


You need a PROcess to check your
running processes and modules.
The bad guys, and red teams are
coming after them!

Michael Gough – Principal NCC Group
Founder MalwareArchaeology.com
& IMFSecurity.com

Who am I

- Blue Team Defender Ninja, Malware Archaeologist, Logoholic and Principal Incident Response Engineer for 
- I love “properly” configured logs – they tell us Who, What, Where, When and hopefully How

Creator of

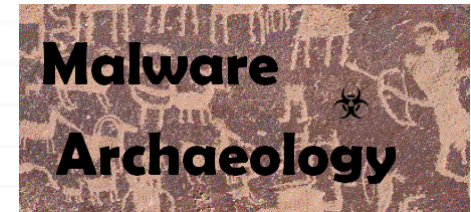
“Windows Logging Cheat Sheet”

“Windows File Auditing Cheat Sheet”

“Windows Registry Auditing Cheat Sheet”

“Windows Splunk Logging Cheat Sheet”

“Malware Management Framework”



- Co-Creator of “Log-MD” – Log Malicious Discovery Tool  **LOG-MD**
- And co-host of “THE Incident Response Podcast”

	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a

Why this talk?

Fileless in memory only malware

- To address this expanding threat that is becoming more and more common, too common
- Commodity malware, Red Team engagements, and of course APT attackers use it
- This method can avoid many security tools

	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	n/a
2T13:26:59:391	0x6b0	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:137	0xaa4	0x6b0	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T13:27:23:81	n/a	n/a	n/a
2T13:27:23:81	n/a	n/a	n/a

Let's rethink or
redefine

Fileless Malware

Rethinking Fileless Malware

- Fileless Malware that can only be found in the memory of a running system (Malware + Memory = **Memware**)
- No files can be found if you scan the disk while the system is running
 - Or are very short lived, just long enough to load (bypasses FIM)
- Typical infection vectors are:
 - Injection
 - Dll side-loading/Hijacking
 - Process Hollowing
 - Download source code and compile on the fly, .NET, JSC
 - User double-click, etc.
- “Fileless” malware, the file lives somewhere, so lets do a better job guiding people where to look for signs of it

Other Fileless Malware types

- Regware – Malware payload is stored in the registry with an autorun/ASEP that calls and loads it into memory (Malware + Payload in Registry = RegWare)
- WMIware - Malware payload is stored in the WMI database with an autorun/ASEP that calls and loads it into memory (Malware + Payload in WMI database = WMIWare)
- PowerShellware - Malware payload is in the form of PowerShell scripts, downloaded or stored somewhere on the fly with an autorun/ASEP that calls and loads it into memory (Malware + Payload in PowerShell = PowerShellWare)
- Compileware – Malware payload is not yet compiled, stored anywhere with an autorun/ASEP that calls and loads it into memory (Malware + Payload compiled on the fly = CompileWare)
- Downloadware – Autorun/ASEP calls out to the Internet to download malware payload or source code that is then compiled and loads it into memory (Malware + Payload downloaded each time = DownloadWare) maybe LOLBASWare ;-)

Autoruns/ASEP

• Keep in mind...

– Not all malware will have an autorun/ASEP

- Latest TrickBot on Domain Controllers

- Especially the Red Team, doesn't like to leave IOCs

– Or, the autorun is created on shutdown, then deleted on startup once the malware loads

- Nothing found when doing live triage/analysis (Dridex)

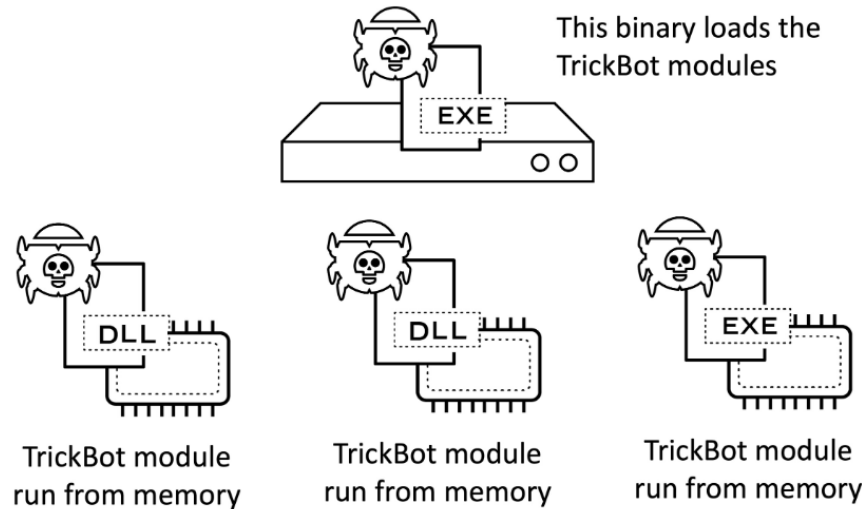
– So what is in memory *may* be all that we can see

Latest TrickBot

TrickBot Caused By Nworm: Not Persistent

When nworm infects a vulnerable DC, the malware is run from memory. No artifacts are found on the infected DC and TrickBot on the DC doesn't survive a reboot.

