Forensics 101

Brian Johnson, 7 Minute Security

Agenda

- Triage a suspect machine
- Analyze drive for malware, Web history & other artifacts
- Sniff the network for badness

Why this talk?

Help find "bad stuff" quickly with:

- Limited staff and budget
- No centralized logging/alerting
- Want "cheap" triage before calling in the big guns

Disclaimer: we won't be doing this…

Lets start with a common scenario

"Hello, IT?
My wallpaper is now a skull and crossbones and…"

"…No, ***I*** didn't click anything bad!!!!"

Remove Malware

Removing malware

Antivirus 2010

Antivirus 2010
Stay protected from the latest threats

Registration | Help

- System Scan
- Security
- Privacy
- Update
- Settings

Antivirus 2010: Status

Protection level: low — Low | Medium | High

Recommendation:
Update antivirus

Virus Protection	NOT FOUND
Spyware Protection	NOT FOUND
General Security	NOT FOUND
Automatic Updating	NOT FOUND

Scan Now
Check your computer for viruses and other threats

Update Now
Download the latest protection to help keep your PC safe

Removing malware

Isolate network connectivity!

Unplug or isolate!

Removing malware

Isolate network connectivity!

Administrator: Windows PowerShell

```
PS C:\Users\brian\Desktop> .\shieldsup.ps1

The interfaces - such as wired/wireless/Bluetooth - are now all disabled.
This script will halt now.
Press Enter to re-enable all interfaces, or exit this script to keep interfaces disabled.

Press Enter to continue...:
```

Network Connections

Control Panel › Network and Internet › Network Connections

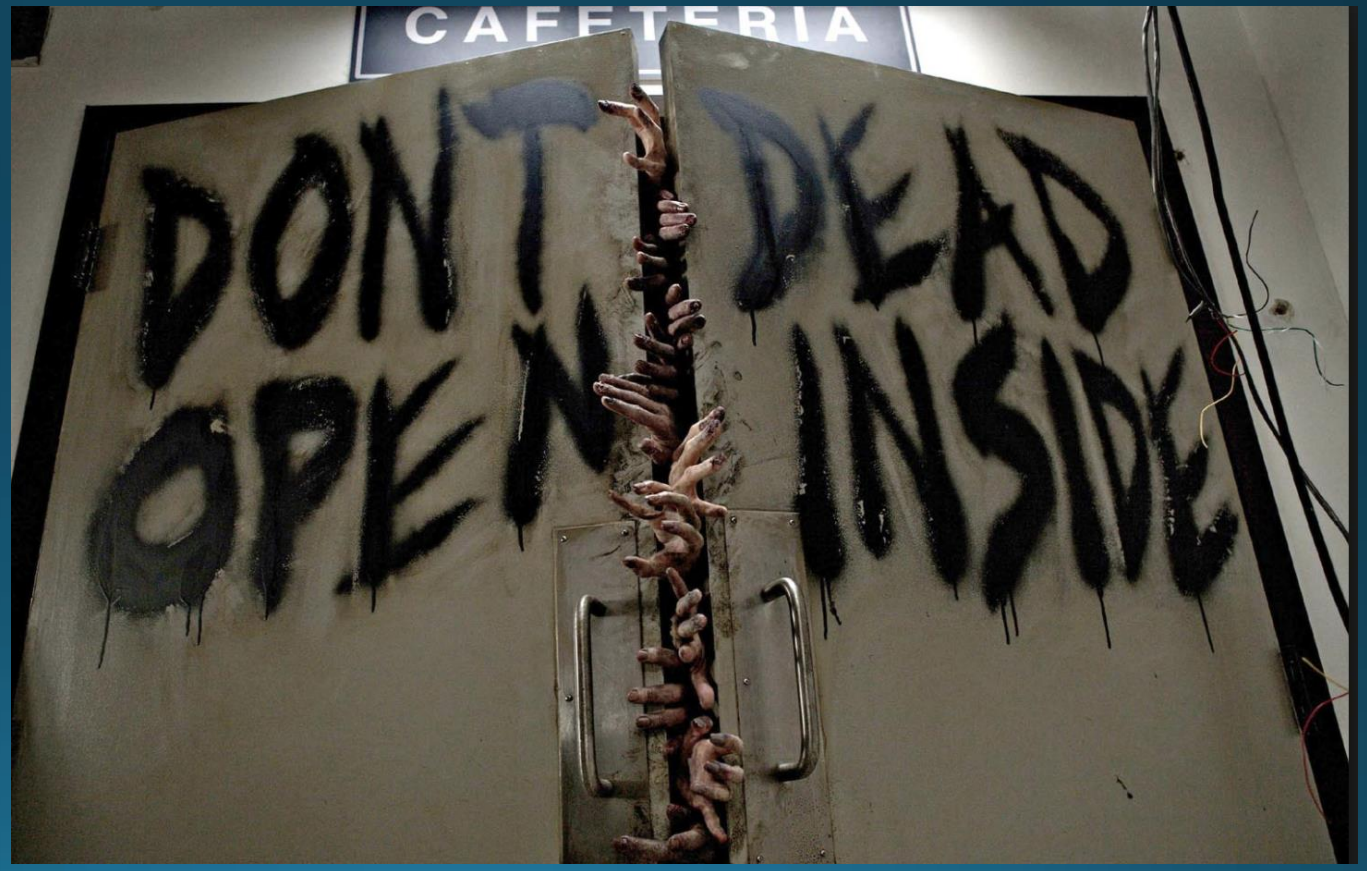
Organize

Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...

Bluetooth Network Connection
Disabled
Bluetooth Device (Personal Area ...

Removing malware

Physically secure the affected machine



Analysis with Sysinternals

live.sysinternals.com - /

Friday, May 30, 2008	3:55 PM	668 About This Site.txt
Tuesday, November 21, 2017	4:48 PM	792208 accesschk.exe
Tuesday, November 21, 2017	4:48 PM	409760 accesschk64.exe
Wednesday, November 1, 2006	1:06 PM	174968 AccessEnum.exe
Thursday, July 12, 2007	5:26 AM	50379 AdExplorer.chm
Wednesday, November 14, 2012	10:22 AM	479832 ADExplorer.exe

- Suite of tools to troubleshoot system issues
- Free download from Microsoft
- Get it "live" from https://live.sysinternals.com/

