PowerShell Hunting Cheat sheet

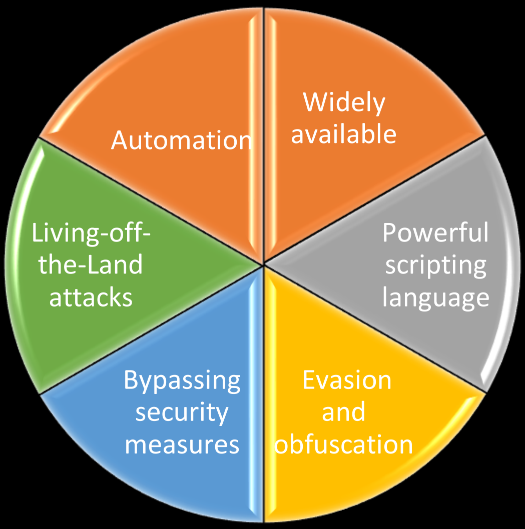
What is PowerShell?

• Task automation and configuration management framework from Microsoft.
• Consisting of a command-line shell and associated scripting language.
• Built on the .NET Framework.
• Enabling administrators to perform administrative tasks on both local and remote Windows systems

Basic Details of PowerShell

ID: T1086
Tactic: Execution
Platform: Windows
Permissions Required: User, Administrator
Data Sources: PowerShell logs, Loaded DLLs, DLL monitoring, Windows Registry, File monitoring, Process monitoring, Process command-line parameters
Supports Remote: Yes

Why attackers love PowerShell ?


Automation
Widely available
Living-off-the-Land attacks
Powerful scripting language
Bypassing security measures
Evasion and obfuscation

Well-known PowerShell Offensive Frameworks

POWERSHELL EMPIRE

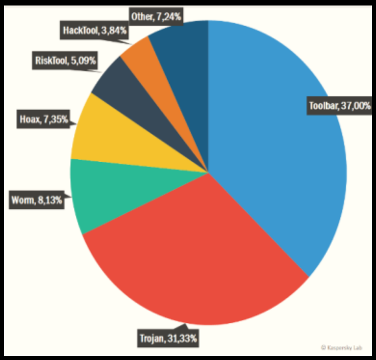
NISHANG

PS > ATTACK

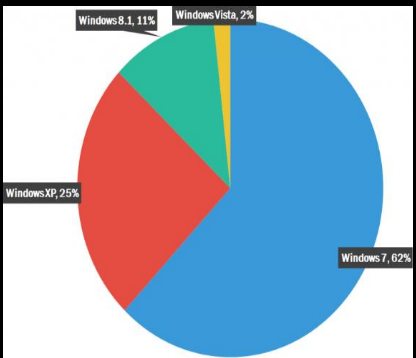
Invoke-Mimikatz

- PowerShell Arsenal
- DSInternals
- Inveigh
- PS>Attack
- PowerCat
- DarkObserver
- Invoke-Mimikatz
- Offensive-PowerShell
- Nishang
- PowerShell Suite
- Sherlock
- PowerShell-AD-Recon
- DSCCompromise
- Invoke-WMILM
- PowerSploit
- Empire
- PowerMemory
- Invoke-Mimikittenz
- Kautilya
- PoshRat
- OWA-Toolkit
- Invoke-Phant0m

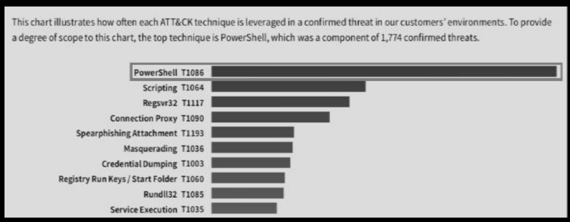
Some statics on PowerShell Attack



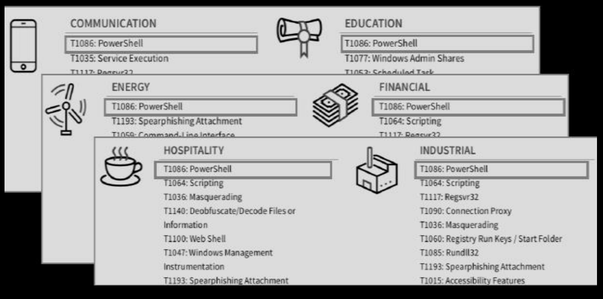
Rise of PowerShell Malware



Most attacked operating systems by malware written in any .NET compatible language.



This chart illustrates how often each ATT&CK technique is leveraged in a confirmed threat in our customers' environments. To provide a degree of scope to this chart, the top technique is PowerShell, which was a component of 1,774 confirmed threats.



