Appendix A — Detections & Emulation

Author: Tafadzwa Victor Chipere | Date: 2025-10-02

# A.1 Sigma — Process Creation (powershell -enc + Graph API)

title: APT29 - PowerShell Encoded Command with Graph API  
id: 0c7d0c6e-5f0e-4d9e-9d6a-apt29-pwsh-graph  
status: experimental  
description: Detects PowerShell with -enc/-EncodedCommand that also references graph.microsoft.com (possible token/API abuse).  
author: Tafadzwa Victor Chipere  
date: 2025-10-02  
references:  
 - https://attack.mitre.org/techniques/T1059/001/  
 - https://attack.mitre.org/techniques/T1106/  
tags:  
 - attack.execution  
 - attack.t1059.001  
 - attack.t1106  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 sel\_encoded:  
 CommandLine|contains:  
 - " -enc "  
 - " -EncodedCommand "  
 sel\_graph:  
 CommandLine|contains|all:  
 - powershell  
 - graph.microsoft.com  
 condition: sel\_encoded and sel\_graph  
falsepositives:  
 - Admin or automation scripts that legitimately call Graph API via encoded payloads  
level: high

# A.2 Sigma — PowerShell ScriptBlock (Event ID 4104)

title: APT29 - PowerShell ScriptBlock Graph API Access  
id: 3bf6f7d3-1b0a-4a14-87c8-apt29-ps-4104-graph  
status: experimental  
description: Detects PowerShell ScriptBlock content that calls Microsoft Graph API, useful for spotting token/API abuse even when process command line is benign.  
author: Tafadzwa Victor Chipere  
date: 2025-10-02  
references:  
 - https://attack.mitre.org/techniques/T1059/001/  
 - https://attack.mitre.org/techniques/T1106/  
tags:  
 - attack.execution  
 - attack.t1059.001  
 - attack.t1106  
logsource:  
 product: windows  
 service: powershell  
detection:  
 sel\_graph:  
 ScriptBlockText|contains:  
 - "graph.microsoft.com"  
 sel\_cmdlets:  
 ScriptBlockText|contains:  
 - "Invoke-RestMethod"  
 - "Invoke-WebRequest"  
 condition: sel\_graph and sel\_cmdlets  
falsepositives:  
 - Legitimate admin/automation scripts that interact with Graph API  
level: high

# A.3 Platform Translations (examples)

Paste the translated queries generated in Uncoder.io here (Elastic, Splunk SPL, Sentinel KQL, QRadar).

• Elastic example: (paste from Uncoder right pane)

• Sentinel (KQL) example: (paste from Uncoder right pane)

• Splunk SPL example: (paste from Uncoder right pane)