Analysis with Sysinternals – Process Explorer

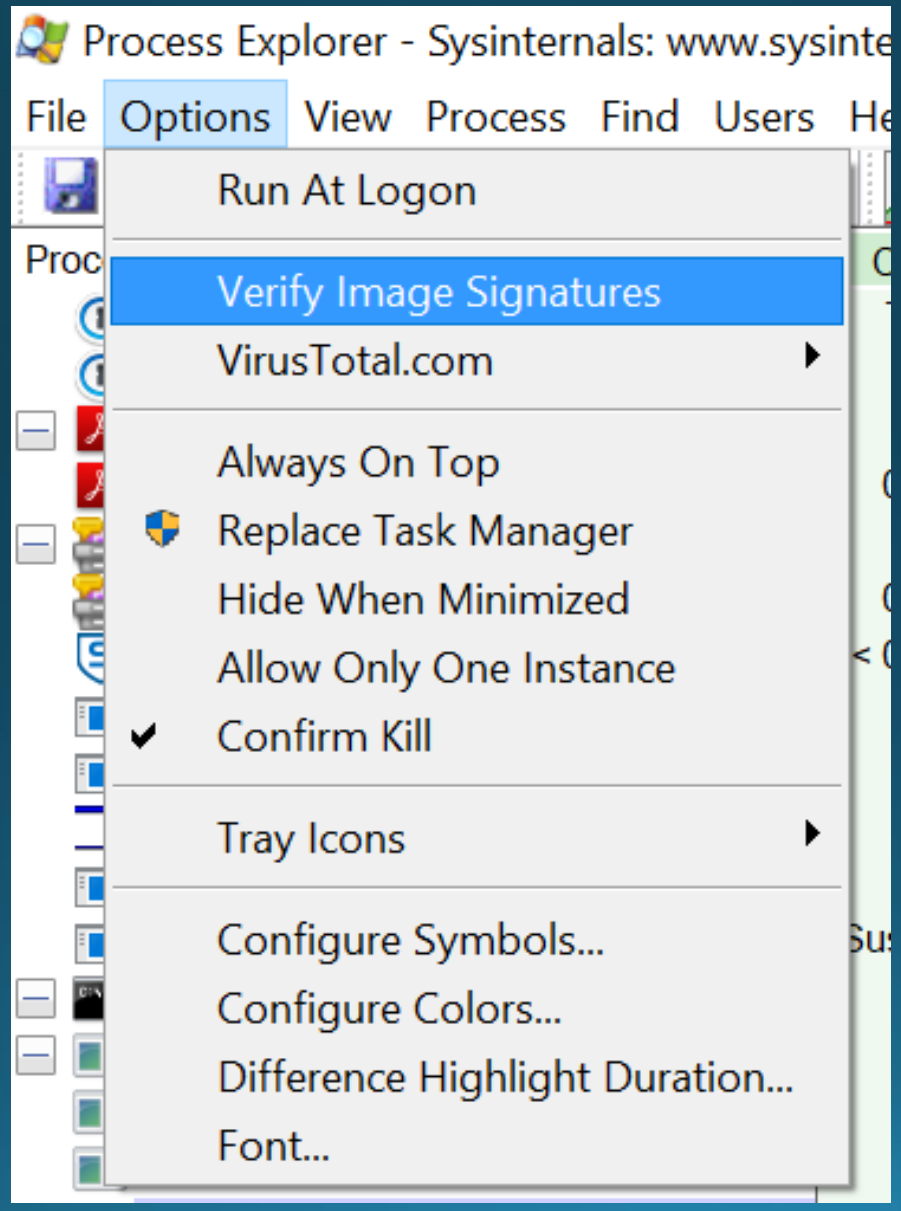
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9M3GQQP\brian]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
1Password.exe	1.55	126,860 K	108,444 K	12960	1Password for Windows desktop	AgileBits Inc.	
1Password.exe		13,792 K	15,984 K	13760	1Password for Windows desktop	AgileBits Inc.	
AcroRd32.exe		11,524 K	23,864 K	24552	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AcroRd32.exe	0.93	40,064 K	65,748 K	16724	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	
AdobeCollabSync.exe		3,044 K	10,784 K	16564	Adobe Collaboration Synchronizer 19.8	Adobe Systems Incorporat...	
AdobeCollabSync.exe	0.12	6,556 K	17,016 K	16976	Adobe Collaboration Synchronizer 19.8	Adobe Systems Incorporat...	
ALMon.exe		6,784 K	2,896 K	13264	Sophos Endpoint Security and Control	Sophos Limited	
ALsvc.exe		6,304 K	3,432 K	4792	Sophos AutoUpdate Service.	Sophos Limited	
ApplicationFrameHost.exe		19,896 K	36,836 K	10992	Application Frame Host	Microsoft Corporation	
armsvc.exe		1,416 K	5,952 K	4220	Adobe Acrobat Update Service	Adobe Systems Incorporat...	
backgroundTaskHost.exe		10,396 K	15,120 K	8952	Background Task Host	Microsoft Corporation	
Calculator.exe	Susp...	14,940 K	37,112 K	14540			
cmd.exe		4,536 K	10,684 K	23576	Windows Command Processor	Microsoft Corporation	
cmd.exe		4,500 K	10,224 K	14792			
conhost.exe		5,368 K	4,396 K	3924			
conhost.exe		5,384 K	4,464 K	13984			
conhost.exe		5,460 K	5,260 K	9400	Console Window Host	Microsoft Corporation	
conhost.exe	< 0.01	5,640 K	6,100 K	18876			
conhost.exe		6,648 K	12,368 K	21712	Console Window Host	Microsoft Corporation	
conhost.exe		6,472 K	11,660 K	22236			
conhost.exe		6,288 K	14,376 K	23008	Console Window Host	Microsoft Corporation	
csrss.exe	< 0.01	1,944 K	4,948 K	564			
csrss.exe	0.87	2,736 K	6,108 K	660			
ctfmon.exe		91,252 K	19,256 K	10396			
dasHost.exe		4,012 K	11,032 K	2284			

Shows parent/child relationship for processes

Analysis with Sysinternals – Process Explorer



Analysis with Sysinternals – Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9M3GQQP\brian]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
1Password.exe	1.05	126,860 K	108,444 K	12960	1Password for Windows desktop	AgileBits Inc.	(Verified) AgileBits Inc.
1Password.exe		13,792 K	15,984 K	13760	1Password for Windows desktop	AgileBits Inc.	(Verified) AgileBits Inc.
AcroRd32.exe		11,524 K	23,864 K	24552	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	(Verified) Adobe Systems
AcroRd32.exe	0.63	40,064 K	65,748 K	16724	Adobe Acrobat Reader DC	Adobe Systems Incorporat...	(Verified) Adobe Systems
AdobeCollabSync.exe		3,044 K	10,784 K	16564	Adobe Collaboration Synchronizer 19.8	Adobe Systems Incorporat...	(Verified) Adobe Systems
AdobeCollabSync.exe	0.08	6,556 K	17,016 K	16976	Adobe Collaboration Synchronizer 19.8	Adobe Systems Incorporat...	(Verified) Adobe Systems
ALMon.exe	< 0.01	6,784 K	680 K	13264	Sophos Endpoint Security and Control	Sophos Limited	(Verified) Sophos Limited
ALsvc.exe		6,304 K	3,432 K	4792	Sophos AutoUpdate Service.	Sophos Limited	(Verified) Sophos Limited
ApplicationFrameHost.exe		19,896 K	36,836 K	10992	Application Frame Host	Microsoft Corporation	(Verified) Microsoft Windows
armsvc.exe		1,416 K	5,952 K	4220	Adobe Acrobat Update Service	Adobe Systems Incorporat...	(Verified) Adobe Systems
backgroundTaskHost.exe		10,396 K	15,120 K	8952	Background Task Host	Microsoft Corporation	(Verified) Microsoft Windows
backgroundTaskHost.exe	Susp...	5,860 K	21,576 K	18148	Background Task Host	Microsoft Corporation	(Verified) Microsoft Windows
backgroundTaskHost.exe	Susp...	8,584 K	24,772 K	24056	Background Task Host		