Initial TrickBot binary saved to disk (usually an EXE, sometimes a DLL)



PaloAlto Unit 42 - <https://unit42.paloaltonetworks.com/goodbye-mworm-hello-nworm-trickbot-updates-propagation-module/>

	or_Proc	w_Proc	Process Command Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:17:922	0x6b0	0x0	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a

So how do we find this stuff?

MITRE ATT&CK

- **First** - Everything you do should be mapped to MITRE ATT&CK - <https://attack.mitre.org/>
- Some of the techniques used
 - T1500 – Compile After Delivery
 - T1127 - Trusted Developer Utilities
 - T1055 – Process Injection
 - T1196 – Control Panel Items
 - etc
- Sub-techniques are coming !!!

<https://www.jaiminton.com/mitreatt&ck>

We need a PROcess

- We need to create a PROcess to start looking for this condition
- Tools are just not preventing this technique
- We need to build this PROcess into our hourly/daily/weekly/monthly routines to detect and alert for this technique
- We need to build this PROcess into our daily/weekly/monthly/yearly routines to Threat Hunt for this technique

Finding Memware

- Traditional forensics has us dumping a memory image and running tools like Volatility against it
- Logs can contain a lot of details that can alert you to this behavior, IF you collect THEN detect OR hunt
 - Process command line is KEY to catching these attacks
- Checking running processes and their modules on a live system is a GREAT option
 - ***Better yet look for signs of injection !!***
- Look for the other artifacts, autorun/ASEP, registry keys storing scripts and/or payloads, WMI databases storing scripts and/or payloads, and odd PowerShell, large blocks, obfuscation, etc.

Examples

+ LOG-MD

• Kovter injects into Svchost 32bit

Process_Name	Executable	Module_Name	VT	Log-MD_Valuation	b9	Injection	Catalog
IASstorIcon.exe	C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IASstorIcon.exe	C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IASstorIcon.dll	Suspect	in digest (trusted)	Hook 1 Det 3 Imp 4	FALSE	
IASstorDataMgrSvc.exe	C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IASstorDataMgrSvc.exe	C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IASstorDataMgrSvc.dll	Suspect	in digest (trusted)	Hook 1 Det 7 Imp 18	FALSE	
SupportAssistAgent.exe	C:\Program Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe	C:\Program Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.dll	Suspect	in digest (trusted)	Hook 1 Det 2	FALSE	
svchost.exe	C:\Windows\SysWOW64\svchost.exe	C:\Windows\SysWOW64\svchost.exe	h	Suspect	in digest (trusted)	Hook 3 Imp 2	TRUE
svchost.exe	C:\Windows\SysWOW64\svchost.exe	C:\Windows\SysWOW64\svchost.exe	h	Suspect	in digest (trusted)	Hook 3 Imp 2	TRUE

• Qakbot

Process_Name	Executable	Module_Name	VT	Log-MD_Valuation	b9	Injection	Catalog	Issuer_Name
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\WINDOWS\Explorer.EXE	Suspect	in digest (trusted)	Imp 3	TRUE	Microsoft Win	
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\WINDOWS\system32\explorerframe.dll	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Unsigned	
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\Windows\System32\Windows.UI.FileExplorer.dll	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Unsigned	
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\WINDOWS\system32\NetworkExplorer.dll	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Unsigned	
explorer.exe	C:\WINDOWS\SysWOW64\explorer.exe	C:\WINDOWS\SysWOW64\explorer.exe	Suspect	in digest (trusted)	Hook 1 Imp 2	TRUE	Microsoft Win	

