IJHSR
ijhighschoolresearch.org
RESEARCH ARTICLE

Utilization of Artificial Intelligence to Enrich Threat Detection Marketplaces for Small and Medium Enterprises

Alfredo Lopez-Salas

Round Rock High School, 01 Deep Wood Dr, Round Rock, Texas, 78681, USA; alfredols1313@gmail.com

ABSTRACT: Traditional Security Operation Centers (SOC) depend on multiple sources of security events to correlate alerts and identify malicious activity that represents an emerging threat against the organization. These sources may generate gigabytes or terabytes of data, which makes it difficult to analyze and identify true positive malicious activity, as it consumes a lot of resources for most organizations. With this large amount of data to analyze, plus the growing volume of malicious actors that intend to affect critical operations, organizations require better responsiveness to address threats and improve the company's cybersecurity posture by reducing the risk. While modern security solutions leverage Artificial Intelligence to improve analysis and correlation of events, those solutions are cost-prohibitive for Small and Medium Enterprises (SME). The introduction of Threat Detection Marketplaces (TDM) helps SOC teams with faster detection of threats by leveraging the collective security industry expertise to empower smart data orchestration and cost-efficient threat hunting. While TDM gives organizations tested Sigma rules from industry experts, Artificial Intelligence can improve the TDM content and offerings in many ways, such as Sigma rules optimization and validation, rules correlation with MITRE tactics for maturity assessments, and new rules based on unusual patterns or behaviors.

KEYWORDS: Systems Software, Cybersecurity, Artificial Intelligence, Threat Detection Marketplaces, Sigma Rules.

Introduction

The past five years have seen a significant increase in cybersecurity incidents targeted at businesses and organizations of varying sizes and industries.[1] These incidents, defined as data breaches or security threats, have led to the compromise of sensitive information, disruption of critical production operations, and hardship associated with considerable financial loss. A business with fewer than 500 employees, also known as a Small and Medium Enterprise (SME), is considered more vulnerable to these targeted incidents due to its limited budget and resources. Therefore, the implementation of strong preventive measures and early detection mechanisms is essential for maintaining operational continuity within an SME.[1]

Security industry threat reports have raised pointed concerns over the shift in attack methodologies amongst malicious actors due to the increase in the timeliness, precision, and overall organization of recent documented cybersecurity incidents.[2] The CrowdStrike 2025 Global Threat Report discussed the perceived change in demeanor of the "typical" malicious actor, stating that these individuals have shown increased maturity and complexity in their tailored attacks compared to previous years.[2] This prioritization of structure displays how attackers have adjusted over time to mirror the same business-like efficiency as the organizations being targeted. The CrowdStrike 2025 Global Threat Report also noted that 2024 experienced a 150% increase in malicious activity originating from foreign countries, such as China, targeted across all business sectors.[2] This observed evolution has rendered SMEs particularly susceptible to long-term damages associated with the increased rate of targeted, complex cybersecurity incidents.

Financial constraints and a lack of established cybersecurity and data integrity infrastructure are two barriers that burden many SMEs. These pervasive obstacles prevent many SMEs from implementing a proactive strategy equipped to adequately respond to a cybersecurity incident.[3] In contrast, well-established, large-scale businesses have resources allotted for the creation and maintenance of dedicated teams focused on the prevention and reaction to cybersecurity incidents. This disparity in cybersecurity measures between SMEs and large-scale companies reveals a necessity for additional research that addresses the market deficiency of adequate cybersecurity techniques tailored towards SMEs. Although SMEs are responsible for employing a large percentage of the global workforce, the volume of cybersecurity research specifically focused on SMEs remains disproportionately low. Furthermore, documented cybersecurity industry reports have shown that approximately 72% of total cybersecurity breaches specifically target SMEs.[4]

An estimated 60% of SMEs cease operations within six months of a significant cybersecurity event.[4] Given that SMEs account for approximately 90% of active businesses and more than 50% of the world's employment rate,[5] an influx of cyberattacks targeting SMEs presents a direct threat to the global economy. Research focused on developing and strengthening techniques to mitigate cybersecurity incidents targeting SMEs should be prioritized, given the undeniable impact they have on the international economy.[3]

Purpose of the Study:

This research focuses on assimilating AI solutions and Sigma rules repositories to enrich Threat Detection Marketplaces

DOI: 10.36838/v8i1.1

(TDM) to help SMEs enhance their current detection capabilities and identify emerging threats that are more applicable to the organization's budget, profile, threat landscape, and current security solutions already acquired. This study also intends to help SMEs develop and implement best practices for low-budget security operations centers, focusing on real case scenarios using AI solutions and publicly available threat simulation indices and Sigma Repositories to enhance the effectiveness of the SOC analysts.