Analysis with Sysinternals – Process Explorer

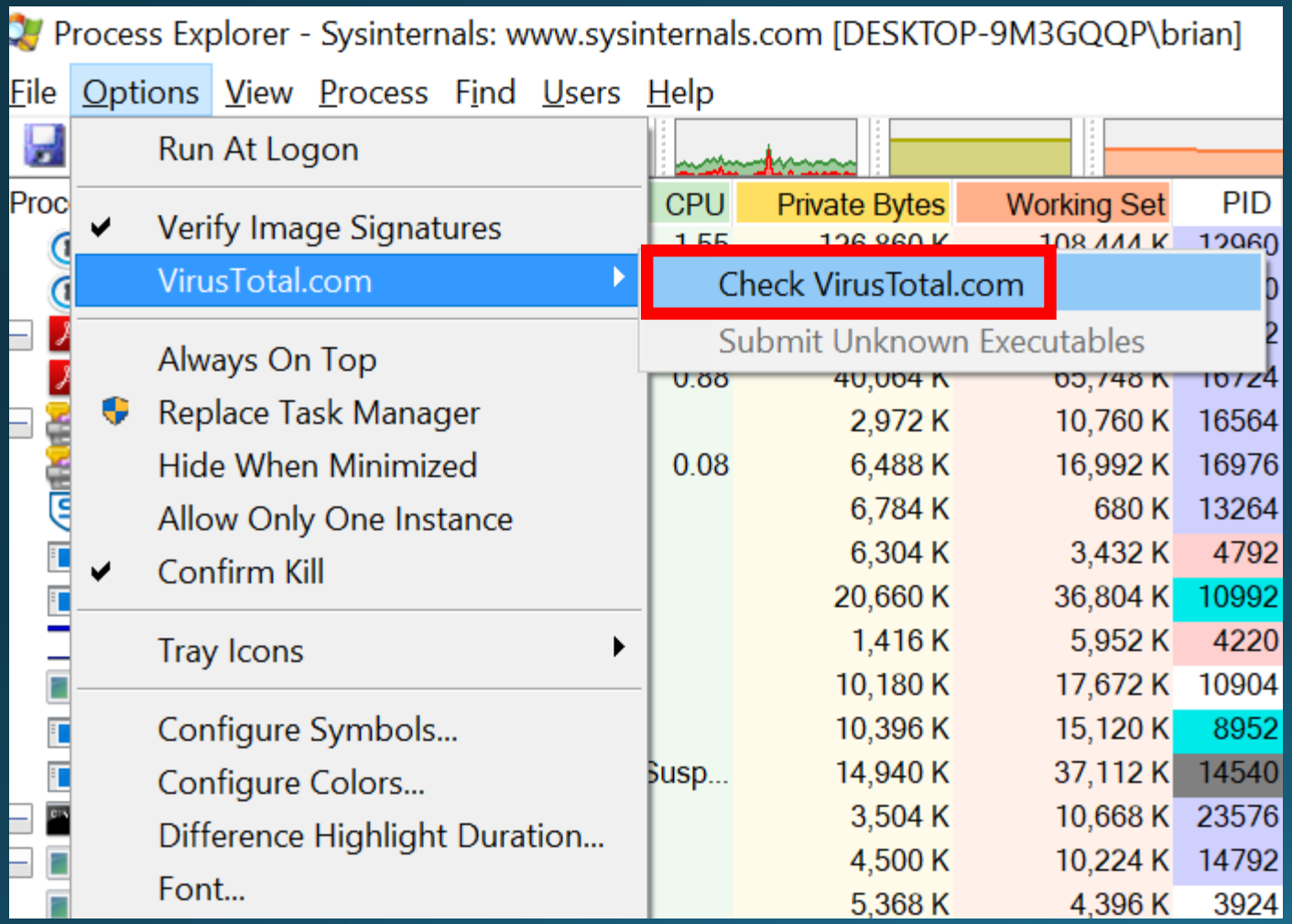
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9M3GQQP\brian]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	Vir
faceoff.exe		980 K	3,700 K	20068			(No signature was present in the subject)	
[illegible]		4,388 K	10,236 K	23892			(No signature was present in the subject)	
Video.UI.exe	Susp...	20,384 K	544 K	18908			(No signature was present in the subject)	
quickset.exe		3,852 K	13,512 K	12136	QuickSet	Dell Inc.	(No signature was present in the subject) Dell...	
SkypeApp.exe	Susp...	221,392 K	128,196 K	11008	SkypeApp	Microsoft Corporation	(No signature was present in the subject) Micr...	
SkypeBackgroundHost.exe	Susp...	2,008 K	10,904 K	11156	Microsoft Skype	Microsoft Corporation	(No signature was present in the subject) Micr...	
WinStore.App.exe	Susp...	50,520 K	69,852 K	11720	Store	Microsoft Corporation	(No signature was present in the subject) Micr...	

No “Company Name” and no “Verified Signature”

Analysis with Sysinternals – Process Explorer



You can even check for viruses on the fly!

Analysis with Sysinternals – Process Explorer

Detection ratio: 13 / 67

Analysis date: 2018-10-01 14:30:17 UTC (2 months ago)

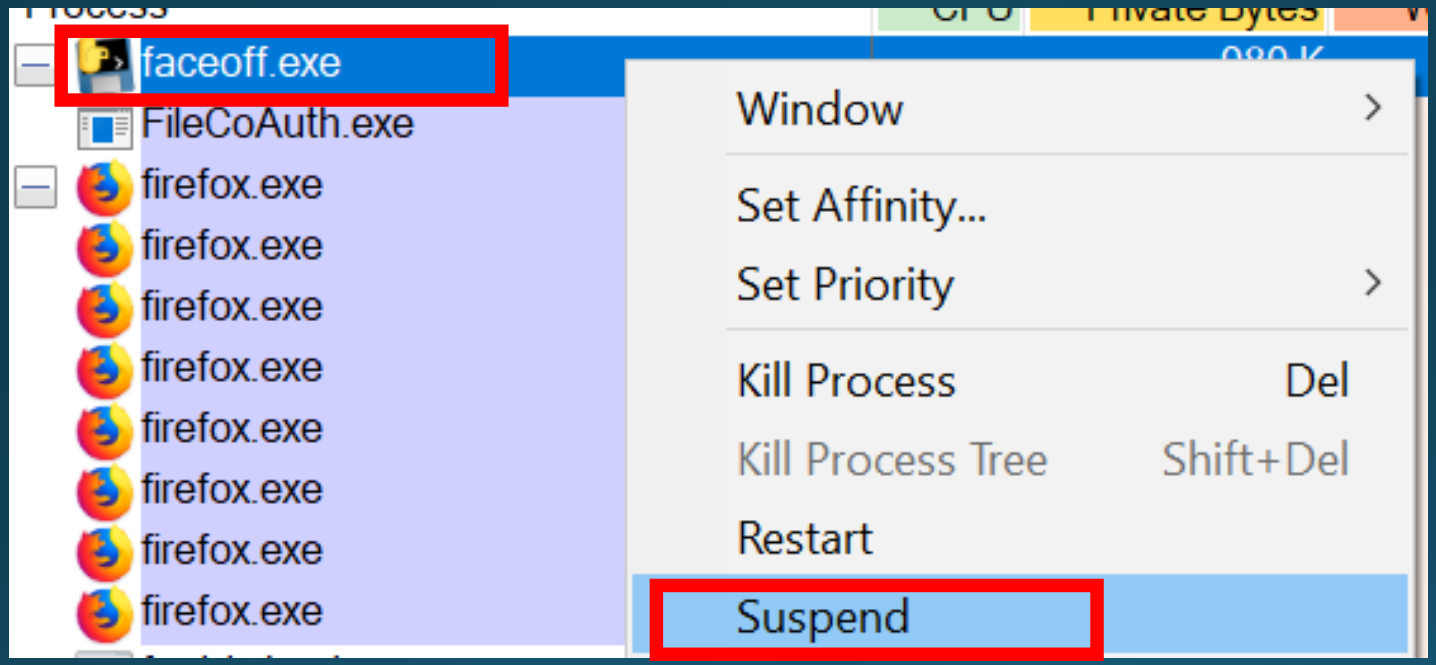
Analysis | File detail | Additional information | Comments 1 | Votes | Behavioural information

Antivirus	Result	Update
AVware	Trojan.Win32.Generic!BT	20180925
CAT-QuickHeal	Trojan.IGENERIC	20181001
Cylance	Unsafe	20181001
Cyren	W32/S-1c56a407!Eldorado	20181001
F-Prot	W32/S-1c56a407!Eldorado	20181001
Fortinet	PossibleThreat	20181001
Microsoft	Trojan:Win32/Bitrep.A	20181001
Symantec	ML.Attribute.HighConfidence	20181001

You can even check for viruses on the fly!

