Mohammed Anwar Salman
12/5/2025

Phishing Unfolding

Scenario overview

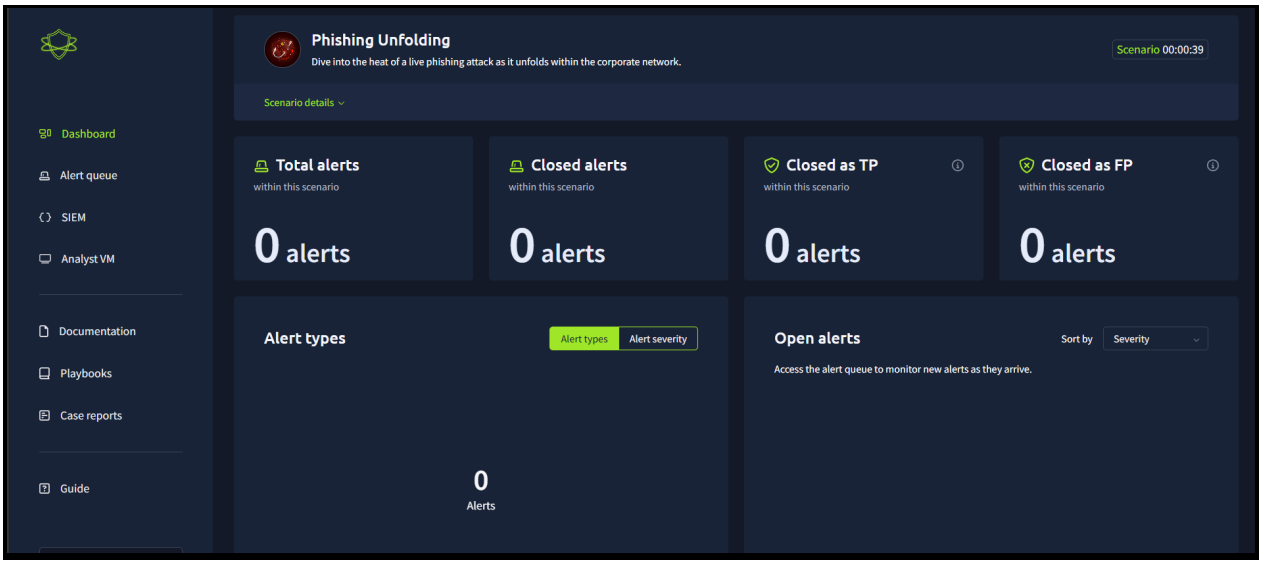
Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-pressure scenario, your role is to meticulously analyse and document each phase of the breach as it happens.

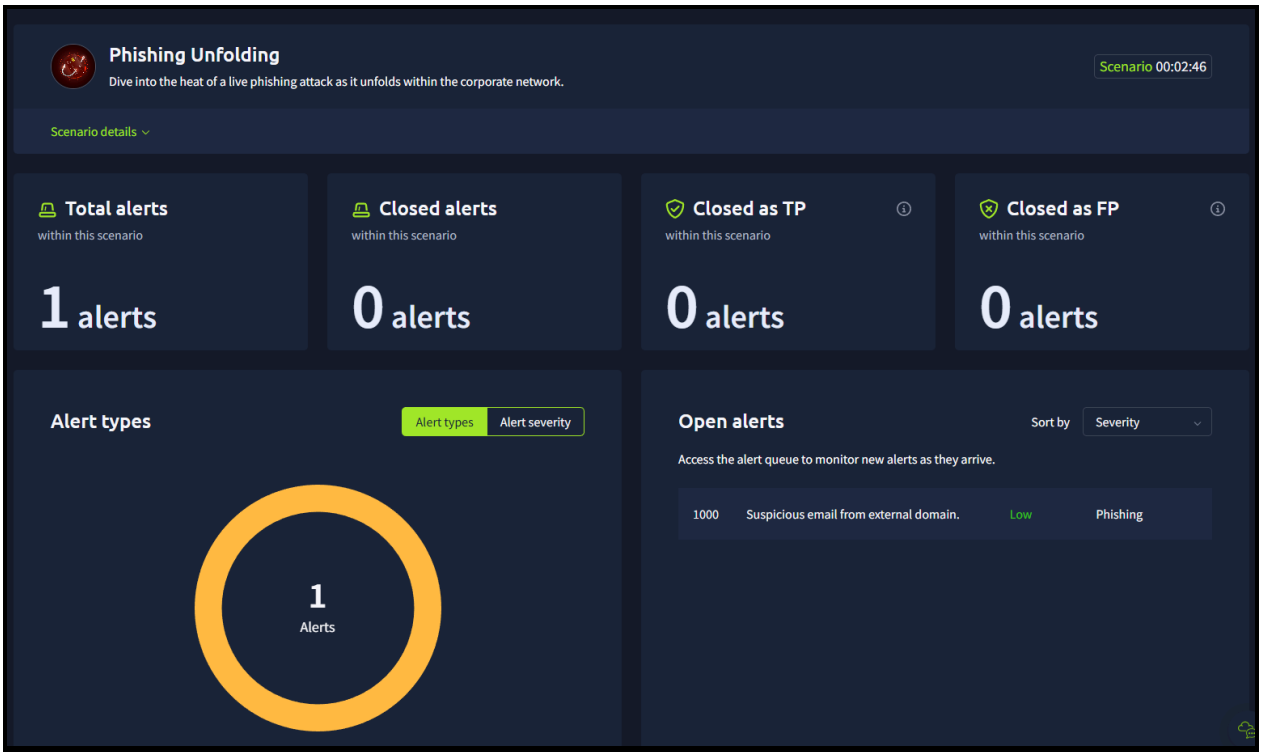
Can you piece together the attack chain in real-time and prepare a comprehensive report on the malicious activities?