Oracle Cloud Infrastructure (OCI) has been adopted by a diverse range of companies, including small and medium enterprises, based on an analysis conducted by Lyft, a platform that provides access to real-time company insights such as technology usage.[6] Analysis from Lyft reported that the Oracle customers who use OCI, 20% are small (less than 50 employees), 37% are medium, and 42% are large (more than 1000 employees).[6] The analysis also reported that the revenue generated by the enterprises that use OCI, 37% small (less than $50M), 15% are medium, and 42% are large (more than$1000M).[6] This data was based on 2,601 companies that use OCI and shows the potential impact of a malicious actor against SMEs and the considerable threat landscape they represent.[6]

On March 21, 2025, cybersecurity company CloudSEK discovered a malicious threat actor that claimed to be selling 6 million data records stolen from Oracle's cloud federated Single Sign-On (SSO) login servers. The threat actor claimed the data, which included Java Keystore (JKS) files, encrypted SSO passwords, and other sensitive data, involved 140,000 OCI tenants.[7] The attacker, active since January 2025, has sought assistance to decrypt the stolen data and secrets, while also demanding payment to delete the stolen data which could affect the SMEs Information Technology (IT) operating procedures and spend money that was not planned in the organization's revenue forecast.[7] The main recommendation to mitigate the impact of this potential incident, besides rotating secrets used to access OCI, is to improve the organization SOC focusing on the logging and monitoring controls to detect malicious activity involving account credential misuse in OCI, due to the potential compromise of user accounts.[7] This scenario describes a real-world threat that could impact SMEs and lists some of the recommended controls to mitigate it. The objective is to raise awareness that SMEs are frequent targets of malicious activity.

The Importance of Security Operations Centers:

An SOC can help organizations continuously analyze malicious events by utilizing centralized logging and monitoring functions to encompass people, technology, and procedures within the organization.[8] Typically, an SOC aligns with the National Institute of Standards and Technology (NIST) cybersecurity framework core recommendations to identify malicious activity affecting credentials misuse and compromise. A traditional SOC can also help the organization's security posture as it covers three of the five concurrent and continuous functions of a cybersecurity framework, which are Identify, Detect, and Respond to security incidents.[8,9] Not all SMEs can afford a scalable SOC platform to prevent and respond to ongoing incidents. Security analysts with the required experience to review the security events to make appropriate decisions are scarce and expensive.[8] To be able to identify malicious activity in the organization's infrastructure, an SOC first needs to obtain and correlate security events from multiple sources. Once the sequence of security events has been identified, the SOC must conduct real-time analysis on the large volumes of cybersecurity data, such as identity and access management logs, threat intelligence feeds, and network perimeter security stack events (e.g., Web Application Firewalls, Network Intrusion Detection and Prevention Systems, etc.).[10] Simultaneously balancing day-to-day operations while prioritizing timely incident response presents a pervasive challenge for SMEs. Examining large volumes of events and determining efficient remediation measures to address incidents can overwhelm SOC analysts.[10] The adoption of Security Incident and Event Management (SIEM) systems can assist SOC analysts in the timely detection and response to cybersecurity incidents. These systems allow for the integration of Artificial Intelligence (AI) and Machine Learning (ML) algorithms to process large volumes of collected events in real-time, allowing analysts to respond to incidents in a timely manner.[10]

Establishing an SOC and implementing SIEM systems can be cost-prohibitive to the typical SME facing financial constraints associated with scaling a business. As such, it is important for research to help in the evolution of techniques and systems focused on properly protecting data while maintaining accessibility across all businesses.

Methods

Threat Detection Marketplace:

A TDM is a centralized platform where security analysts can download specific SOC security alert content and tailor the detection rules into the security solution of their choice, such as SIEM or Endpoint Detection and Response (EDR). A TDM also allows security engineers to create custom detection rules and content lists based on Sigma rule repositories that are continuously enhanced with new detection ideas from the incident response and detection community. Leveraging TDM, cybersecurity analysts can save time as they offer security rules based on MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and real-world incidents that have been validated by the security community.[11]

SOC Prime is a commercial example of a TDM that provides a continuously updated library of behavioral analytics and detection rules, mapped to the ATT&CK techniques for coverage analysis that can be used in any SIEM platform. SOC Prime, as a TDM that is geared towards organizations with large SOCs, can be expensive for most of the SMEs due to its complex-grade detections and customer support services for content validation.[11] There are affordable TDM solutions such as SigmaHQ, which is the TDM that this paper leveraged, as part of the Indicators of Attack (IOA) examples that are presented in the following sections.