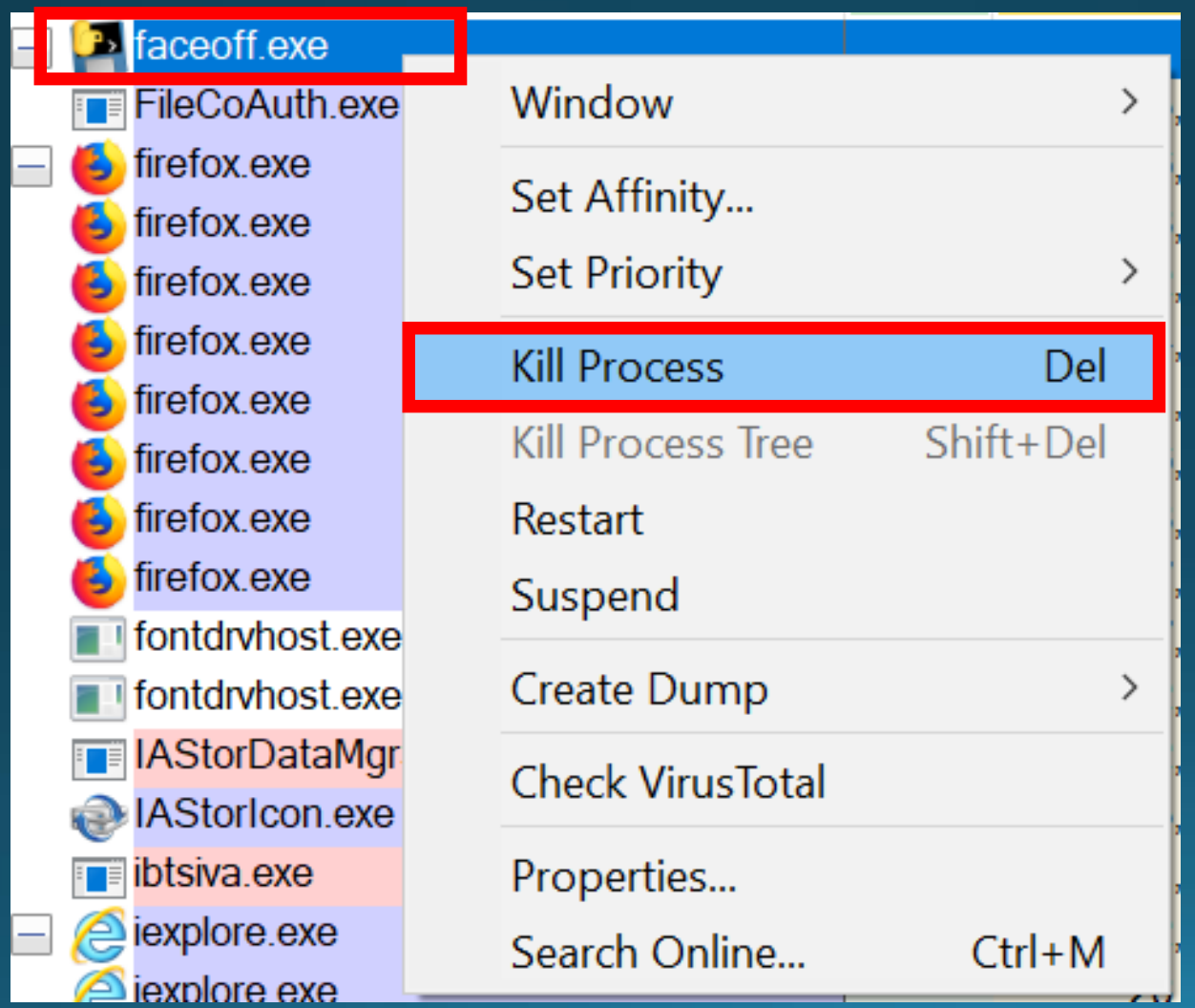
Analysis with Sysinternals – Process Explorer

Put malware to sleep first – *then* kill it



Analysis with Sysinternals – Process Explorer

Put malware to sleep first – *then* kill it



Analysis with Sysinternals – Autoruns

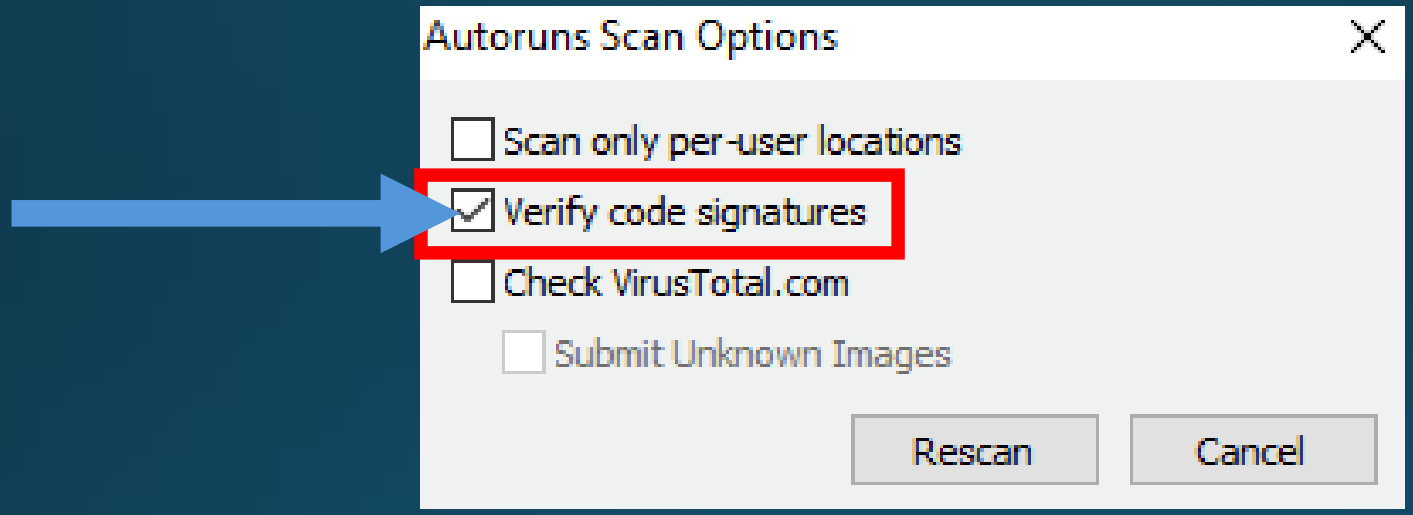
Shows startup items, scheduled tasks and more

Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers

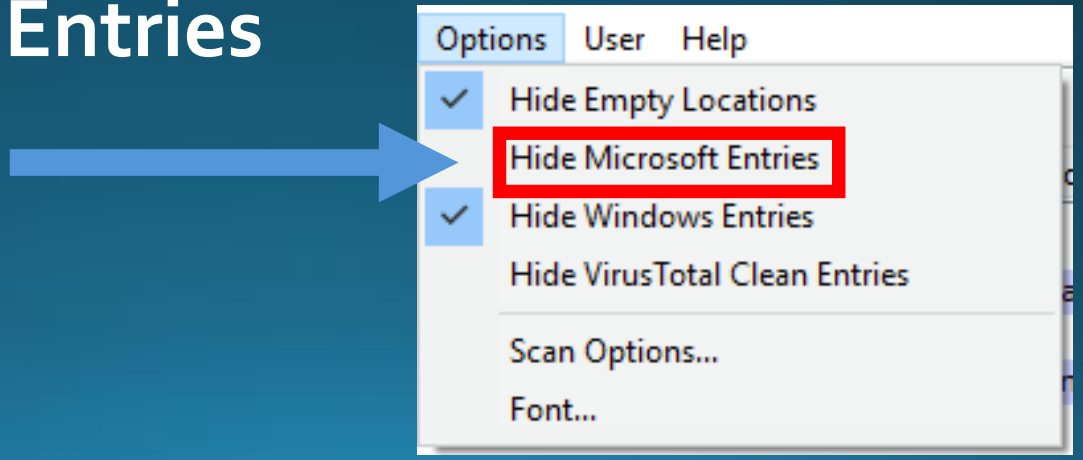
Autorun Entry	Description
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	
☑ cmd.exe	Windows Command Processor
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
☑ SecurityHealth	Windows Defender notification icon
☑ VMware User Process	VMware Tools Core Service
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
☑ OneDrive	Microsoft OneDrive
☑ Updater	Windows PowerShell
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	
☑ Microsoft Windows	Windows Mail
☑ n/a	Windows host process (Rundll32)
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	
☑ Microsoft Windows	Windows Mail
☑ n/a	Windows host process (Rundll32)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	
☑ SolDisk Mount Notification	CBDisk Mount Notifier

