

Background

You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks

Uetz et al.
USENIX '24

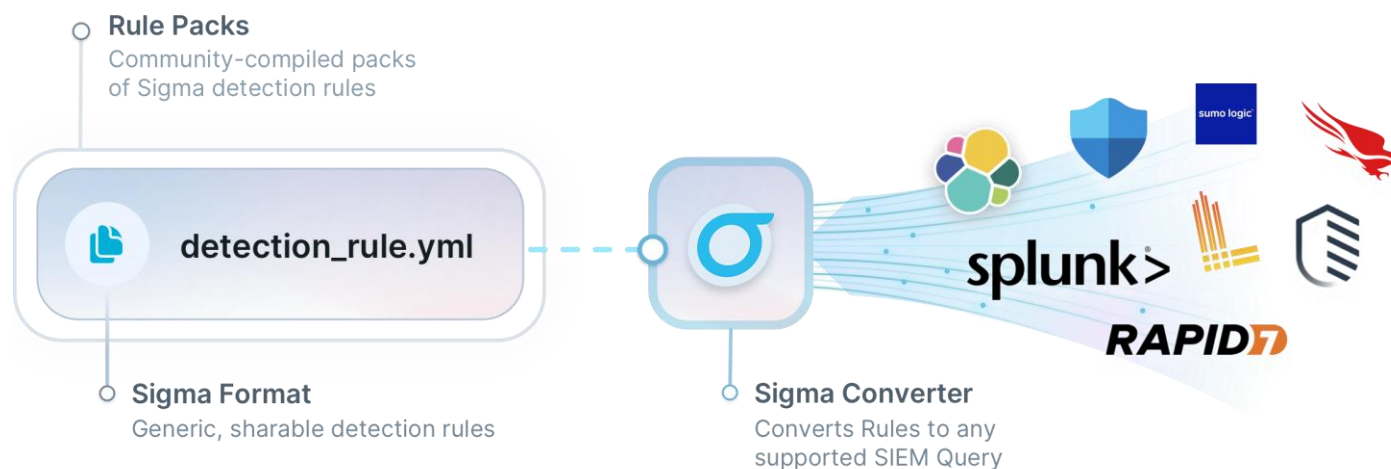
What is SIEM?

- Definition
 - Security Information and Event Management (SIEM) systems **collect, store, and analyze security-related data**
- Key Function
 - Aggregating logs from endpoints, server, network drivers, etc.
 - Correlating events to identify potential security incidents
- Purpose
 - Provide real-time alerts and support incident response in enterprise networks



SIEM Rules explained – Introduction


- Rule-based Detection
 - SIEM systems largely rely on expert-crafted rules
 - Match patterns in event data (e.g., process creation, network connections..)
- Examples: Sigma Rules
 - Highly active open-sourced rule sets






SIEM Rules explained – Sigma Rules

- Sigma Rules?
 - More than 3,000 detection rules, fully open-sourced
 - Standardized signature format to describe relevant log events.
 - Can be converted to queries for any SIEM or log management platform.
- Three-types
 - Generic Detection Rules: Detect behaviors or techniques used by threat actors, regardless of the specific threat.
 - Threat Hunting Rules: Serve as starting points for analysts to proactively hunt for suspicious activities.
 - Emerging Threat Rules: Focus on timely threats, such as new APT campaigns or zero-day exploits.

SIEM Rules explained – Sigma Rules (Examples)

[sigma](#) / [rules-emerging-threats](#) / [2023](#) / [TA](#) / [FIN7](#) / [file_event_win_apt_fin7_powershell_scripts_naming_convention.yml](#) 

[sigma](#) / [rules-emerging-threats](#) / [2023](#) / [TA](#) / 

 **frack113** Merge PR #5169 from @frack113 - Add missing `detection.emerging-threa...  

Name



..