Sigma Rules:

As described in the previous section, today, cybersecurity experts collect security events for threat detection analysis and are starting to create their own searches, queries, and correlations of events.[12] While this is a great approach that changes the mindset of cybersecurity analysts, they lack a common format to build those queries and rules in which analysts can share their work with the rest of the security industry, following the Open-Source Community approach.[12] That is exactly what a Sigma rule is: a generic signature template that enables security analysts to describe security logs applicable to the profile or the organization in a structured, flexible, and easy-to-write format.[12] Sigma signatures shall not be confused with other rules, such as Yet Another Recursive Acronym (YARA) or Indicators of Compromise (IOC) rules that detect network traffic from malicious actors or malicious files that could be used as malware or ransomware attacks; Sigma rules are focused on security log event solutions, such as SIEM platforms.[12] Some of the Sigma rules' benefits and characteristics include that they are vendor agnostic, easy to write and share between the security industry communities, and that they are supported by a big community of Threat Detection analysts that contribute to the list of detection and hunting rules. Other important aspects are that Sigma is easy to read because they are written in plain YAML format and which allows fast threat detection coverage as it allows analysts to respond to new security threats quickly across their organizations.[12]

ChatGPT:

ChatGPT has the potential to allow cybersecurity analysts to focus on more complex and strategic tasks by reducing the need for extra employees to handle SOC operations, such as the creation of new detection rules.[13] ChatGPT could also enhance the operations of a SIEM solution by making it faster to create security event queries and by assisting the SOC employees in learning more about the SIEM.[13] To improve the SIEM capabilities of monitoring and threat detection, ChatGPT can be asked to generate an IOA, using Sigma rules, with the required format and syntax, without needing to be a subject matter expert in the detection platform.[13]

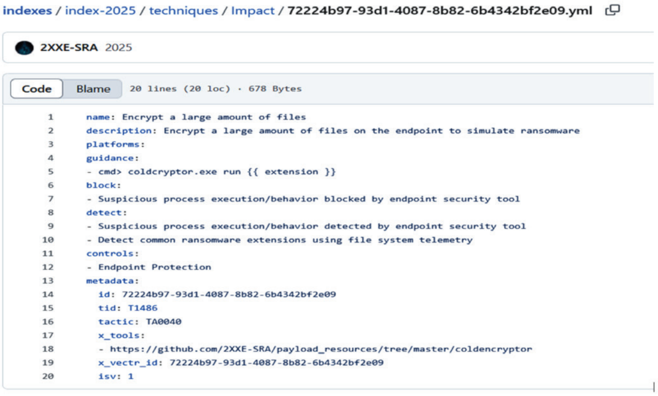
Using ChatGPT for this threat detection use case brings several benefits for the SIEM operations, but it could also present challenges, such as extra validation required, as ChatGPT does not have direct access to the organization's logs. SMEs shall not include production logs within the ChatGPT queries to avoid data privacy regulation issues.

Result and Discussion

A critical aspect that every cybersecurity specialist needs to keep in mind when working with ChatGPT or other AI technology is to be as descriptive as possible when creating the query. The more details around the use cases and requirements are provided to the AI solution, the better output will be provided with fewer errors and false positives when detecting a potential threat. As a rule, bad input equals bad output, great input equals great output. It is recommended to work with each of the solutions experts to identify gaps in the rules provided by ChatGPT and improve the detection capabilities. This and other best practices, such as iterating and monitoring, testing in a controlled environment, and tailoring the rules to the organization's environment, will avoid false positives.

CrowdStrike Indicator of Attack, Ransomware – Example 1:

The following example shows the steps to create an IOA signature for the EDR solution CrowdStrike, based on the YARA attack technique taken from the Security Risk Advisor Index hosted in the path: index-2025/techniques/Impact/72224b97-93d1-4087-8b82-6b4342bf2e09.yml.[14] Figure 1 shows the YARA rule used to identify malware samples based on detection patterns.



indexes / index-2025 / techniques / Impact / 72224b97-93d1-4087-8b82-6b4342bf2e09.yml

2XXE-SRA 2025

20 lines (20 loc) · 678 Bytes

```
name: Encrypt a large amount of files
description: Encrypt a large amount of files on the endpoint to simulate ransomware
platforms:
guidance:
- cmd> coldcryptor.exe run {{ extension }}
block:
- Suspicious process execution/behavior blocked by endpoint security tool
detect:
- Suspicious process execution/behavior detected by endpoint security tool
- Detect common ransomware extensions using file system telemetry
controls:
- Endpoint Protection
metadata:
  id: 72224b97-93d1-4087-8b82-6b4342bf2e09
  tid: T1486
  tactic: TA0040
  x_tools:
  - https://github.com/2XXE-SRA/payload_resources/tree/master/coldencryptor
  x_vectr_id: 72224b97-93d1-4087-8b82-6b4342bf2e09
  isv: 1
```

Figure 1: The YARA attack technique was used to create the IOA signature for CrowdStrike. This security risk advisory technique detects a suspicious process that encrypts many files on an endpoint to simulate a ransomware attack. This technique also detects common ransomware extensions using file system telemetry controls.

