1300 - Revoke-Obfuscation: PowerShell Obfuscation Detection (And Evasion) Using Science

Sunday at 13:00 in Track 4
45 minutes | Art of Defense, Demo, Tool
Daniel Bohannon (DBO)*Senior Consultant, MANDIANT*

Lee Holmes*Lead Security Architect, Microsoft*

Attackers, administrators and many legitimate products rely on PowerShell for their core functionality. However, its power has made it increasingly attractive for attackers and commodity malware authors alike. How do you separate the good from the bad?

A/V signatures applied to command line arguments work sometimes. AMSI-based (Anti-malware Scan Interface) detection performs significantly better. But obfuscation and evasion techniques like Invoke-Obfuscation can and do bypass both approaches.

Revoke-Obfuscation is a framework that transforms evasion into a treacherous deceit. By applying a suite of unique statistical analysis techniques against PowerShell scripts and their structures, what was once a cloak of invisibility is now a spotlight. It works with .evtx files, command lines, scripts, ScriptBlock logs, Module logs, and is easy to extend.

Approaches for evading these detection techniques will be discussed and demonstrated.

Revoke-Obfuscation has been used in numerous Mandiant investigations to successfully identify obfuscated and non-obfuscated malicious PowerShell scripts and commands. It also detects all obfuscation techniques in Invoke-Obfuscation, including two new techniques being released with this presentation.

Daniel Bohannon (DBO)
Daniel Bohannon is a Senior Incident Response Consultant at MANDIANT with over seven years of operations and information security experience. He is the author of the Invoke-Obfuscation and Invoke-CradleCrafter PowerShell obfuscation frameworks

@danielhbohannon
Lee Holmes
Lee Holmes is the lead security architect of Microsoft's Azure Management group, covering Azure Stack, System Center, and Operations Management Suite. He is author of the Windows

PowerShell Cookbook, and an original member of the PowerShell development team.

@Lee_Holmes, http://www.leeholmes.com/blog/

#defcon25/by_track/track4/sunday #defcon25/By_Day/_Sunday