Analysis with Sysinternals – Autoruns

Filter out some noise in **Options → Scan Options**



And **Options → Hide Microsoft Entries**



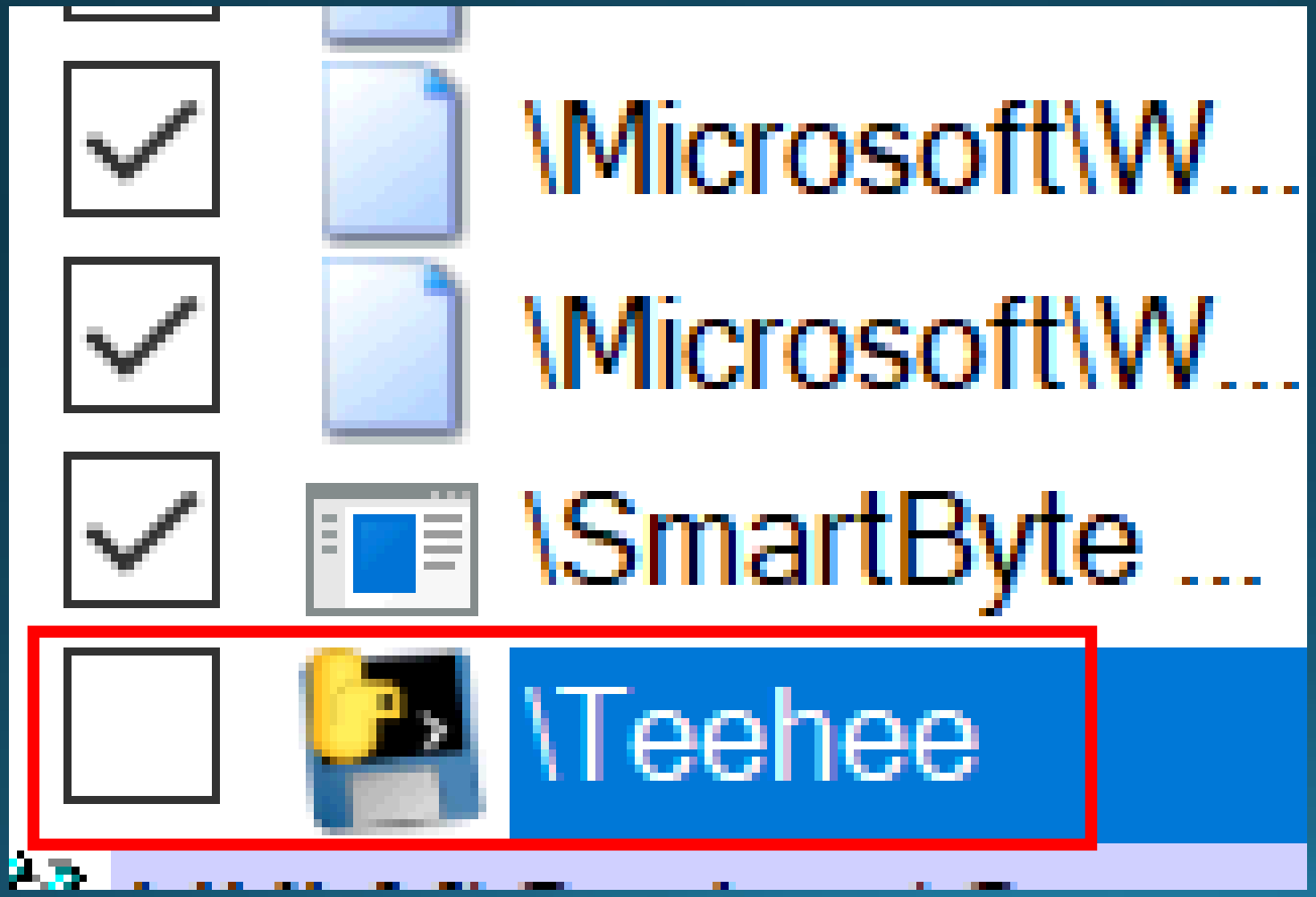
Analysis with Sysinternals – Autoruns

Interesting findings!

	Task Scheduler				
✓	\Adobe Acro...	Adobe Reader and Acro...	(Verified) Adobe System...	c:\program files (x86)\common files\adob...	8/14/2018 1:22 AM
✓	\Dell Suppor...	SupportAssistInstaller	(Verified) Dell Inc.	c:\program files\dell\supportassistagent\bi...	10/25/2018 12:43 PM
✓	\DropboxUp...	Dropbox Update	(Verified) Dropbox, Inc	c:\program files (x86)\dropbox\update\dro...	10/21/2015 12:52 PM
✓	\DropboxUp...	Dropbox Update	(Verified) Dropbox, Inc	c:\program files (x86)\dropbox\update\dro...	10/21/2015 12:52 PM
✓	\G2MUpdat...	GoToMeeting	(Verified) LogMeIn, Inc.	c:\users\brian\appdata\local\gotomeeting\...	11/29/2018 2:05 PM
✓	\G2MUpload...	GoToMeeting	(Verified) LogMeIn, Inc.	c:\users\brian\appdata\local\gotomeeting\...	11/29/2018 2:05 PM
✓	\GoogleUpd...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\goo...	7/13/2017 8:07 PM
✓	\GoogleUpd...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\goo...	7/13/2017 8:07 PM
✓	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
✓	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
✓	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
✓	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
✓	\Microsoft\W...	Windows host process (...	(Verified) Microsoft Wind...	c:\windows\system32\rundll32.exe	4/14/1957 5:35 AM
✓	\SmartByte ...	SmartByteTelemetry	(Verified) Rivet Networks...	c:\program files\rivet networks\smartbyte\...	9/12/2018 12:01 PM
✓	\Teehee			c:\users\brian\desktop\faceoff.exe	3/3/2022 1:29 AM

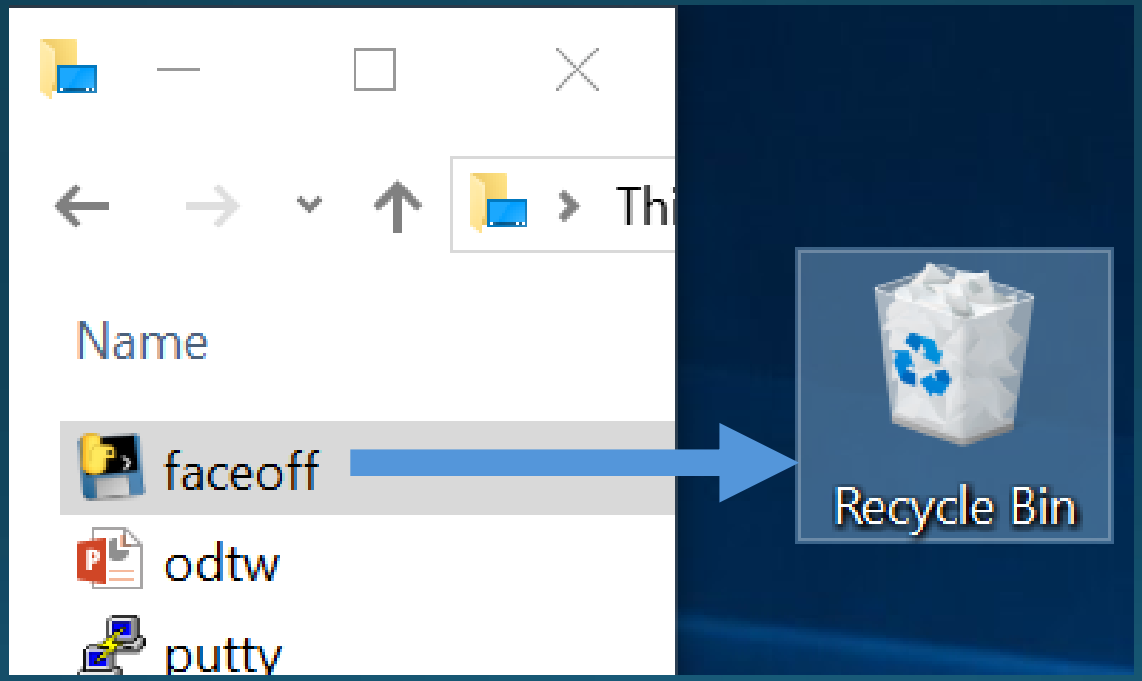
Analysis with Sysinternals – Autoruns

Interesting findings!