ChatGPT Query. The objective is to build a CrowdStrike IOA rule that matches the behavior documented in the YARA rule that the security analyst provides as part of the input to ChatGPT. The YARA rule is intended to detect malicious elements within files on endpoints. In this case, the IOA will detect malicious activity like a ransomware attack, encrypting multiple files, triggered by the file coldcryptor.exe. The text below is the full query provided to ChatGPT. The black text represents the request to ChatGPT, while the blue text indicates the YARA attack technique that will be included as part of the query input.

Build a CrowdStrike Indicator of Attack (IOA) to detect malicious activity on endpoints based on the following YARA Attack Technique. Obtain the JSON file template that I can use to upload the IOA via CrowdStrike APIs. Here is the YARA Attack Technique:

Name: Encrypt a large number of files
Description: Encrypt a large number of files on the endpoint to simulate ransomware
Platforms:
guidance:
- cmd> coldcryptor.exe run {{ extension }}
block:
- Suspicious process execution/behavior blocked by endpoint security tool

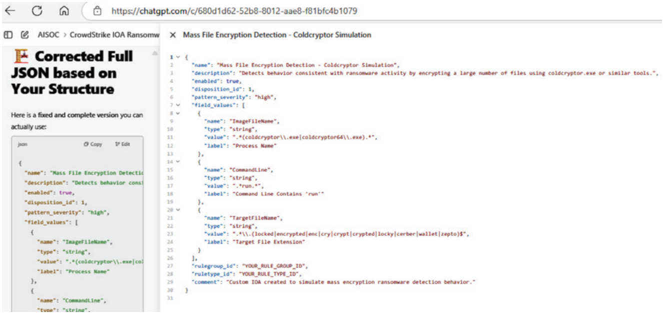
```
  detect:
  - Suspicious process execution/behavior detected by endpoint security tool
  - Detect common ransomware extensions using file system telemetry
  controls:
  - Endpoint Protection
  metadata:
  id: 72224b97-93d1-4087-8b82-6b4342bf2e09
  tid: T1486
  tactic: TA0040
  x_tools:
  - https://github.com/2XXE-SRA/payload_resources/tree/master/coldencryptor
  x_vectr_id: 72224b97-93d1-4087-8b82-6b4342bf2e09
  isv: 1
```

The diagram (Figure 2) shows the IOA rule output from our query, in JavaScript Object Notation (JSON) format, that can be imported to CrowdStrike manually or via an Application Program Interface (API). ChatGPT facilitated the work by working on the following tasks:

1. Translated the initial YARA rule from the Security Risk Advisory Index.
2. Created a template in JSON format that can be imported into the CrowdStrike Falcon platform manually or using APIs.
3. Formatted the rule detection logic around the process execution coldcryptor.exe run {{extension}} and file telemetry, including several encrypted extensions such as "*.locked", "*.encrypted", "*.enc", "*.cry", and other extensions.
4. Mapped the IOA to the MITRE ATT&CK technique T1486, which is important to help SMEs show compliance in terms of existing security solutions protecting against well-known threat attacks.

While AI solutions such as ChatGPT are powerful tools to facilitate cybersecurity analysis, AI still has several limitations that need improvement over time. These limitations may lead to negative results that cause delays in its adoption across different sectors, including the cybersecurity industry, and eventually may reduce the interest in investing time and resources in such technology.[15] That is why it is important to have human insights and intervention with the AI adoption to ensure that the IOA rules in JSON format generated by ChatGPT will be adopted by the intended vendor solution. The initial JSON rule that was produced was correct for CrowdStrike Falcon API pattern-based requirements; however, it did not match the expected format for uploading IOA rules based on full-field values to upload to the CrowdStrike Custom IOA Management. The IOA rule was fixed by adding the following details to the original ChatGPT query: "*Obtain the JSON file template that I can upload the IOA via CrowdStrike APIs.*"

The following Figure 2 shows the corrected and final version of the JSON rule that can now be imported to CrowdStrike.


https://chatgpt.com/c/680d1d62-52b8-8012-aae8-f81bfc4b1079
AISOC › CrowdStrike IOA Ransomw
Mass File Encryption Detection - Coldcryptor Simulation
Copy
Edit
json

Corrected Full JSON based on Your Structure

Here is a fixed and complete version you can actually use:

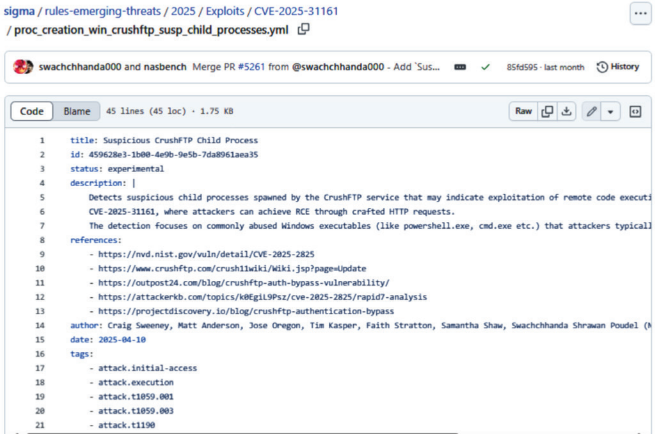
```
{
  "name": "Mass File Encryption Detection - Coldcryptor Simulation",
  "description": "Detects behavior consistent with ransomware activity by encrypting a large number of files using coldcryptor.exe or similar tools.",
  "enabled": true,
  "disposition_id": 1,
  "pattern_severity": "high",
  "field_values": [
    {
      "name": "ImageFileName",
      "type": "string",
      "value": ".*(coldcryptor\\.exe|coldcryptor64\\.exe).*",
      "label": "Process Name"
    },
    {
      "name": "CommandLine",
      "type": "string",
      "value": ".*run.*",
      "label": "Command Line Contains 'run'"
    },
    {
      "name": "TargetFileName",
      "type": "string",
      "value": ".*\\.(locked|encrypted|enc|cry|crypt|crypted|locky|cerber|wallet|zepto)$",
      "label": "Target File Extension"
    }
  ],
  "rulegroup_id": "YOUR_RULE_GROUP_ID",
  "ruletype_id": "YOUR_RULE_TYPE_ID",
  "comment": "Custom IOA created to simulate mass encryption ransomware detection behavior."
}
```

Figure 2: The final version of the IOA signature in JSON format, which can be imported into CrowdStrike. This signature is the output from ChatGPT that formatted the rule detection logic around the execution of the coldcryptor.exe process and file telemetry, including multiple ransomware extensions. This signature matches the expected format for uploading rules to the CrowdStrike Custom IOA Management feature. The complete output was included in Supplement Figure 2.

It is also critical to test any new IOA that is implemented on any EDR solution. Security analysts shall not implement the new IOA on production endpoints; first, test the rule on a representative sample of systems before the rule is applied to the rest of the organization, especially in production. While it may not disrupt operations, it may create unnecessary false positives that will consume time and resources from the Security Operations Center team receiving the false positive alerts.

Splunk Indicator of Attack – CrushFTP Exploit (CVE-2025-31161) – Example 2:

The following example shows the steps to create an IOA rule for the SIEM solution Splunk, based on the Sigma rule taken from the SigmaHQ repository hosted in the path: sigma/rules-emerging-threats/2025/Exploits/CVE-2025-31161/proc_creation_win_crushftp_susp_child_processes.yml.[16] Figure 3 shows the Sigma rule used to identify suspicious processes that may indicate the exploitation of the vulnerability CVE-2025-31161.


sigma / rules-emerging-threats / 2025 / Exploits / CVE-2025-31161
/ proc_creation_win_crushftp_susp_child_processes.yml
...
swachchhanda000 and nasbench Merge PR #5261 from @swachchhanda000 - Add `Sus...
85fd595 · last month
History
Code
Blame
45 lines (45 loc) · 1.75 KB
Raw

```
title: Suspicious CrushFTP Child Process
id: 459628e3-1b00-4e9b-9e5b-7da8961aea35
status: experimental
description: |
    Detects suspicious child processes spawned by the CrushFTP service that may indicate exploitation of remote code executi
    CVE-2025-31161, where attackers can achieve RCE through crafted HTTP requests.
    The detection focuses on commonly abused Windows executables (like powershell.exe, cmd.exe etc.) that attackers typicall
references:
    - https://nvd.nist.gov/vuln/detail/CVE-2025-2825
    - https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update
    - https://outpost24.com/blog/crushftp-auth-bypass-vulnerability/
    - https://attackerkb.com/topics/k0EgiL9Psz/cve-2025-2825/rapid7-analysis
    - https://projectdiscovery.io/blog/crushftp-authentication-bypass
author: Craig Sweeney, Matt Anderson, Jose Oregon, Tim Kasper, Faith Stratton, Samantha Shaw, Swachchhanda Shrawan Poudel (N
date: 2025-04-10
tags:
    - attack.initial-access
    - attack.execution
    - attack.t1059.001
    - attack.t1059.003
    - attack.t1190
```

Figure 3: The Sigma rule from SigmaHQ was used to create the IOA signature for Splunk. This rule detects suspicious processes spawned by the service CrushFTP, which may indicate a potential exploitation of the vulnerability CVE-2025-31161, which is a Remote Code Execution (RCE) attack. This RCE detection rule focuses on commonly abused Windows executables that attackers use to perform malicious commands.

