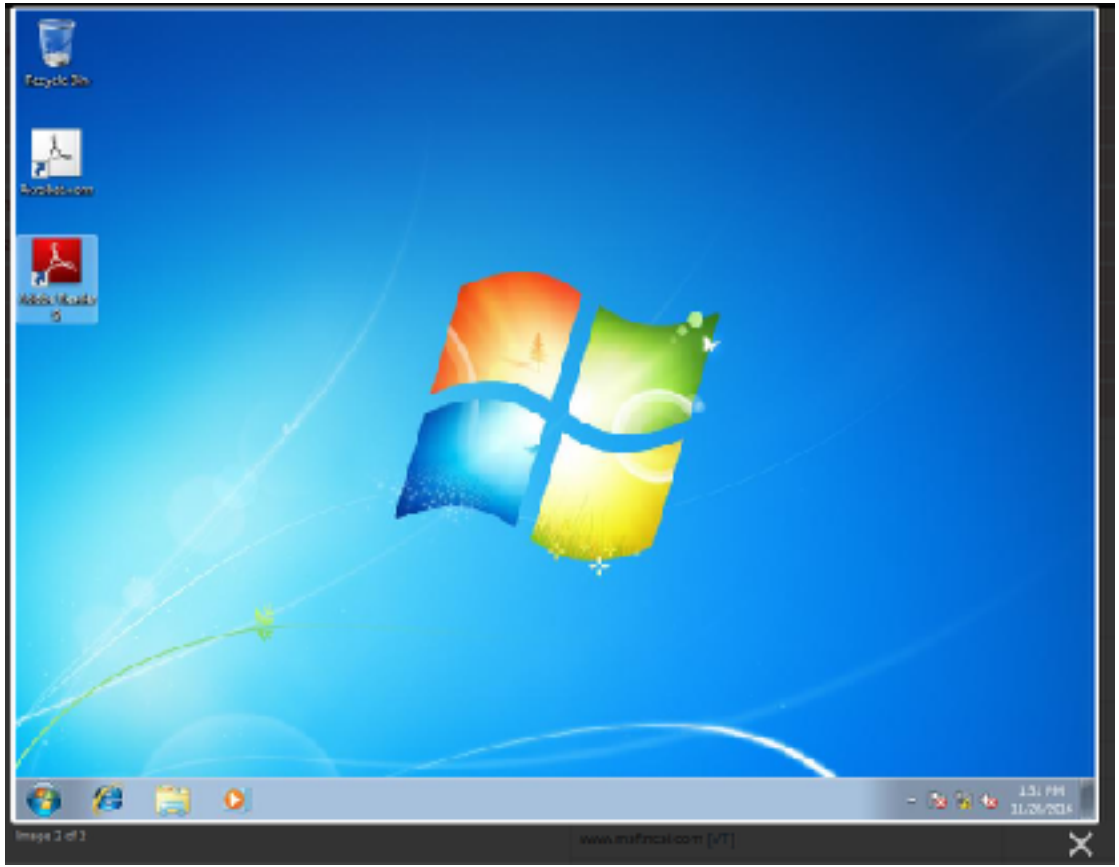
IE8 on Win7
IE9 on Win7
IE10 on Win7
IE11 on Win7
IE11 on Win81
Microsoft Edge on Win 10 Stable (13.10586)
Microsoft Edge on Win 10 Preview (14.14366)
MSEdge on Win10_preview

Let's Look at Malware!

Secure Innovations

News.exe

Sha256: 039058cd0f349c8987a4a61a3de12660b78007235126ee75228933fda2343e4f



News.exe

Sha256: 039058cd0f349c8987a4a61a3de12660b78007235126ee75228933fda2343e4f

‘Syrian Malware’ (Bladabindi Backdoor)

Static Information:

- Compile Time: 2014-10-05 16:05:59
- LegalCopyright: Copyright \xa9 2005
- InternalName/OriginalFilename: 5.exe

Sandbox Results:

- DNS Call: aliahmahhmod.zapto.org
- Multiple Startup Registry Keys created
- Invokes user32.dll.GetAsyncKeyState - Keylogger!

