



Bio Lab: Dissecting a Live PowerShell Attack

Mr. Ashley McGlone

Twitter: @GoateePFE

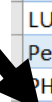
Technical Account Manager, Tanium





? !

A Comparison of Shell and Scripting Language Security – Lee Holmes

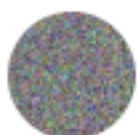


Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	Application Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	Untrusted Input Tracking
Bash	No**	No*	No	No	Yes	No	No*	Yes	No
CMD / BAT	No	No	No	No	Yes	No	No	No	No
Jscript	No	No	No	No	Yes	Yes	No	No	No
LUA	No	No	No	No	No	No	No*	Yes	Yes
Perl	No	No	No	No	No	No	No*	Yes	Yes
PHP	No	No	No	No	No	No	No*	Yes	Yes
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No**
Python	No	No	No	No	No	No	No	No	No**
Ruby	No	No	No	No	No	No	No**	No**	Yes
sh	No**	No*	No	No	No	No	No*	Yes	No
T-SQL	Yes	Yes	Yes	No	No	No	No**	No**	No
VBScript	No	No	No	No	Yes	Yes	No	No	No
zsh	No**	No*	No	No	No	No	No*	Yes	No

* Feature exists, but cannot enforce by policy

** Experiments exist

<https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/>



Matt Graeber

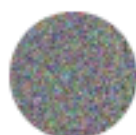
@mattifestation

Following



The security transparency is so good in PowerShell that I'm investing in other languages/frameworks w/ less/no security insight.

7:37 PM - 8 Sep 2017



Matt Graeber

@mattifestation

Following



Burning PS w/ fire in your org doesn't bother me. PS is never the reason ppl get owned and when it is used for evil, I'll have rich insight.

7:46 PM - 8 Sep 2017



FBI Warns of Banking Trojan That Eludes Antivirus as Fileless ...

Fileless malware is a growing threat to the banking industry requiring ... or using legitimate system administration tools such as PowerShell.

4 weeks ago



Ransomware, "wiper" malware attacks have more than doubled, IBM team says

X-Force's response to cases of destructive malware ... PowerShell scripts are still heavily used by ransomware ... 1 month ago



Crypto-Mining Malware Attacks up 29% in Q1: McAfee Report

Crypto-mining malware campaigns climbed 29 percent from Q4 2018 ... By using PowerShell, vulnerabilities in servers were exploited to mine ...

5 days ago



Cloud Atlas threat group updates weaponry with polymorphic malware

"This updated version is carried out in order to make the malware more effective ... This PowerShell-based module is also able to receive ... 3 weeks ago



FIN6 Switches Up PoS Tactics to Target E-Commerce

The backdoor code is the More_eggs JScript backdoor malware ... and Metasploit and PowerShell to move laterally and deploy malware.

4 days ago



```
PowerShell.exe  
-ExecutionPolicy Bypass  
-File c:\temp\invoke-evil.ps1
```

<https://blogs.msdn.microsoft.com/powershell/2008/09/30/powershells-security-guiding-principles/>

PowerShell Forensics Feature Matrix

WMF = Windows Management Framework (PowerShell upgrade)

	Win/Mac/Linux	Windows 10	Windows 8.1	Windows 8	Windows 7
	PS Core	WS 2016	WS 2012 R2	WS 2012	WS 2008 R2
Module Logging	Built-In	Built-In	Built-In	Built-In	WMF 5.1
Script Block Logging			WMF 5.1	WMF 5.1	
Transcription			Available	Available	
PSReadline Command History			n/a	n/a	Available
Anti-Malware Scan Interface	n/a				n/a

PowerShell Forensics Events & Log Files

	Event Log	Event IDs
Module Logging	Windows PowerShell	400, 800, 403
Module Logging	Microsoft-Windows-PowerShell/Operational	4103
Script Block Logging	Microsoft-Windows-PowerShell/Operational	4105, 4104, 4106
Anti-Malware Scan Interface	Microsoft-Windows-Windows Defender/Operational	1116, 1117
Transcription ◆	HKLM:\Software\Policies\Microsoft\Windows\PowerShell\Transcription\OutputDirectory	
PSReadline Command History ◆◆	C:\Users*\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline*.txt	

◆ *Path configured by policy*

◆◆ *Default path*

PS> Start-Demo



PowerShell Hygiene

Level 0: Upgrade all machines to Windows PowerShell 5.1 (WMF 5.1)

Level 1: Implement and monitor: logging & transcription

Level 2: Enable and secure remoting (default endpoint, firewall)

Level 3: Block evil code: AppLocker / DeviceGuard / AMSI

Key Takeaways

PowerShell is a POST-exploitation tool, not a vulnerability.

PowerShell is the MOST security-featured scripting language.

Properly configured, PowerShell leaves glowing fingerprints.

Don't be afraid of PowerShell remoting. Lock it down with JEA.

Upgrade to PowerShell 5.1 and remove the PS 2.0 Windows Feature.

THIS IS ALL FREE!

Resources

Free lab guide for learning PowerShell security

Reading list

PDF of this slide deck

<http://bit.ly/TNISSA19>



Mr. Ashley McGlone @GoateePFE



Security Feature Windows Integration Points