• Dridex

Process_Name	Module_Name	VT	Log-MD_Valuation	b9	Injection	Catalog	Issuer_Name	Subject_Name	Process_ID	Parent
svchost.exe	Process likely terminated during capture.								10356	688
rundll32.exe	C:\Windows\SysWOW64\rundll32.exe	h	Suspect	in digest (trusted)	Rep 1	TRUE	Unsigned	Unsigned	6356	12492
rundll32.exe	C:\Windows\SYSTEM32\ntdll.dll	h	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Microsoft	Microsoft	6356	12492
rundll32.exe	C:\Windows\system32\imagehlp.dll	h	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Microsoft	Microsoft	6356	12492
rundll32.exe	C:\Users\Hackme\Desktop\Dridex.dll	h	Malicious	Suspicious	Parent Injection Indicator	FALSE	Unsigned	Unsigned	6356	C:\Windows\System32\rundll32.exe

+ LOG-MD
Discover it



Extracted Files LOG-MD & Volatility

- QakBot
- Kovter
- Dridex

File Name	Original Filename	Internal Filename	Result	PDB_Path	Certificates
Qakbot_1.exe			suspicious	C:\Users\parkhyunseo\source\repos\Project28\Debug\Project28.pdb	None found.
Faxprint.dll			malware		None found.
Kovter_1.exe	diffuseGravity.exe	diffuseGravityP	malware		None found.
QakBot_2.exe	rjrwer.exe	Java(TM) Control Panel	malware		None found.
QakBot_3.exe	nio.dll		malware		None found.
Dridex.dll		Process Fire	suspicious	c:\stop\Soft\duck\liquid\build\wide\DivideDictionary.pdb	None found.
Kovter_2.exe			suspicious		
rofce.dll			suspicious		

- Evaluated with LOG-MD B9 module

Examples

- They can call out to the Internet to download the code to compile, or fetch the malware so it does not live on disk. Some examples:
 - CobaltStrike and Sythe custom malware packages
 - LoLBins/LoLBas – Rundll32, Regsvr32, Regasm, etc.
 - <https://github.com/LOLBAS-Project/LOLBAS>
 - Compilers - Csc.exe, MSBuild.exe, JSC.exe, etc.
 - May write to disk on shutdown, delete on startup

CSC.exe example

Time	PID	PPID	Process	Command Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	/n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	/n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a	
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe	/c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe	/c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a	

Process Monitor

- Procmon.exe (2856)
- Procmon64.exe (2140)
- cmd.exe (6732)
 - conhost.exe (5064)
 - powershell.exe (1756)
 - csc.exe (384)
 - cvtres.exe (1884)

Description: Visual C# Command Line Compiler
Company: Microsoft Corporation
Path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Command: "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C
User: DESKTOP-Q4NDIRQ\testuser1
PID: 384 Started: 10/14/2019 9:16:36 PM
Exited: 10/14/2019 9:16:38 PM

Go To Event Include Process Include Subtree

```
C:\WINDOWS\system32\cmd.exe
C:\Users\testuser1\AppData\Local\Temp>dir
Volume in drive C has no label.
Volume Serial Number is CAED-FF5D

Directory of C:\Users\testuser1\AppData\Local\Temp

10/14/2019 09:20 PM <DIR> .
10/14/2019 09:20 PM <DIR> ..
10/14/2019 09:14 PM 0 aria-debug-5148.log
10/14/2019 09:20 PM 36 oj5z1fcy.0.cs
10/14/2019 09:20 PM 359 oj5z1fcy.cmdline
10/14/2019 09:20 PM 0 oj5z1fcy.dll
10/14/2019 09:20 PM 0 oj5z1fcy.err
10/14/2019 09:20 PM 0 oj5z1fcy.out
10/14/2019 09:20 PM 0 oj5z1fcy.tmp
10/14/2019 09:15 PM <DIR> vmware-testuser1
10/10/2019 02:06 AM 35,077,976 wct5500.tmp
10/11/2019 09:50 PM 20,668 wctABEA.tmp
9 File(s) 35,099,039 bytes
3 Dir(s) 47,555,522,560 bytes free

C:\Users\testuser1\AppData\Local\Temp>
```

- <random.cs>
- <random.cmdline>
- Csc.exe /noconfig /fullpaths @
<https://blog.didierstevens.com/2019/10/15/powershell-add-type-csc-exe/>

Control Panel Applets

- .CPL files are all those Control Panel applets

– Rundll32 C:\<whateverdir>\Fakejava.cpl



- Launches a bad DLL into memory - LOLBIN

- .cpl files load all the time, so it's noisy

- 3rd party applets are not well signed

- Many EDRs do not alert on this method

- The Red Team LOVES this method - CobaltStrike

	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:751	n/a		
2T13:26:59:391	n/a		
2T13:26:59:391	0x6b0	0x17	
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:137	0xaa4	0x10	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:200	0xaa4	0x18	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKNS4\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a