Analysis with Sysinternals – Autoruns

Interesting findings!



You might at least cripple the malware!

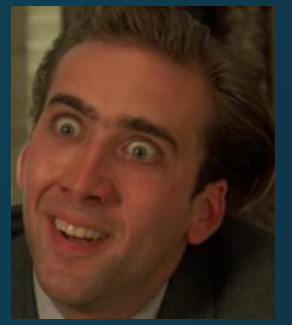
Cleaning Malware – Summary

Cleaning steps:

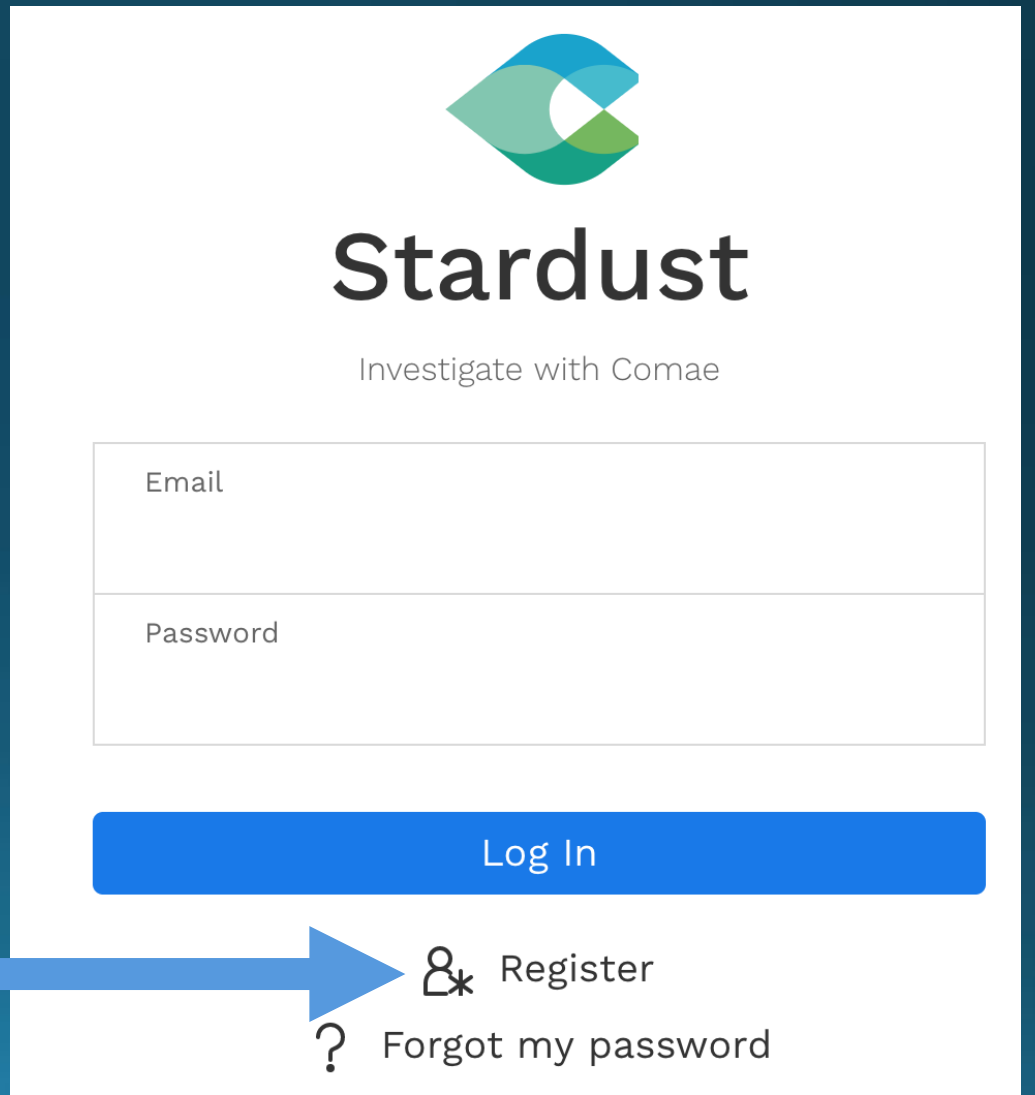
1. Disconnect from the network
2. Find malicious processes/drivers
3. Suspend & kill suspicious processes
4. Find & remove malicious items
5. Delete files associated with malware
6. Reboot and repeat

Searching for evil the “easy” way

DumpIt

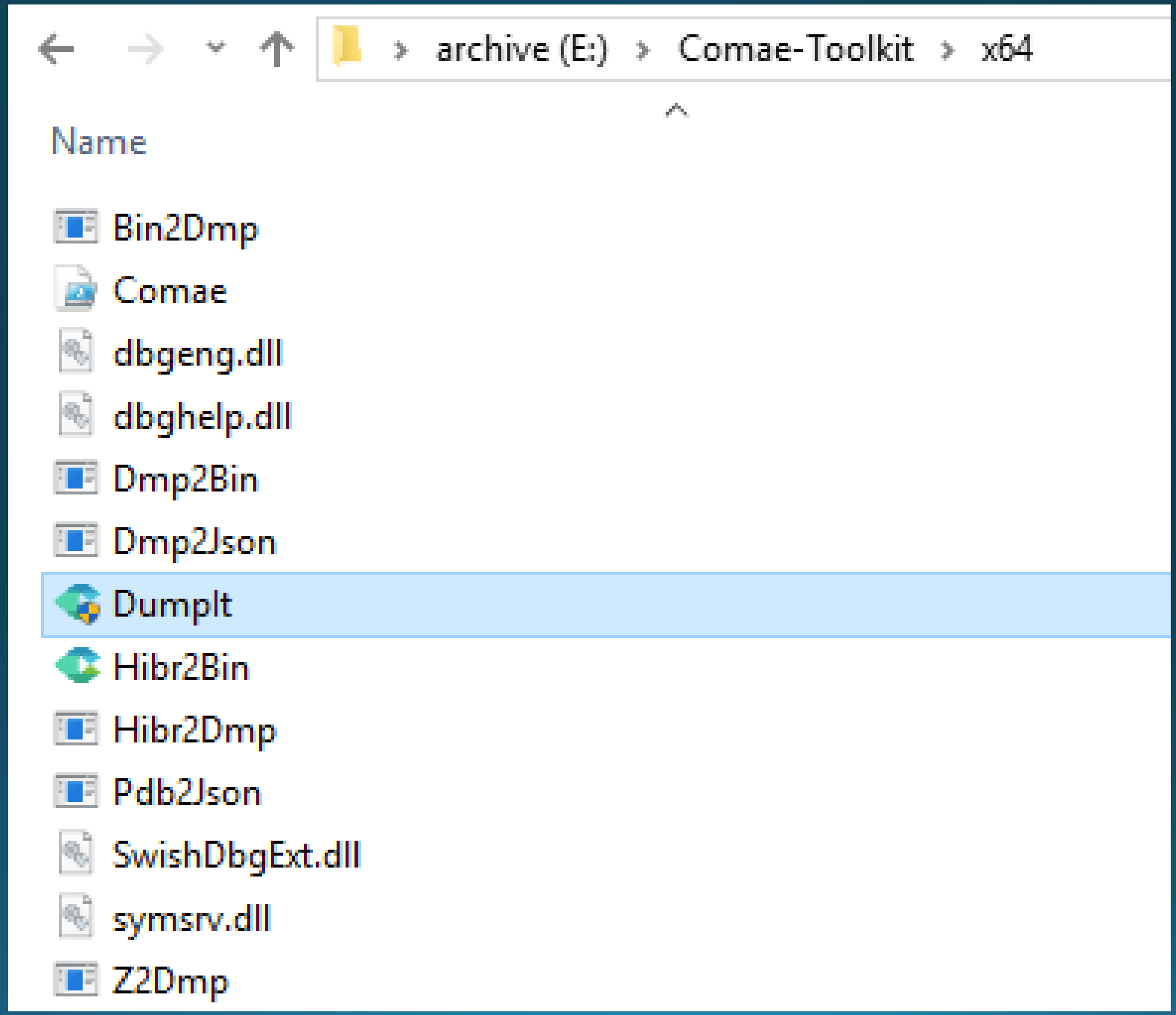


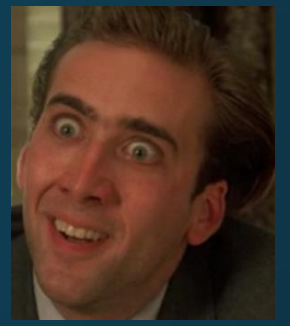
- Does a quick dump of memory – easy peasy!
- Free (!) to download and use (https://my.comae.io/)
- Sign up for free account



DumpIt

Portable = fun!