COMMUNICATION
T1086: PowerShell
T1035: Service Execution
T1117: Regsvr32

EDUCATION
T1086: PowerShell
T1077: Windows Admin Shares
T1053: Scheduled Task

ENERGY
T1086: PowerShell
T1193: Spearphishing Attachment
T1059: Command-Line Interface

FINANCIAL
T1086: PowerShell
T1064: Scripting
T1117: Regsvr32

HOSPITALITY
T1086: PowerShell
T1064: Scripting
T1036: Masquerading
T1140: Deobfuscate/Decode Files or Information
T1100: Web Shell
T1047: Windows Management Instrumentation
T1193: Spearphishing Attachment

INDUSTRIAL
T1086: PowerShell
T1064: Scripting
T1117: Regsvr32
T1090: Connection Proxy
T1036: Masquerading
T1060: Registry Run Keys / Start Folder
T1085: Rundll32
T1193: Spearphishing Attachment
T1015: Accessibility Features

Fileless Attack Example Exploiting PowerShell

1. The User Visits an Infected Website or Opens a Malicious Link.

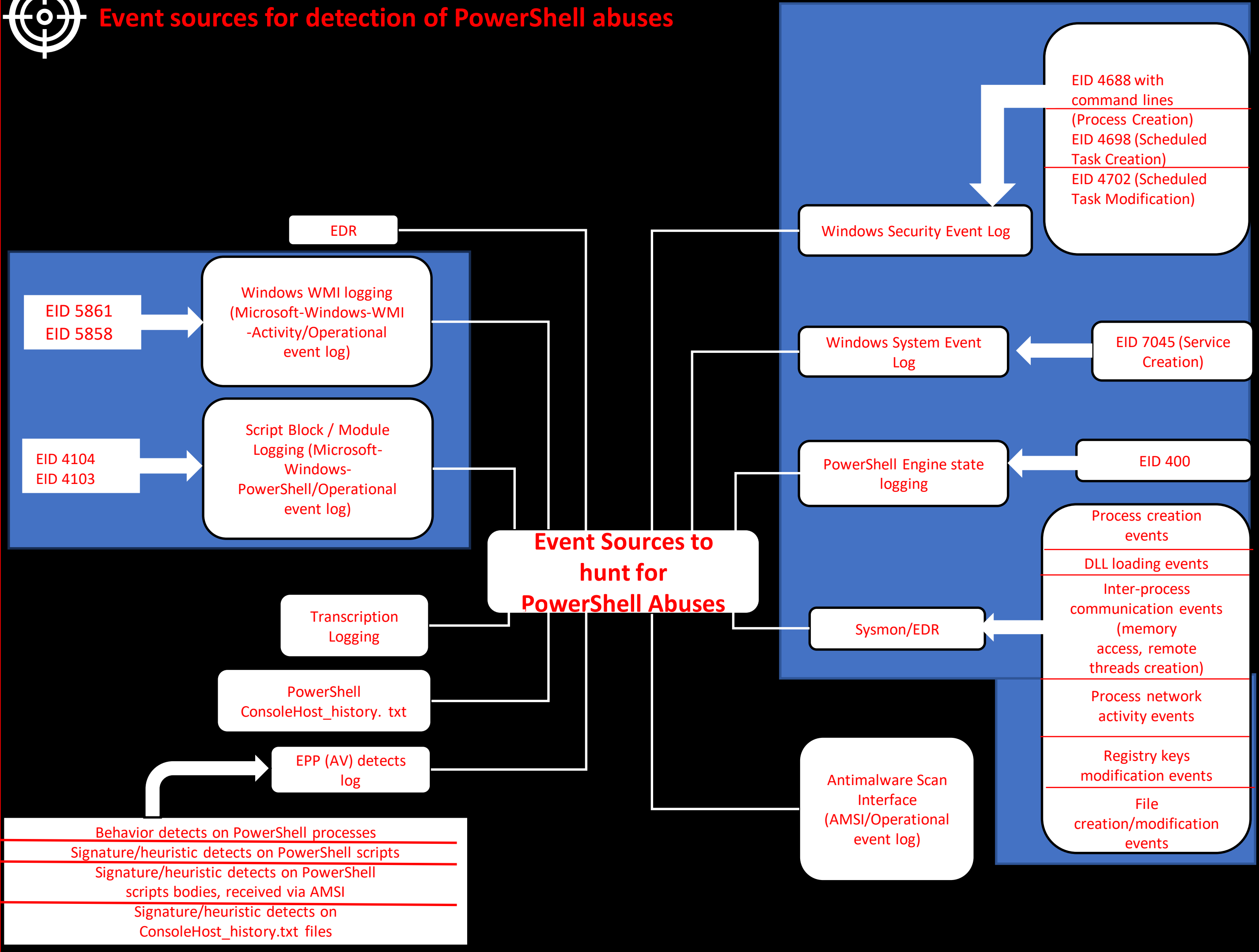
2. Flash Java Is Loaded on the Website and the User's Device Is Scanned for Vulnerabilities.

3. A Shell Code Launches PowerShell. The Attacker Can Run Malicious Command Line Operations In the User's OS Memory.

4. The Script In PowerShell Downloads and Executes a Payload Carrying Out Malicious Activity in the User's OS Memory.

5. The Fileless Attack Is Successful. The Cybercriminal Can Now Steal Sensitive Data, Launch a Ransomware Attack, and More.