Monitoring for and Threat Hunting

Monitor for & Threat Hunting

- We need to develop a PROcess to monitor/detect for and/or Threat Hunt for signs of these techniques

• Step 1

- Enable the data
- Configure logs per the Windows Logging Cheat Sheet(s)
- Enable to collect 'Process Command Line'

• Step 2

- Create detections for many of these techniques
- Process command line is KEY.. It's in the parameters

Monitor for & Threat Hunting

Step 3

- Come up with a PROcess to scan Running Processes and their loaded Modules
 - Detect these memory only infections
 - This should be both for regular detection and for Threat Hunting
 - Watch for indications of injection

Monitor for & Threat Hunting

Strings

• Maybe a PROcess to scan strings for API calls such as;

- OpenProcess
- VirtualAlloc
- VirtualAllocEx
- WriteProcessMemory
- LoadLibrary
- LoadLibraryA
- CreateRemoteThread
- ResumeThread
- ReflectiveLoader()
- OpenProcess
- GetProcAddress
- CreateProcess
- ZwUnMapViewOfSection
- NtUnmapViewOfSection
- GetThreadContext
- SetThreadContext
- ResumeThread

LOLBINS/LOLBAS that can download

Short list per Cisco Talos

- powershell.exe
 - bitsadmin.exe
 - certutil.exe
 - psexec.exe
 - wmic.exe
 - mshta.exe
 - mofcomp.exe
 - cmstp.exe
 - windbg.exe
 - cdb.exe
 - msbuild.exe
 - csc.exe
 - regsvr32.exe
 - Excel too !!!
- mshta.exe
 - certutil.exe
 - bitsadmin.exe
 - regsvr32.exe
 - powershell.exe

Process Command Line is KEY

Map to MITRE ATT&CK

<https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html>

Best options for PROcess tools

- Log Management is your BEST friend here
 - If you have, and can afford to put agents on all your endpoints and collect the needed data
- If not, then you will need a PROcess to manually check running process, their modules and signs of injection
- LOG-MD-Premium, Systeinternals, Sysmon ID 8 & 10, using WinRM and ARTHIR, Memory dump with Volatility are possible options

	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\14323.vbs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T13:27:23:87	n/a	n/a	n/a

CONCLUSION

Conclusion

- Create a PROcess to look at running processes and their modules
- Look for signs of injection
- Log the process command line execution
- Monitor for the executions discussed in this presentation

Some tools to consider

Please let me know of any others

- LOG-MD-Premium
 - Running Process and Modules, Injection, and B9 static file analysis
- Volatility
 - <https://www.volatilityfoundation.org/>
 - HollowFind Plugin (Win 10 compatible?)
 - <https://github.com/monnappa22/HollowFind>
- PESieve (OpenSource)
 - <https://github.com/hasherezade/pe-sieve>
- Get-InjectedThread.ps1
 - <https://gist.github.com/jaredcatkinson/23905d34537ce4b5b1818c3e6405c1d2>
- PSReflect
 - <https://github.com/mattifestation/PSReflect>

Some tools to consider

Please let me know of any others

- GRR

- <https://github.com/google/grr>

- Rekall

- <http://www.rekall-forensic.com/home>

- InVtero

- <https://github.com/ShaneK2/inVtero.net>

- <https://github.com/seancomeau/inVtero.net>

- MemHunter (Old, requires .NET 3.5)

- <https://github.com/marcosd4h/memhunter>

Resources

- Red Canary Presentation
 - ATT&CK Deep Dive: Process Injection
- Article on MITRE ATT&CK Sub-Techniques (coming soon)
 - <https://medium.com/mitre-attack/attack-sub-techniques-preview-b79ff0ba669a>
- DeepInstinct - Process Injection and Manipulation
 - <https://www.deepinstinct.com/2019/09/15/malware-evasion-techniques-part-1-process-injection-and-manipulation/>
- EndGame – Hunting in Memory
 - <https://www.slideshare.net/JoeDesimone4/taking-hunting-to-the-next-level-hunting-in-memory>

Resources

- Websites

- [Log-MD.com](#)

- [ARTHIR.com](#)

- The “*Windows Logging Cheat Sheet(s)*”

- [MalwareArchaeology.com](#)

- This presentation and others on SlideShare

- Search for [MalwareArchaeology](#) or [LOG-MD](#)

Questions?

You can find us at:

- Log-MD.com
- [@HackerHurricane](https://twitter.com/HackerHurricane)
- MalwareArchaeology.com