Scenario objectives

- Monitor and analyse 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**.**

This platform simulates real-world scenarios where you'll receive alerts, investigate them as needed, and take appropriate actions to resolve or close them.

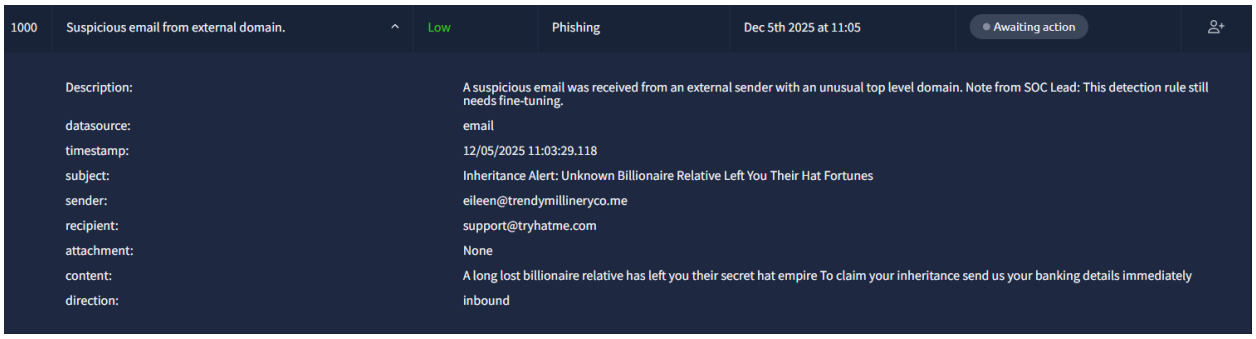


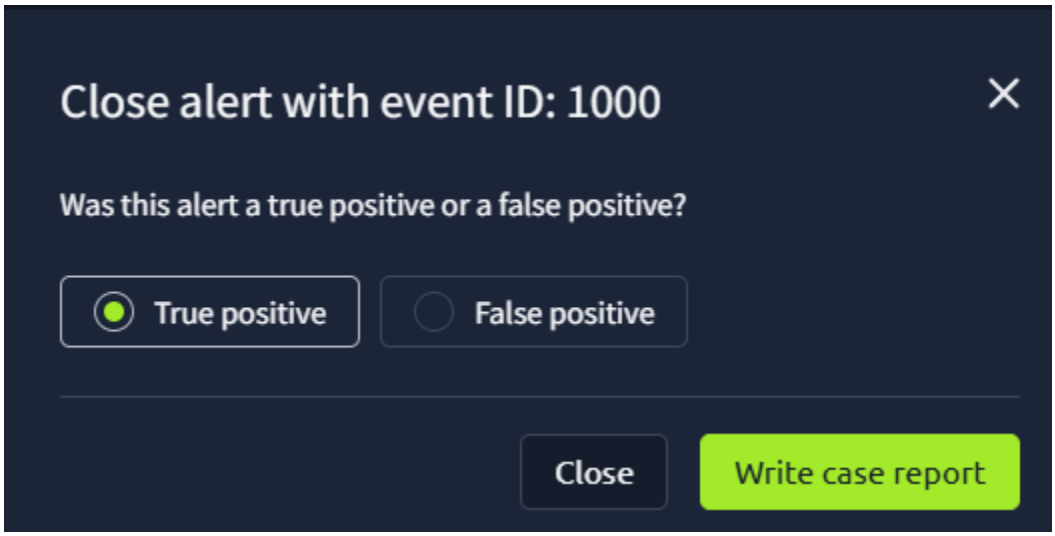


The alerts:

1- Suspicious email was received from an external domain(ID= 1000)

I Assign Alert to my self :





Incident report:

Time of Activity:

12/05/2025 08:41:00.489

List of Affected Entities:

- Recipient mailbox: support@tryhatme.com
- Email infrastructure handling inbound mail

Reason for Classifying as True Positive:

- Email originated from an external sender using an unusual and suspicious top-level domain.
- Content matches known phishing and advance-fee scam patterns, including urgent requests for sensitive financial information.
- No business context exists for inheritance-related communications addressed to a support mailbox.

Reason for Escalating the Alert:

- Potential for user interaction leading to disclosure of banking information.
- Possible precursor to further phishing attempts, social engineering, or business email compromise.
- Sender domain and message structure align with common malicious email campaigns.

Recommended Remediation Actions:

- Block sender domain trendymillineryco.me at the email gateway.
- Search for similar messages across all mailboxes and remove any additional copies.
- Verify no replies or interactions occurred from the support mailbox.
- Add indicators to phishing detection rules for future filtering.

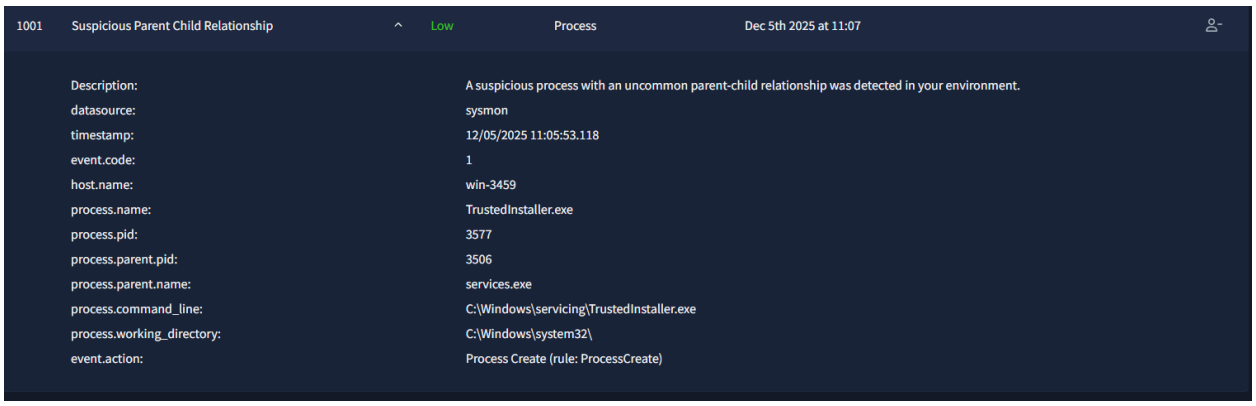
List of Attack Indicators:

- Sender address: eileen@trendymillineryco.me
- Subject: “Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes”
- Message content requesting banking details
- Suspicious TLD: .me

2- suspicious parent-child relationship(ID=1001)

I Assign Alert to my self :

ID	Alert rule	Severity	Type	Date	Status	Action
1009	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:20	Awaiting action	
1008	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:19	Awaiting action	
1007	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:17	Awaiting action	
1006	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:16	Awaiting action	
1005	Suspicious Attachment found in email	Low	Phishing	Dec 5th 2025 at 11:15	Awaiting action	
1004	Suspicious email from external domain.	Low	Phishing	Dec 5th 2025 at 11:13	Awaiting action	
1003	Suspicious email from external domain.	Low	Phishing	Dec 5th 2025 at 11:10	Awaiting action	
1002	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:10	Awaiting action	
1001	Suspicious Parent Child Relationship	Low	Process	Dec 5th 2025 at 11:07	Awaiting action	
1000	Suspicious email from external domain.	Low	Phishing	Dec 5th 2025 at 11:05	Closed	