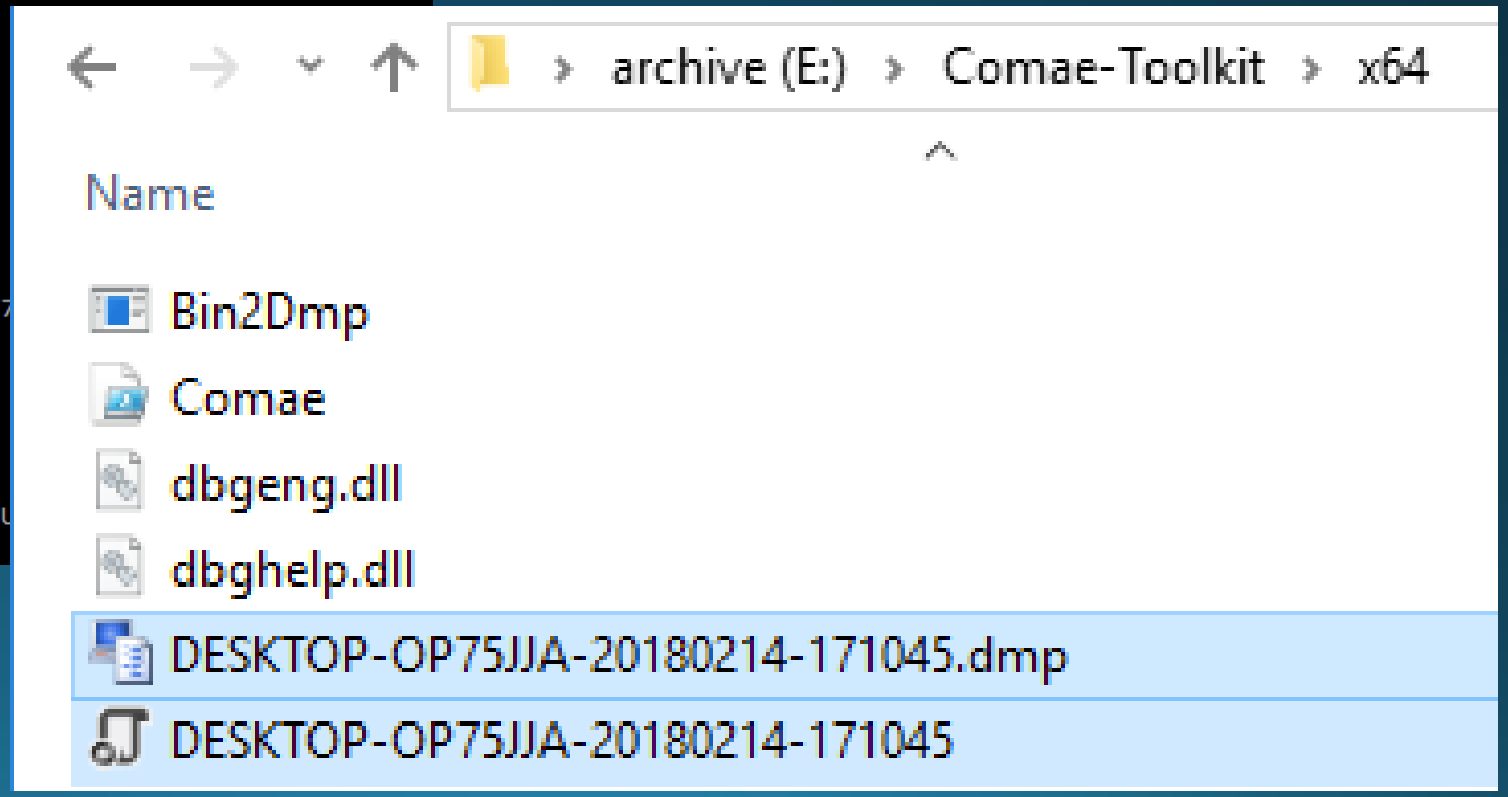


DumpIt

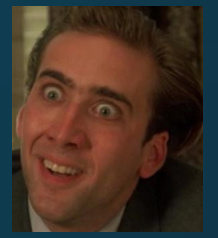
Run **Dumpit.Exe**

E:\Comae-Toolkit\x64\DumpIt.exe

```
DumpIt 3.0.20171228.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\E:\Comae-Toolkit\x64\DESKTOP-OP75JJA-20180214-170853.dmp

  Computer name:              DESKTOP-OP75JJA


  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.15063
  MachineId:                   0C474D56-867C-CAED-602E-9363147C577
  TimeStamp:                   131631017467350422
  Cr3:                         0x1aa002
  KdCopyDataBlock:             0xfffff801aa8082ac
  KdDebuggerData:              0xfffff801aa9484f0
  KdpDataBlockEncoded:         0xfffff801aa97b6f0

  Current date/time:           [2018-02-14 (YYYY-MM-DD) 17:09:06 (U
  + Processing...
```



Volatility



- A "completely open collection of tools… for the extraction of digital artifacts from volatile memory (RAM)"

- Free (!) to download and use (http://www.volatilityfoundation.org/)

- Runs on everything:

Volatility 2.6 Windows Standalone Executable (x64)
Volatility 2.6 Mac OS X Standalone Executables (x64)
Volatility 2.6 Linux Standalone Executables (x64)
Volatility 2.6 Source Code (.zip)
Integrity Hashes
View the README
View the CREDITS

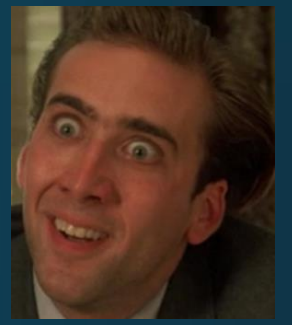
Volatility

Find evil 1/3: *dlldump*

Dump all executables in memory – and their supporting DLLs

```
root@pt-kali:~/Desktop/stux# /opt/vol/vol.py -f stuxnet.vmem --profile=WinXPSP2x86 dlldump -D dlldump-export/
Volatility Foundation Volatility Framework 2.6
Process(V) Name                 Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0x820df020 smss.exe             0x048580000 smss.exe             OK: module.376.22df020.48580000.dll
0x820df020 smss.exe             0x07c900000 ntdll.dll            OK: module.376.22df020.7c900000.dll
0x821a2da0 csrss.exe            0x04a680000 csrss.exe            OK: module.600.23a2da0.4a680000.dll
0x821a2da0 csrss.exe            0x07c900000                      Error: DllBase is paged
0x821a2da0 csrss.exe            0x075b40000 CSRSRV.dll           OK: module.600.23a2da0.75b40000.dll
0x821a2da0 csrss.exe            0x077f10000 GDI32.dll            Error: DllBase is paged
0x821a2da0 csrss.exe            0x07e720000 sxs.dll              Error: DllBase is paged
0x821a2da0 csrss.exe            0x077e70000 RPCRT4.dll           Error: DllBase is paged
0x821a2da0 csrss.exe            0x077dd0000 ADVAPI32.dll         Error: DllBase is paged
0x821a2da0 csrss.exe            0x077fe0000 Secur32.dll          Error: DllBase is paged
0x821a2da0 csrss.exe            0x075b50000 basesrv.dll          Error: DllBase is paged
0x821a2da0 csrss.exe            0x07c800000 KERNEL32.dll         Error: DllBase is paged
0x821a2da0 csrss.exe            0x07e410000 USER32.dll           OK: module.600.23a2da0.7e410000.dll
0x821a2da0 csrss.exe            0x075b60000 winsrv.dll           OK: module.600.23a2da0.75b60000.dll
0x81da5650 winlogon.exe         0x001000000 winlogon.exe         OK: module.624.1fa5650.1000000.dll
0x81da5650 winlogon.exe         0x07c900000 ntdll.dll            OK: module.624.1fa5650.7c900000.dll
```