Event sources for detection of PowerShell abuses



Event Sources to hunt for PowerShell Abuses

EDR

EID 5861
EID 5858
→ Windows WMI logging (Microsoft-Windows-WMI-Activity/Operational event log)

EID 4104
EID 4103
→ Script Block / Module Logging (Microsoft-Windows-PowerShell/Operational event log)

Transcription Logging

PowerShell ConsoleHost_history. txt

EPP (AV) detects log

Behavior detects on PowerShell processes
Signature/heuristic detects on PowerShell scripts
Signature/heuristic detects on PowerShell scripts bodies, received via AMSI
Signature/heuristic detects on ConsoleHost_history.txt files

EID 4688 with command lines (Process Creation)
EID 4698 (Scheduled Task Creation)
EID 4702 (Scheduled Task Modification)
→ Windows Security Event Log

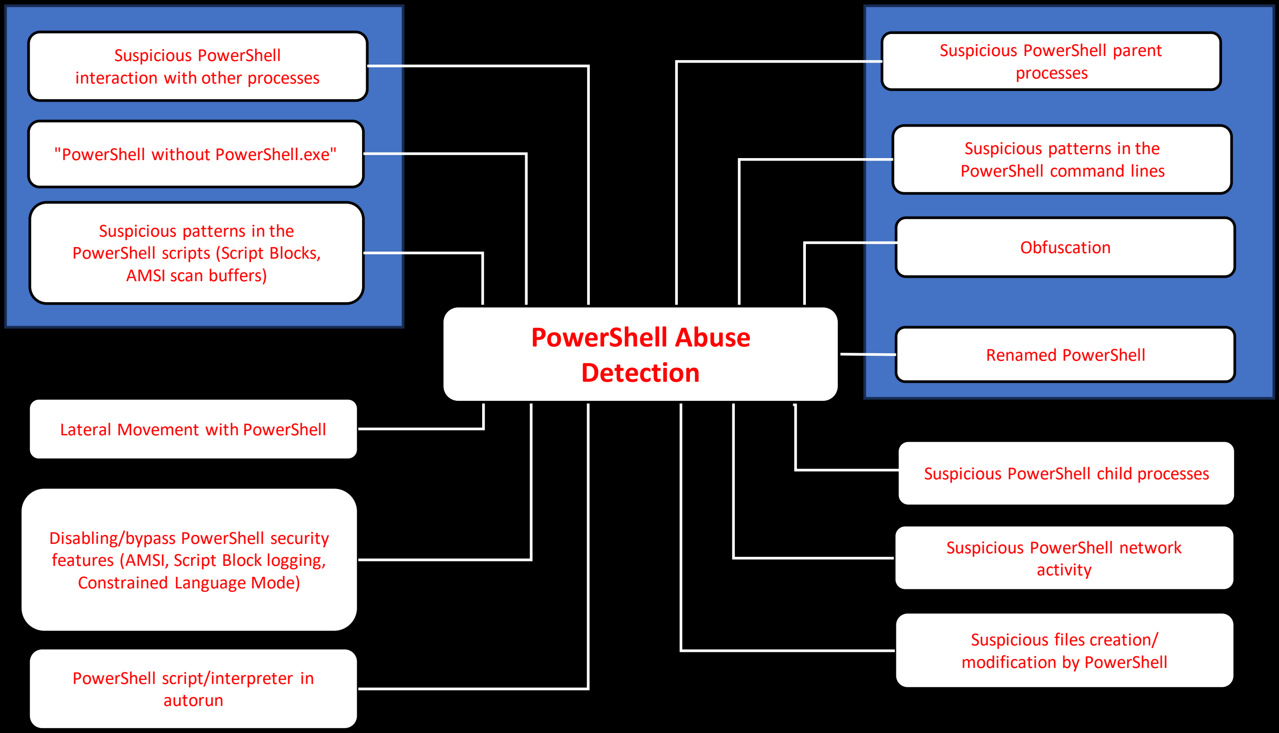
EID 7045 (Service Creation) → Windows System Event Log

EID 400 → PowerShell Engine state logging

Process creation events
DLL loading events
Inter-process communication events (memory access, remote threads creation)
Process network activity events
Registry keys modification events
File creation/modification events
→ Sysmon/EDR

Antimalware Scan Interface (AMSI/Operational event log)

PowerShell abuse patterns



PowerShell Abuse Detection

Suspicious PowerShell interaction with other processes

"PowerShell without PowerShell.exe"

Suspicious patterns in the PowerShell scripts (Script Blocks, AMSI scan buffers)

Lateral Movement with PowerShell

Disabling/bypass PowerShell security features (AMSI, Script Block logging, Constrained Language Mode)

PowerShell script/interpreter in autorun

Suspicious PowerShell parent processes

Suspicious patterns in the PowerShell command lines

Obfuscation

Renamed PowerShell

Suspicious PowerShell child processes

Suspicious PowerShell network activity

Suspicious files creation/ modification by PowerShell