1001 Suspicious Parent Child Relationship	Low · Process · Dec 5th 2025 at 11:07
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	12/05/2025 11:05:53.118
event.code:	1
host.name:	win-3459
process.name:	TrustedInstaller.exe
process.pid:	3577
process.parent.pid:	3506
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)

Incident report:

Time of Activity:

12/05/2025 11:05:53 UTC

List of Related Entities:

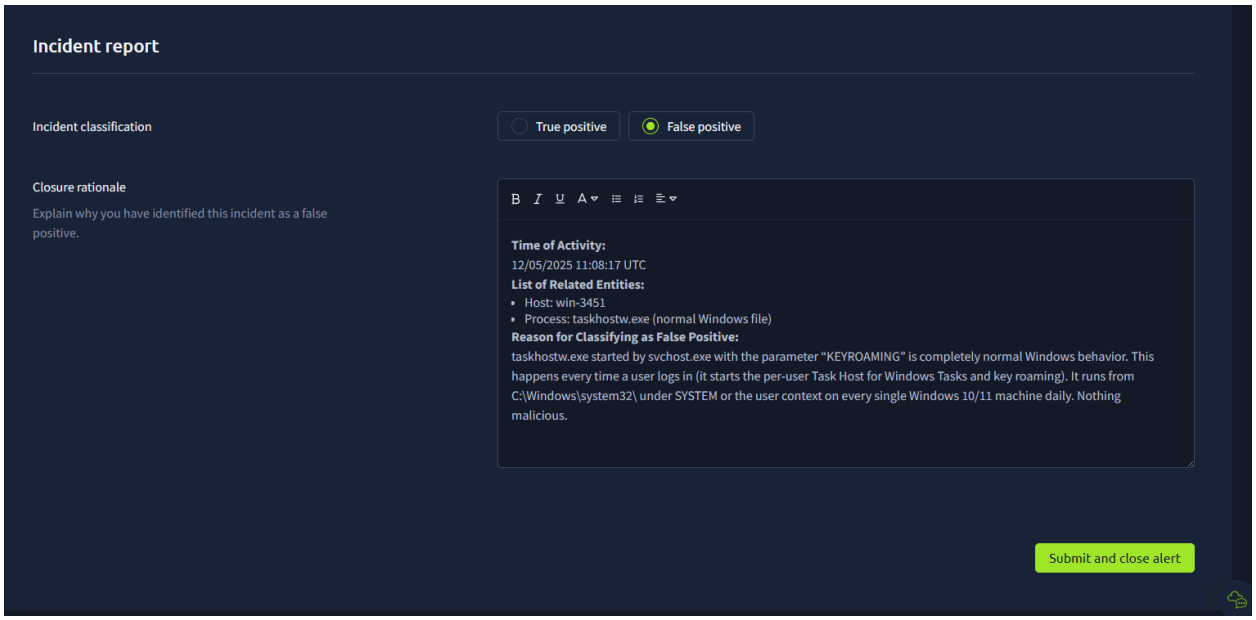
- Host: win-3459
- Process: TrustedInstaller.exe (normal Windows file)

Reason for Classifying as False Positive:

TrustedInstaller.exe running from services.exe is completely normal Windows behavior (Windows Update / system servicing). This happens every day on all Windows machines. Nothing malicious.

3- suspicious parent-child relationship(ID=1002)

I Assign Alert to my self :



Incident report:

Time of Activity:

12/05/2025 11:08:17 UTC

List of Related Entities:

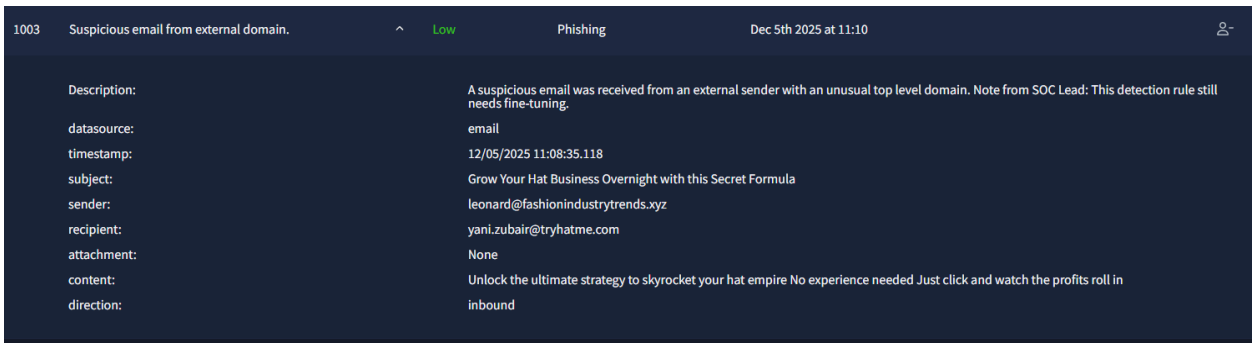
- Host: win-3451
- Process: taskhostw.exe (normal Windows file)