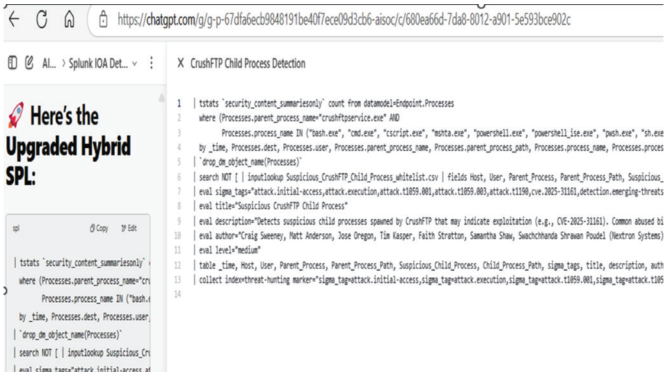
ChatGPT Query. The objective is to build a Splunk IOA rule that detects malicious activity from the Windows logs as a source of events, where the parent process is crushftpservice.exe and the child processes are some of the most commonly used by malicious actors, such as cmd.exe, powershell.exe, bash.exe, etc. The rest of the requirements to build the Splunk IOA signature are provided by the Sigma rule, which is the actual purpose of the Sigma rule. The text below is the full query provided to ChatGPT.

Build a Splunk Indicator of Attack (IOA) that detects suspicious child processes as part of an exploit. The generated IOA shall be in SPL (Splunk Processing Language). The IOA in SPL shall be based on the following Sigma rule.

```
title: Suspicious CrushFTP Child Process
id: 459628e3-1b00-4e9b-9e5b-7da8961aea35
status: experimental
description: |
Detects suspicious child processes spawned by the CrushFTP service that may indicate exploitation of remote code execution vulnerabilities, such as
CVE-2025-31161, where attackers can achieve RCE through crafted HTTP requests.
The detection focuses on commonly abused Windows executables (like PowerShell.exe, cmd.exe, etc.) that attackers typically use post-exploitation to execute malicious commands.
references:
- https://nvd.nist.gov/vuln/detail/CVE-2025-2825
- https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update
- https://outpost24.com/blog/crushftp-auth-bypass-vulnerability/
- https://attackerkb.com/topics/k0EgiL9Psz/cve-2025-2825/rapid7-analysis
- https://projectdiscovery.io/blog/crushftp-authentication-bypass
author: Craig Sweeney, Matt Anderson, Jose Oregon, Tim Kasper, Faith Stratton, Samantha Shaw, Swachchhanda Shrawan Poudel (Nextron Systems)
date: 2025-04-10
tags:
- attack.initial-access
- attack.execution
- attack.t1059.001
- attack.t1059.003
- attack.t1190
- CVE. 2025-31161
- detection.emerging-threats
logsource:
category: process_creation
product: Windows
detection:
selection_parent:
ParentImage|endswith: '\crushftpservice.exe'
selection_child:
Image|endswith:
- '\bash.exe'
- '\cmd.exe'
- '\cscript.exe'
- '\mshta.exe'
- '\powershell.exe'
- '\powershell_ise.exe'
- '\pwsh.exe'
- '\sh.exe'
- '\wscript.exe'
condition: all of selection_*
falsepositives:
- Legitimate CrushFTP administrative actions
- Software updates
level: medium
```

The following diagram (Figure 4) shows the IOA rule output from our AI query in Splunk Search Processing Language (SPL) format, which includes all the necessary search functions, commands, and arguments necessary to detect malicious activity from the security event sources.[17] ChatGPT facilitated the work by working on the following tasks:

1. Translated the initial Sigma rule from the Sigma HQ repository without the need to deploy Python on the local endpoint of the security analyst.
2. Created a template in SPL format that can be imported into the Splunk platform manually.
3. Improved SPL signature that combines speed of detection and metadata that easily maps the rule with the MITRE ATT&CK framework for Sigma compliance requirements.


https://chatgpt.com/g/g-p-67dfa6ecb9848191be40f7ece09d3cb6-aisoc/c/680ea66d-7da8-8012-a901-5e593bce902c
AI... › Splunk IOA Det... ⌄
🚀 Here's the Upgraded Hybrid SPL:
spl
Copy
Edit
X CrushFTP Child Process Detection

```
| tstats `security_content_summariesonly` count from datamodel=Endpoint.Processes
  where (Processes.parent_process_name="crushftpservice.exe" AND
        Processes.process_name IN ("bash.exe", "cmd.exe", "cscript.exe", "mshta.exe", "powershell.exe", "powershell_ise.exe", "pwsh.exe", "sh.exe
  by _time, Processes.dest, Processes.user, Processes.parent_process_name, Processes.parent_process_path, Processes.process_name, Processes.proces
| `drop_dm_object_name(Processes)`
| search NOT [ | inputlookup Suspicious_CrushFTP_Child_Process_whitelist.csv | fields Host, User, Parent_Process, Parent_Process_Path, Suspicious_
| eval sigma_tags="attack.initial-access,attack.execution,attack.t1059.001,attack.t1059.003,attack.t1190,cve.2025-31161,detection.emerging-threats
| eval title="Suspicious CrushFTP Child Process"
| eval description="Detects suspicious child processes spawned by CrushFTP that may indicate exploitation (e.g., CVE-2025-31161). Common abused bi
| eval author="Craig Sweeney, Matt Anderson, Jose Oregon, Tim Kasper, Faith Stratton, Samantha Shaw, Swachchhanda Shrawan Poudel (Nextron Systems)
| eval level="medium"
| table _time, Host, User, Parent_Process, Parent_Process_Path, Suspicious_Child_Process, Child_Process_Path, sigma_tags, title, description, auth
| collect index=threat-hunting marker="sigma_tag=attack.initial-access,sigma_tag=attack.execution,sigma_tag=attack.t1059.001,sigma_tag=attack.t105
```