# A.4 Screenshots (placeholders)

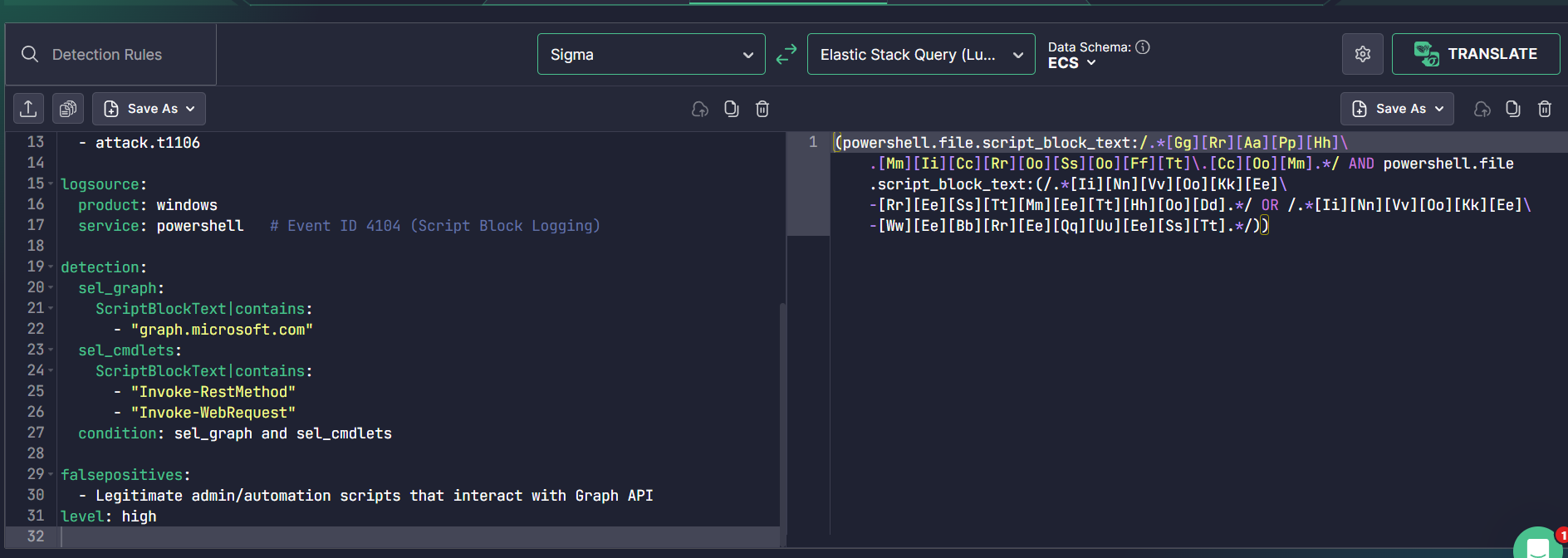


Figure A1 — Uncoder.io translation of Sigma (process\_creation → Elastic). [Insert image]

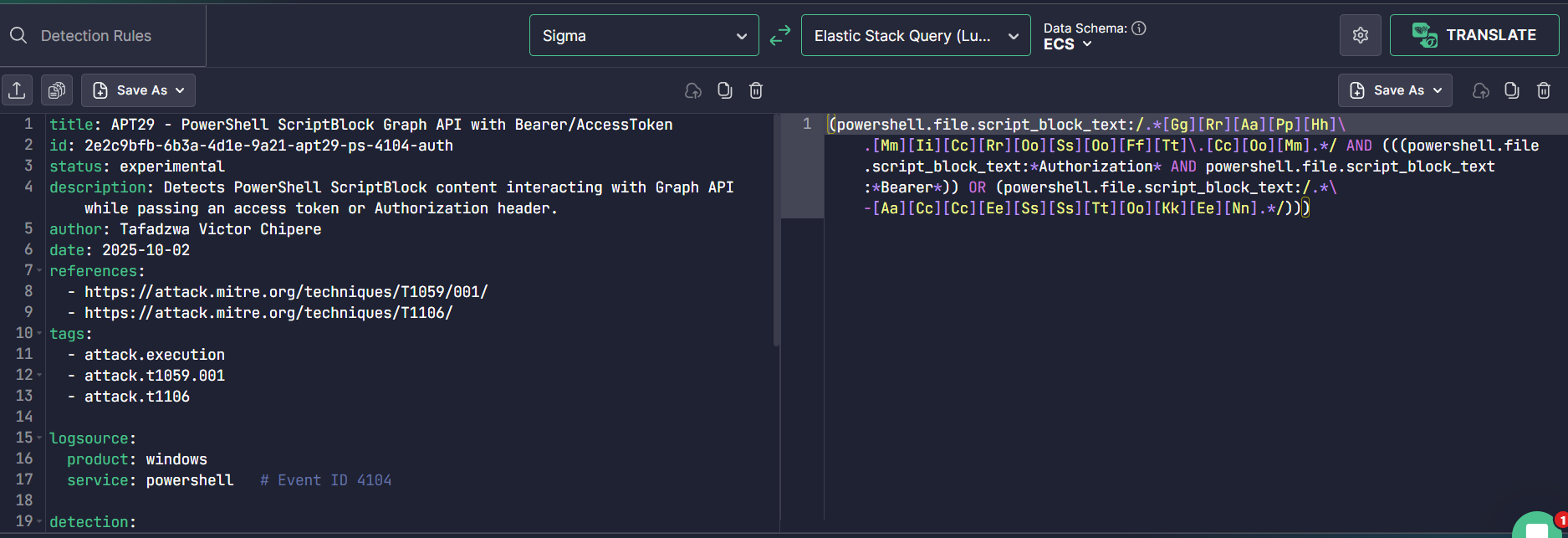


Figure A2 — Uncoder.io translation of Sigma (ScriptBlock EID 4104 → KQL/Splunk). [Insert image]

# A.5 Emulation & Validation Notes

Validated in a lab using Atomic Red Team (T1059.001) to trigger PowerShell behaviours. MITRE CALDERA was used to simulate higher‑level behaviours. Ensure testing is performed only in isolated environments.