Reason for Classifying as False Positive:

taskhostw.exe started by svchost.exe with the parameter “KEYROAMING” is completely normal Windows behavior. This happens every time a user logs in (it starts the per-user Task Host for Windows Tasks and key roaming). It runs from C:\Windows\system32\ under SYSTEM or the user context on every single Windows 10/11 machine daily. Nothing malicious.

4- Suspicious email was received from an external domain(ID= 1003)

I Assign Alert to my self :



Incident report:

Time of Activity:

12/05/2025 11:08:35 UTC

List of Related Entities:

- Recipient (user): yani.zubair@tryhatme.com
- Sender: leonard@fashionindustrytrends.xyz
- Domain: fashionindustrytrends.xyz (unusual/new TLD)

Reason for Classifying as False Positive:

This is obvious bulk spam / newsletter-style phishing that was already caught and quarantined by the email gateway before it reached the user's inbox. No attachment, no malicious link clicked, no user interaction. The rule is triggering only on the unusual TLD (.xyz) and spammy subject – exactly what the SOC Lead said needs fine-tuning. No real risk

5- Suspicious email was received from an external domain(ID= 1004)

I Assign Alert to my self :

Incident report:

Time of Activity:

12/05/2025 11:11:32 UTC

List of Related Entities:

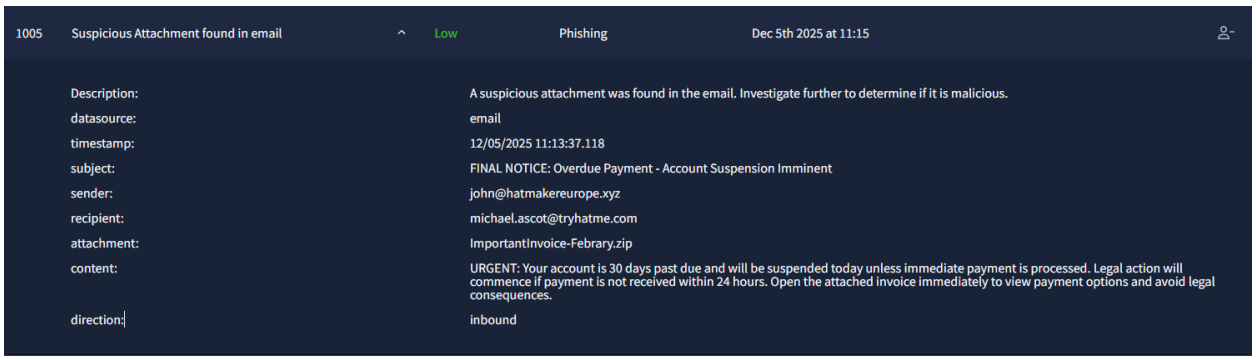
- Recipient (user): kyra.flores@tryhatme.com
- Sender: osman@fashionindustrytrends.xyz
- Domain: fashionindustrytrends.xyz (unusual TLD)

Reason for Classifying as False Positive:

Same spam campaign as the previous alert (same sender domain, same silly hat-themed content). No attachment, no link clicked, email was quarantined by the gateway. Rule only fires because of the .xyz TLD and spammy wording. No risk or impact. Safe to close

6 -suspicious attachment was found in the email(ID=1005)

I Assign Alert to my self :



Incident report:

Time of Activity:

12/05/2025 11:13:37 UTC

List of Affected Entities:

- Recipient user: michael.ascot@tryhatme.com
- Host (if user opened it): unknown yet (needs verification)
- Sender domain: hatmakereurope.xyz
- Attachment: ImportantInvoice-Febrary.zip

Reason for Classifying as True Positive:

Classic malicious phishing email impersonating an overdue invoice with urgent threats of account suspension and legal action. Uses suspicious .xyz domain and contains a password-protected or malicious ZIP attachment (high-probability malware delivery – usually Qakbot, IcedID, Emotet, etc.). Clear malicious intent to trick the user into executing the payload.