Figure 4: The final version of the IOA signature in SPL format, which can be imported into Splunk. This signature is the output from ChatGPT that translated the initial Sigma rule and created a template in SPL with the necessary functions and arguments to detect Windows executables such as PowerShell.exe and cmd.exe. Attackers leverage these commonly abused executables to perform malicious commands to achieve an RCE attack based on crafted HTTP requests. The complete ChatGPT output was included in Supplement Figure 4.

It is recommended to compare different outputs of Sigma signatures translated into SPL rules to improve AI Machine Learning and obtain better SPL rules that will produce fewer false positives. For example, security analysts can use the script Sigma2SplunkAlert that converts multiple Sigma detection rules into a Splunk savedsearches.conf configuration to compare outputs.[18]

Conclusion

The majority of the SME organizations do not consider themselves as a target of malicious actors, due to their business profile and the fact that the majority of industry compromises have targeted big organizations. Also, some SMEs often neglect basic security controls such as logging and monitoring, and a strong Security Operations Center that detects attacks against their infrastructure and applications. This oversight allows malicious adversaries to exploit security issues affecting these companies without getting noticed due to a lack of proper security event detection. Malicious actors may take advantage of this situation as they see SMEs as an avenue to compromise bigger organizations that rely on SME as suppliers of services and *adhoc* Information Technology operations. In summary, SMEs are becoming an easy-to-compromise avenue or the weakest link to obtain unauthorized access to bigger enterprises, as SME already have some level of access to the asset components within the scope of the services provided.

In this research, a different approach to improve the detection of emerging threats was introduced. The predominant advantage of the proposed approach, besides being cost-effective, is to leverage publicly available Security Registries and Sigma Rules repositories to enrich the detection capabilities of the security solutions and SIEM systems already acquired by the SMEs. Via different examples, the author provided guidelines for SMEs to continue improving their detection capabilities of cybersecurity solutions such as EDR and SIEM.

Future research should focus on provisioning a GitHub subscription that serves as an IOA rules repository to receive feedback from users about attacks detection success in real SME scenarios.

Acknowledgments

I would like to thank Juang M. Keeton, MPH, for her insightful feedback provided throughout the writing process. Additionally, I want to thank my parents for their support and encouragement throughout the writing of this paper.

References

1. Laue, Tim; Klecker, Timo; Kleiner, Carsten; Detken, Kai-Oliver A SIEM Architecture for Advanced Anomaly Detection. *Open J. Big Data*. **2022**, *6*(1) https://doi.org/10.25968/opus-2321
2. CrowdStrike 2025 Global Threat Report https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0 (accessed March 1, 2025)
3. Fernandez de Arroyabe, J.C.; Arroyabe, M.F.; Fernandez, I.; Arranz, C.F. Cybersecurity resilience in SMEs. A machine learning approach. J. *Comput. Inf. Syst.* **2023** 1–17 https://doi.org/10.1080/08874417.2023.2248925
4. Fernandez de Arroyabe, J.C.; Fernandez de Arroyabe, Ignacio. The severity and effects of Cyber-breaches in SMEs: a machine learning approach, *Enterprise Information Systems*. **2021**, *17*(3) https://doi.org/10.1080/17517575.2021.1942997
5. Fernandez de Arroyabe, J.C.; Arroyabe, M.F.; Fernandez, I.; Arranz, C.F. Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*. **2024**, 141 https://doi.org/10.1016/j.cose.2024.103826
6. Companies using Oracle Cloud Infrastructure https://enlyft.com/tech/products/oracle-cloud-infrastructure (accessed April 10, 2025)
7. The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants (accessed April 10, 2025)
8. Bassey, Christian; Tonye Chinda, Ebenezer; Idowu, Samson. Building a Scalable Security Operations Center: A Focus on Open-source Tools. *J. Eng. Res. Rep.* **2024**, *26*, 196-209 https://doi.org/10.9734/jerr/2024/v26i71203
9. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed April 9, 2025)
10. Islam, Mohammad Anwarul. Application of Artificial Intelligence and Machine Learning in a Security Operations Center. *Issues in Information Systems*. **2023**, *24* (4), 311-327 https://doi.org/10.48009/4_iis_2023_124
11. Gartner Threat Detection Marketplace Reviews https://www.gartner.com/reviews/market/security-solutions-others/vendor/soc-prime/product/threat-detection-marketplace (Accessed April 11, 2025)
12. Sigma - Generic Signature Format for SIEM Systems https://github.com/SigmaHQ/sigma (accessed April 10, 2025)
13. M. Charfeddine, H. M. Kammoun, B. Hamdaoui, and M. Guizani, ChatGPT's Security Risks and Benefits: Offensive and Defensive Use-Cases, Mitigation Measures, and Future Implications, *IEEE Access*. **2024** *12*, 30263-30310 https://ieeexplore.ieee.org/document/10443401
14. Security Risk Advisors - Threat Simulation Indexes https://github.com/SecurityRiskAdvisors/indexes (Accessed April 11, 2025)
15. Alawamleh, Mohammad; Shammas, Natalie; Alawamleh, Kamal; Bani Ismail, Loiy. Examining the limitations of AI in business and the need for human insights using Interpretive Structural Modelling. *JOItmC*, **2024**, *11*(3), https://doi.org/10.1016/j.joitmc.2024.100338
16. Sigma: A generic rule format to express search queries on log data https://github.com/SigmaHQ/sigma (accessed April 11, 2025)
17. Splunk - About the search language https://docs.splunk.com/Documentation/Splunk/9.4.1/Search/Aboutthesearchlanguage (accessed April 12, 2025)
18. Sigma 2 Splunk Alert https://github.com/P4T12ICK/Sigma2SplunkAlert (Access April 13, 2025)