News.exe

Sha256: 039058cd0f349c8987a4a61a3de12660b78007235126ee75228933fda2343e4f

Execution Tree

- news.exe 2804
  - news.exe 2976
    - chrome.exe 976
      - chrome.exe 2332
        - netsh.exe 2296 *netsh firewall add allowedprogram "C:\Users\ \AppData\Local\Temp\chrome.exe" "chrome.exe" ENABLE*
- services.exe 496 C:\Windows\system32\services.exe
  - svchost.exe 616 C:\Windows\system32\svchost.exe -k DcomLaunch
    - WmiPrvSE.exe 2616 C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
  - svchost.exe 872 C:\Windows\system32\svchost.exe -k netsvcs
  - svchost.exe 1332 C:\Windows\system32\svchost.exe -k netsvcs
  - svchost.exe 1968 C:\Windows\System32\svchost.exe -k netsvcs
  - svchost.exe 1680 C:\Windows\System32\svchost.exe -k WerSvcGroup

Signatures

- Creates RWX memory
- A process attempted to delay the analysis task.
- Checks the Windows Registry for the systems install date; commonly used in malware
- Drops a binary and executes it
- The binary likely contains encrypted or compressed data.
- Uses the Smart Assembly obfuscator to hide .NET code
- Executed a process and injected code into it, probably while unpacking
- Sniffs keystrokes
- Queries information on disks, possibly for anti-virtualization
- Installs itself for autorun at Windows startup
- Retrieves Windows ProductID, probably to fingerprint the sandbox
- File has been identified by at least ten AntiViruses on VirusTotal as malicious
- Checks the version of Bios, possibly for anti-virtualization
- Creates a copy of itself
- Collects information to fingerprint the system
- Creates or deletes or executes a type library file

News.exe

Sha256: 039058cd0f349c8987a4a61a3de12660b78007235126ee75228933fda2343e4f

Loader.exe

sha256: ffb4a81fc336b1d77c81eef96eab0a5249ebb053c8920dd0c02e1d9f3ac257b0

Chimera Ransomware

- Accessed file lists spider important directories
  - For every deleted file there is a new file
    - With a .crypt extension!
  - Also: YOUR_FILES_ARE_ENCRYPTED.HTML

Secure Innovations

Loader.exe (26)

Chimera Ransomware

- Static IP calls
- Attempts to identify local system public IP address
- Windows crypto functions utilized:
  - Advapi32.dll
  - cryptsp.dll

```
advapi32.dll.CryptAcquireContextA
advapi32.dll.CryptReleaseContext
advapi32.dll.CryptCreateHash
advapi32.dll.CryptDestroyHash
advapi32.dll.CryptHashData
advapi32.dll.CryptGetHashParam
advapi32.dll.CryptImportKey
advapi32.dll.CryptExportKey
advapi32.dll.CryptGenKey
advapi32.dll.CryptGetKeyParam
advapi32.dll.CryptDestroyKey
advapi32.dll.CryptVerifySignatureA
advapi32.dll.CryptSignHashA
advapi32.dll.CryptGetProvParam
advapi32.dll.CryptGetUserKey
advapi32.dll.CryptEnumProvidersA
```

```
cryptsp.dll.CryptAcquireContextA
cryptsp.dll.CryptGenRandom
cryptsp.dll.CryptReleaseContext
```

Autohotkey.exe

sha256: e03e2d150b8135cfb330394c35f9bf372801b8a7c52a7a271db0a4ee46abbdd7

Petya Ransomware

- Scans drive for Antivirus
- Modifies \??\PhysicalDrive0
- Similar Crypto calls to Chimera
- Invokes ntdll.dll.NtRaiseHardError

NtRaiseHardError	ErrorStatus: 0xc0000350 ResponseOptions: 6

Autohotkey.exe

sha256: e03e2d150b8135cfb330394c35f9bf372801b8a7c52a7a271db0a4ee46abbdd7

Petya Ransomware

- \??\PhysicalDrive0 - What is this?
- Modified Bootloader
- Crash Host, Reboot (NTRaiseHardError)
- Custom Kernel which encrypts system on Startup
- Cuckoo 2.0 RC2 - Analysis Reboot Survival (*beta*)

More info on Petya: https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

This is just the beginning!

There is so much more out there to learn.

Secure Innovations

Useful Resources

- Malware Analyst's Cookbook
- Practical Malware Analysis
- The Art of Memory Forensics
- Twitter:
  - @PhysicalDrive0 - Cool Malware Resource
  - @skier_t - Cuckoo Author
  - @botherder - Cuckoo Author
  - @skankinmonkey - Me!
- Reddit: /r/malware /r/netsec
- http://www.primalsecurity.net/ Blog and Podcast!
- https://infosecspeakeasy.org/

Questions?

Lane Huff, Security Engineer

lhuff@secure-innovations.net

Twitter: @skankinmonkey

Blog/Podcast: http://www.primalsecurity.net/

Slides: https://github.com/lehuff/BSides_Philly

Secure Innovations