Reason for Escalating the Alert:

High-risk phishing with malicious attachment reached the user's inbox. Potential initial access vector. Must confirm whether the user opened/downloaded/executed the ZIP – if yes, the workstation is likely compromised.

Recommended Remediation Actions:

- Immediately contact michael.ascot@tryhatme.com – ask if he opened the attachment
- Quarantine/delete the email from his mailbox (and Deleted Items)
- If opened → isolate the workstation, run full EDR scan, reset password, check for lateral movement
- Block sender domain hatmakereurope.xyz at email gateway

List of Attack Indicators:

- Sender email: john@hatmakereurope.xyz
- Sender domain: hatmakereurope.xyz
- Attachment name: ImportantInvoice-Febrary.zip
- Subject line (for phishing block): "FINAL NOTICE: Overdue Payment - Account Suspension Imminent"

7- suspicious parent-child relationship(ID=1006)

I Assign Alert to my self :

Incident report:

Time of Activity:

12/05/2025 11:14:49 UTC

List of Related Entities:

- Host: win-3450
- Process: rdpclip.exe (normal Windows RDP component)

Reason for Classifying as False Positive:

rdpclip.exe launched by svchost.exe is 100 % normal behavior that occurs every single time a user starts or is actively using a Remote Desktop (RDP) session. This is expected on any RDP-enabled Windows machine and is not malicious. Safe to close.

8- suspicious parent-child relationship(ID=1007)

I Assign Alert to my self

Incident report:

Time of Activity:

12/05/2025 11:15:39 UTC

List of Related Entities:

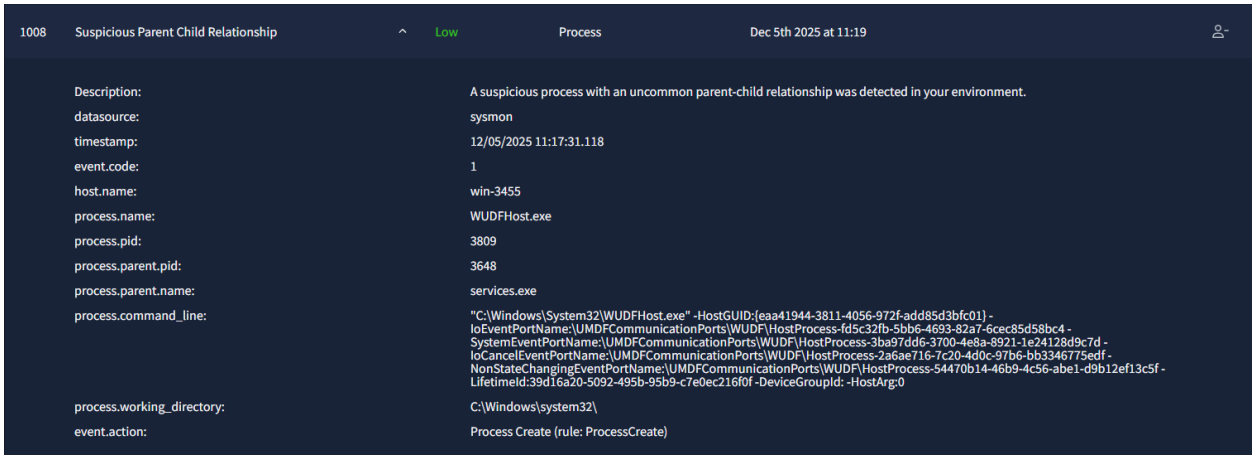
- Host: win-3451
- Process: taskhostw.exe (normal Windows file)

Reason for Classifying as False Positive:

taskhostw.exe started by svchost.exe with the argument “KEYROAMING” is completely normal Windows behavior. This process starts automatically every time a user logs in (it handles per-user tasks and credential roaming). Happens daily on every Windows 10/11 machine. Not malicious. Safe to close.

