**Usecase**

Powershell Obfuscation

**Background**

Usecase ini berkaitan dengan Teknik MITRE berikut :

**1027.010 Obfuscated Files or Information: Command Obfuscation**

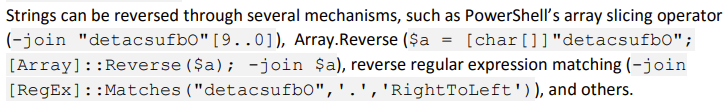
**A screenshot of a computer

Description automatically generated**

Ada beberapa teknik yang digunakan untuk mendeteksi Powershell Obfuscation,

salah 1 nya adalah Reverse Command (existing usecase).

1. **Potential PowerShell Obfuscation Via Reversed Commands**

****

**A screenshot of a computer code

Description automatically generated**

1. **Potential PowerShell Obfuscation Via WCHAR**

Detects suspicious encoded character syntax often used for defense evasion.

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated

1. **Powershell Obfuscation and Escape Characters**

Looks for the execution of PowerShell with unusually high counts of characters like ^, +, $, and %.

Inspired by the 2022 Red Canary Threat Detection report.

**A screenshot of a computer

Description automatically generated** **A screenshot of a computer

Description automatically generated**

Usecase akan memonitor jika dalam command powershell ditemukan,

sedikitnya 5 karakter - ^, +, $, and %

**Detection**

**Process name Is:**

Powershell

**Command Is:**

|  |  |  |
| --- | --- | --- |
| * Hctac * kaerb * dnammoc * ekovn * ekovni * eliFd * rahc * etirw * golon | * tninon * eddih * tpircS * ssecorp * llehsrewop * esnopser * daolnwod * tneilCbeW * tneilc | * hcaerof * ptth * elifotevas * 46esab * htaPpmeTteG * tcejbO * maerts * retupmoc |

* char\)\s+0x
* char\]\s+0x
* '^([^^+$%]\*[\^+$%]){5,}[^^+$%]\*$'

**Procedure**

* Periksa aktivitas parent process (aplikasi) yang menjalankan perintah powershell, baik sesudah maupun sebelum alert ke trigger.
* Jalankan full scan antivirus.

**Reference**

<https://www.blackhat.com/docs/us-17/thursday/us-17-Bohannon-Revoke-Obfuscation-PowerShell-Obfuscation-Detection-And%20Evasion-Using-Science-wp.pdf>

<https://redcanary.com/threat-detection-report/techniques/powershell/>