Supplement Information

Supplement Figure 2: Complete IOA rule output from ChatGPT, in JSON format for CrowdStrike.

```
{
"name": "Mass File Encryption Detection – Coldcryptor Simulation",
"description": "Detects behavior consistent with ransomware activity by encrypting a large number of files using coldcryptor.exe or similar tools.",
"enabled": true,
"disposition_id": 1,
"pattern_severity": "high",
"field_values": [
{
"name": "ImageFileName",
  "type": "string",
  "value": ".*(coldcryptor\\.exe|coldcryptor64\\.exe).*",
  "label": "Process Name"
  },
  {
  "name": "CommandLine",
  "type": "string",
  "value": ".*run.*",
  "label": "Command Line Contains 'run'"
  },
  {
  "name": "TargetFileName",
  "type": "string",
  "value": ".*\\.(locked|encrypted|enc|cry|crypt|crypted|locky|cerber|wallet|zepto)$",
  "label": "Target File Extension"
  }
  ],
  "rulegroup_id": "YOUR_RULE_GROUP_ID",
  "ruletype_id": "YOUR_RULE_TYPE_ID",
  "comment": "Custom IOA created to simulate mass encryption ransomware detection behavior."
  }
```

Supplement Figure 4. Complete IOA rule output from ChatGPT, in SPL format for Splunk.

```
  | tstats `security_content_summariesonly` count from datamodel=Endpoint.Processes
  where (Processes.parent_process_name="crushftpservice.exe" AND
  Processes.process_name IN ("bash.exe", "cmd.exe", "cscript.exe", "mshta.exe",
  "powershell.exe", "powershell_ise.exe", "pwsh.exe", "sh.exe", "wscript.exe"))
  By _time, Processes.dest, Processes.user, Processes.parent_process_name, Processes.parent_process_path, Processes.process_name, Processes.process_path
  | `drop_dm_object_name(Processes)`
  | search NOT [ | inputlookup Suspicious_CrushFTP_Child_Process_whitelist.csv | fields Host, User, Parent_Process, Parent_Process_Path, Suspicious_Child_Process, Child_Process_Path ]
  | eval sigma_tags=" attack. Initial access, attack.execution, attack.t1059.001, attack.t1059.003, attack.t1190,cve. 2025-31161, detection.emerging-threats"
  | eval title="Suspicious CrushFTP Child Process"
  | eval description="Detects suspicious child processes spawned by CrushFTP that may indicate exploitation (e.g., CVE-2025-31161). Common abused binaries like powershell.exe, cmd.exe, etc."
  | eval author=" Craig Sweeney, Matt Anderson, Jose Oregon, Tim Kasper, Faith Stratton, Samantha Shaw, Swachchhanda Shrawan Poudel (Nextron Systems)"
  | eval level="medium"
  | table _time, Host, User, Parent_Process, Parent_Process_Path, Suspicious_Child_Process, Child_Process_Path, sigma_tags, title, description, author, level
  | collect index=threat-hunting marker="sigma_tag=attack.initial-access,sigma_tag=attack.execution,sigma_tag=attack.t1059.001,sigma_tag=attack.t1059.003,sigma_tag=attack.t1190,sigma_tag=cve.2025-31161,sigma_tag=detection.emerging-threats"
```

Authors

Alfredo Lopez-Salas is a junior at Round Rock High School. He has undertaken research as a student who aspires to study how Artificial Intelligence is changing the cybersecurity threat landscape. He enjoys Taekwondo, playing piano, and is the founder of the non-profit organization, Latino Athletes USA.