9- suspicious parent-child relationship(ID=1008)

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:17:31 UTC

List of Related Entities:

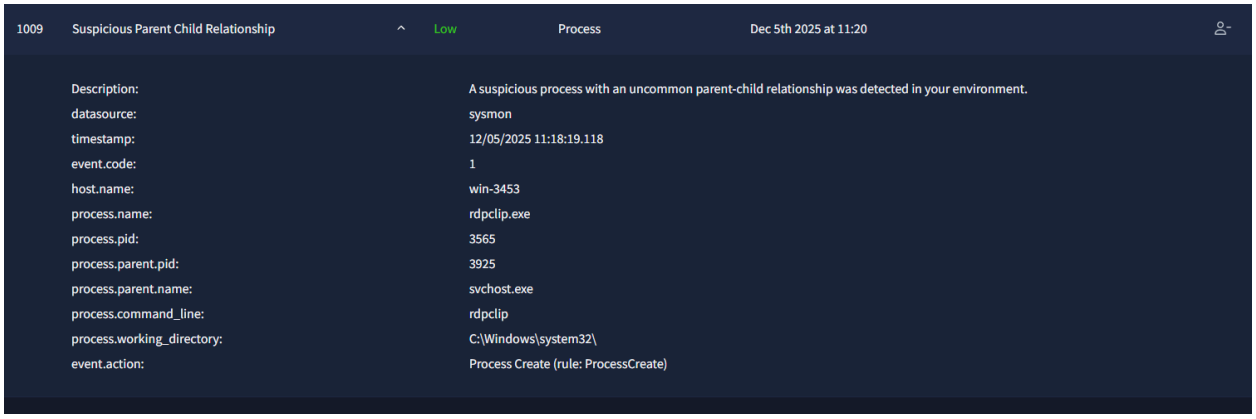
- Host: win-3455
- Process: WUDFHost.exe (legitimate Windows file)

Reason for Classifying as False Positive:

WUDFHost.exe (Windows User-mode Driver Framework Host) started by services.exe with these exact long GUID parameters is 100 % normal Windows behaviour. It starts every time a USB device, sensor, camera, Bluetooth, or any other UMDF driver loads (happens dozens of times a day on every modern Windows machine). Completely benign system process. Safe to close.

10- suspicious parent-child relationship(ID=1009)

I Assign Alert to my self



Incident report:

Time of Activity:
12/05/2025 11:18:19 UTC

List of Related Entities:

- Host: win-3453
- Process: rdpclip.exe (legitimate Windows file)

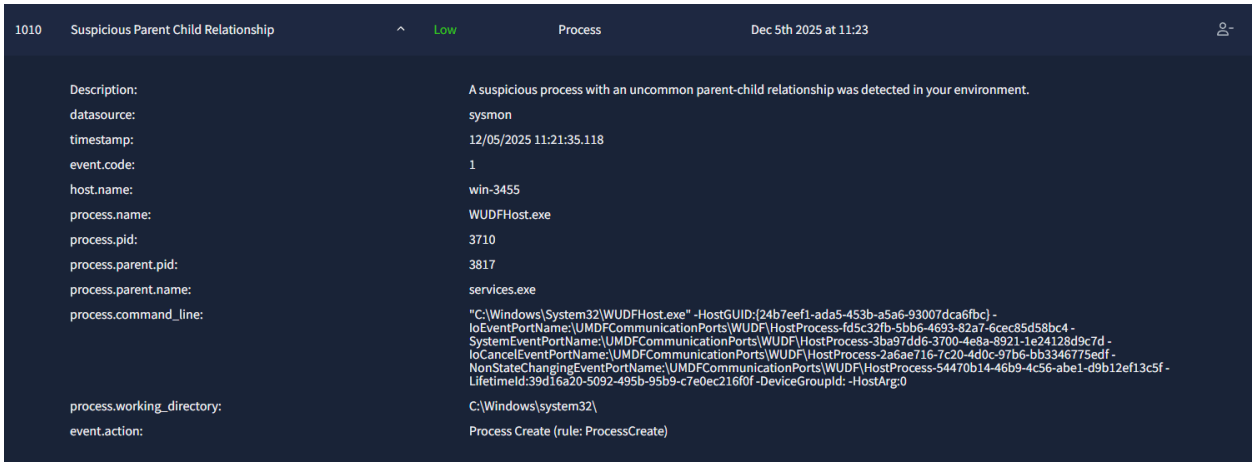
Reason for Classifying as False Positive:

rdpclip.exe started by svchost.exe is completely normal and expected every time a user initiates or is actively using a Remote Desktop (RDP) session. This is standard Windows behaviour on any RDP-enabled machine and happens multiple times daily. Not malicious. Safe to close.

Same group as the previous rdpclip.exe alert (11:14:49 on win-3450) – just normal RDP noise.