Volatility

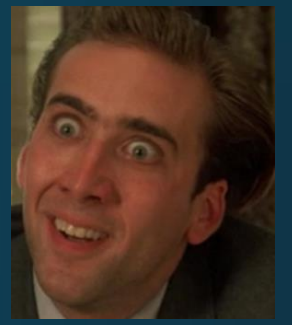


Find evil 2/3: *malfind*

Search for malicious executables and shellcode

```
root@pt-kali:~/Desktop/stux# /opt/vol/vol.py -f stuxnet.vmem --profile=WinXPSP2x86 malfind -D mal-dump/
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 600 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 1f 01 00 00 ff ee ff ee 08 70 00 00   .............p..
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00   ................
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f   ................
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x7f6f0000 c8000000          ENTER 0x0, 0x0
0x7f6f0004 1f                POP DS
0x7f6f0005 0100              ADD [EAX], EAX
```

Volatility



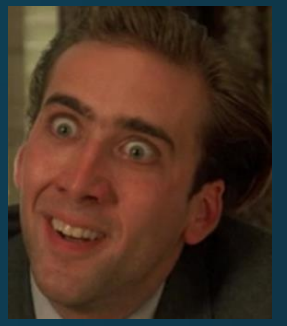
Find evil 3/3: *moddump*

Extract all drivers from memory (a ton of info!)

```
root@pt-kali:~/Desktop/stux# /opt/vol/vol.py -f stuxnet.vmem --profile=WinXPSP2x86 moddump -D moddump-export/
Volatility Foundation Volatility Framework 2.6
Module Base Module Name          Result
---------- -------------------- ------
0x0804d7000 ntoskrnl.exe         OK: driver.804d7000.sys
0x0806d0000 hal.dll              OK: driver.806d0000.sys
0x0f7470000 update.sys           OK: driver.f7470000.sys
0x0f89ba000 usbehci.sys          OK: driver.f89ba000.sys
0x0f8a1a000 HIDPARSE.SYS         OK: driver.f8a1a000.sys
0x0f8b5a000 CmBatt.sys           OK: driver.f8b5a000.sys
0x0f855a000 pci.sys              OK: driver.f855a000.sys
0x0f89aa000 usbuhci.sys          OK: driver.f89aa000.sys
0x0bf800000 win32k.sys           OK: driver.bf800000.sys
```

Volatility

Scan infected files from memory dump



WARNING! WARNING! WARNING!

Volatility

Analysis using a basic Ubuntu Linux VM

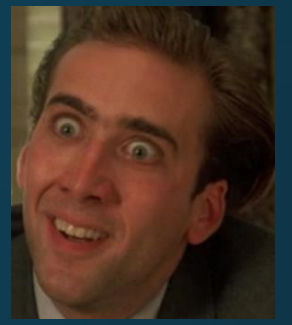
mi — root@quarantine: ~ — ssh ◂ -bash — 80×24

```
root@quarantine:~# apt-get install clamav
```

Install open-source AV with a single command

Volatility

Analysis using a basic Ubuntu Linux VM



```
root@pt-kali:~/Desktop/stux# clamscan -r ~/Desktop/stux/ | grep -v ": OK$"
/root/Desktop/stux/moddump-export/driver.f895a000.sys: Win.Trojan.Rootkit-8720 FOUND
/root/Desktop/stux/mal-dump/process.0x81c498c8.0x1000000.dmp: Win.Trojan.5873027-1 FOUND
/root/Desktop/stux/mal-dump/process.0x81c498c8.0x80000.dmp: Win.Worm.Stuxnet-49 FOUND
/root/Desktop/stux/mal-dump/process.0x81e61da0.0xb7000.dmp: Win.Worm.Stuxnet-49 FOUND
/root/Desktop/stux/mal-dump/process.0x81c47c00.0x6f000.dmp: Win.Worm.Stuxnet-49 FOUND
/root/Desktop/stux/mal-dump/process.0x81c47c00.0x1000000.dmp: Win.Trojan.5873027-1 FOUND
/root/Desktop/stux/mal-dump/process.0x81c47c00.0x80000.dmp: Win.Worm.Stuxnet-49 FOUND
/root/Desktop/stux/dlldump-export/module.940.2061da0.c00000.dll: Win.Trojan.Agent-229176 FOUND
/root/Desktop/stux/dlldump-export/module.868.1e498c8.1000000.dll: Win.Trojan.Duqu-10 FOUND
/root/Desktop/stux/dlldump-export/module.1928.1e47c00.1000000.dll: Win.Trojan.Duqu-10 FOUND
```

Can you smell what the network is cooking?

Security Onion

https://securityonion.net

About Security Onion

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

Security Onion

https://securityonion.net/

Security Onion

Dashboard

kibana

Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse

Dashboard / Overview Full screen Share

*

Add a filter +

Navigation

Home
Help

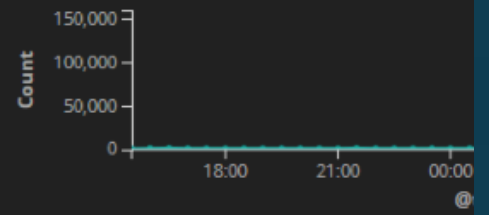
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS

Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB

Total Number of Logs

392,206

Total Log Count Over Time



All Sensors - Log Type

Log Type(s)	Count
bro_conn	182,054
bro_dns	87,460
bro_weird	45,649
ossec_archive	43,776
CRON	23,842
bro_files	2,794
bro_ssl	1,909
bro_x509	1,216
su	1,146
ossec	1,036

Security Onion

NIDS alert

NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address
ET INFO Packed Executable Download	173.194.54.235	192.168.55.210
ET POLICY DNS Update From External net	192.168.55.210	192.168.55.200
ET POLICY DNS Update From External net	192.168.55.220	192.168.55.200
ET POLICY PE EXE or DLL Windows file download HTTP	173.194.54.235	192.168.55.210
ET POLICY RDP connection confirm	192.168.55.200	192.168.3.20
ET POLICY RDP connection confirm	192.168.55.200	192.168.3.50
ET POLICY RDP connection confirm	192.168.55.220	192.168.3.20
ET CURRENT_EVENTS Possible MyEtherWallet Phishing Landing - Title over non SSL	159.65.205.186	192.168.55.210
ET INFO DNS Query for Suspicious .cf Domain	192.168.55.210	192.168.55.200
ET POLICY MS Remote Desktop Administrator Login Request	192.168.3.50	192.168.55.200

Security Onion

Hits on “Baby” domains

DNS - Baby Domain Requests

Domain	creation_date: Descending	Count
giveaway-user.com	December 4th 2018, 13:14:51.000	6
l-obmen.pro	November 29th 2018, 10:14:06.000	3

Security Onion

DNS query count

DNS - Queries

Query	Count
lol.7minsec.com	32,016
lol.7minsec.com.faceoff.now	32,014
200.55.168.192.in-addr.arpa	16,026
isatap	329
fo-dc01	288
wpad.faceoff.now	225
settings-win.data.microsoft.com	205
array505-prod.do.dsp.mp.microsoft.com	175
v10.events.data.microsoft.com	161
array506-prod.do.dsp.mp.microsoft.com	156

Conclusion

- Quick malware triage with Sysinternals
- Dumped/analyzed malware with Dumpit and Volatility
- Sniffed the network with Security Onion