3CX-Supply-Chain



Cozy-Bear



Diamond-Sleet



EquationGroup



FIN7



Lace-Tempest



Lazarus



Mint-Sandstorm



Mustang-Panda-Australia-Campaign



Okta-Support-System-Breach



Onyx-Sleet






PaperCut-Print-Management-Exploitation



Peach-Sandstorm



UNC4841-Barracuda-ESG-Zero-Day-Exploitation

 **nasbench** Merge PR #4950 from @nasbench - Comply With v2 Spec Changes  

Code

Blame

23 lines (23 loc) · 727 Bytes

```
1  title: Potential APT FIN7 Related PowerShell Script Created
2  id: a88d9f45-ec8a-4b0e-85ee-c9f6a65e9128
3  status: test
4  description: Detects PowerShell script file creation with specific name or suffix which was seen being used often by FIN7 PowerShell scripts
5  references:
6    - https://labs.withsecure.com/publications/fin7-target-veeam-servers
7  author: Nasreddine Bencherchali (Nextron Systems)
8  date: 2023-05-04
9  tags:
10   - attack.execution
11   - attack.g0046
12   - detection.emerging-threats
13  logsource:
14    category: file_event
15    product: windows
16  detection:
17    selection:
18      - TargetFilename|endswith: '_64refl.ps1'
19      - TargetFilename: 'host_ip.ps1'
20    condition: selection
21  falsepositives:
22    - Unknown
23  level: high
```

To resolve the list of collected IP addresses to their respective host names, a custom PowerShell script, "host_ip.ps1", was executed. The PowerShell script content is nearly identical to a code snippet shared online for resolving IP to Hostname with PowerShell[8]. "host_ip.ps1" file name has been reportedly observed in FIN7's attack arsenal[7].

```
# Get list from file, initialize empty array
```

```
$ListOfIPs=Get-content "ips.txt"
$ResultList = @()
```

Sigma Rules– Double-edged

- **Advantages:**
 - Broad community review and improvement
 - Rapid updates in response to emerging threats
- **Challenges:**
 - Transparency: Attackers can study the rules
 - Adaptation: Allows adversaries to modify attacks to evade detection
 - Detection Blind Spots: Easier for attackers to exploit minor variations not covered by existing rules

Sigma Rules– Evasion techniques

- **Techniques:**
 - **Insertion:** Insert characters (e.g., extra spaces, double quotes)
 - **Substitution:** Replace standard symbols (e.g., `-O -> --remote-rename`)
 - **Omission:** Remove characters or shorten arguments
 - **Reordering:** Change order (e.g., `-ma ls -> ls -ma`)
 - **Recoding:** Alter encoding or representation of arguments (e.g., `127.0.0.1 -> 2130706433`)

Table 1: Almost half of the analyzed SIEM rules (129 of 292) can be evaded using the five straightforward evasion types presented in this table (each with one concrete example), thus causing critical detection blind spots in enterprise networks.

Evasion type	Sample affected rule	Affected search term	Sample match	Sample evasion
Insertion	win_susp_schtask_creation	<code>* /create *</code>	<code>schtasks.exe /create ...</code>	<code>schtasks.exe /"create" ...</code>
Substitution	win_susp_curl_download	<code>_ -O _</code>	<code>curl -O http://...</code>	<code>curl --remote-name http://...</code>
Omission	win_mal_adwind	<code>*cscript.exe *Retrive*.vbs *</code>	<code>cscript.exe ...\Retrive.vbs</code>	<code>cscript ...\Retrive.vbs</code>
Reordering	win_susp_procdump	<code>* -ma ls*</code>	<code>procdump -ma ls</code>	<code>procdump ls -ma</code>
Recoding	win_vul_java_remote_dbg	<code>*address=127.0.0.1*</code>	<code>...address=127.0.0.1,...</code>	<code>...address=2130706433,...</code>

SIEM systems – Misuse detection, Limitation

- Misuse detection
 - Detecting intrusions based on known patterns (i.e., signatures/rules)
 - Simplicity, clarity → predominant method in enterprise security monitoring
- Limitation:
 - Coverage: Rules may not cover all attack variations (i.e., evasion techniques)
 - Complexity: Expanding rule sets to cover all possibilities may computationally feasible
 - Risk: Relying on static rules result when attacker understands rules, they can tailor attacks to fly under a radar.

SIEM systems – Need for adaptive misuse detection

- Core problem: Blind spots due to “evasions”
- Adaptive misuse detection
 - Enhance established technique by comparing events not only against rules but also against known-benign behavior.
 - Approach: Leverage ML to identify events resemble malicious activity even it doesn't match any specific rule.
 - **AMIDES** (Rule-based alerts + Adaptability of anomaly detection)

Thank You! Any Questions?