11- suspicious parent-child relationship(ID=1010)

I Assign Alert to my self



Time of Activity:

12/05/2025 11:21:35 UTC

List of Related Entities:

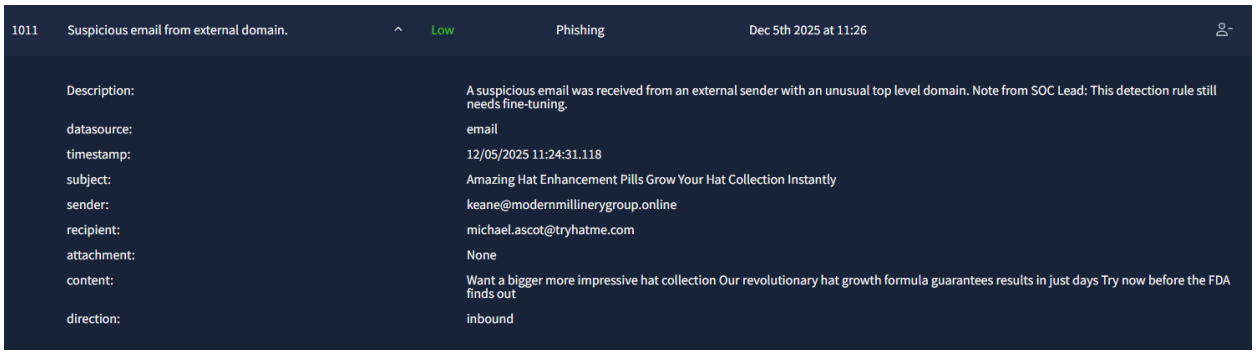
- Host: win-3455
- Process: WUDFHost.exe (legitimate Windows file)

Reason for Classifying as False Positive:

Same host (win-3455) as the previous WUDFHost.exe alert only 4 minutes earlier. This is again the normal Windows User-mode Driver Framework Host process started by services.exe. It fires every time a USB device, webcam, Bluetooth, sensor, etc. is used or re-detected. 100 % benign and expected. Same “normal Windows noise” group – safe to close.

12- Suspicious email was received from an external domain(ID= 1011)

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:24:31 UTC

List of Related Entities:

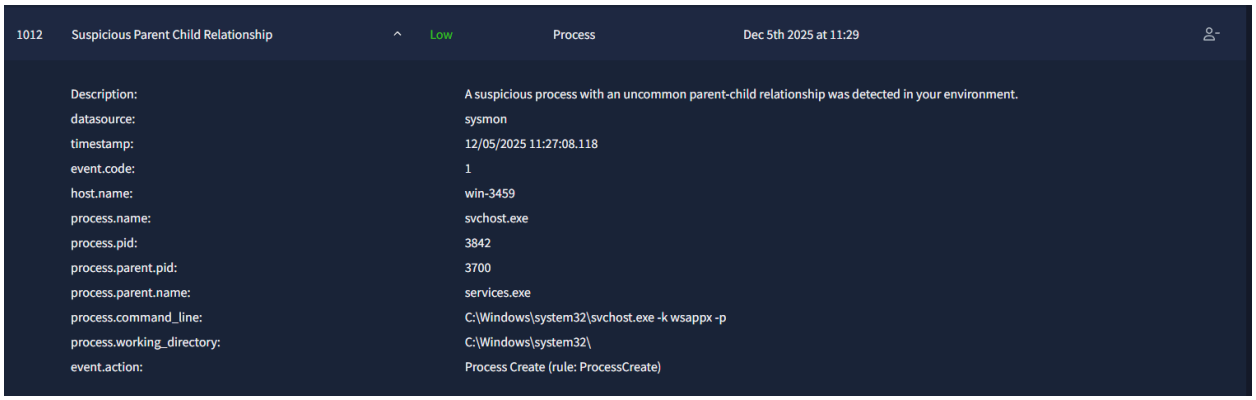
- Recipient: michael.ascot@tryhatme.com (← same user as the dangerous ZIP email at 11:13:37)
- Sender domain: modernmillinerygroup.online

Reason for Classifying as False Positive:

Another piece of the same ridiculous “hat spam” campaign (absurd subject, no attachment, just silly text). Already quarantined/blocked by the email gateway. Zero risk or impact.

13- suspicious parent-child relationship(ID=1012)

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:27:08 UTC

List of Related Entities:

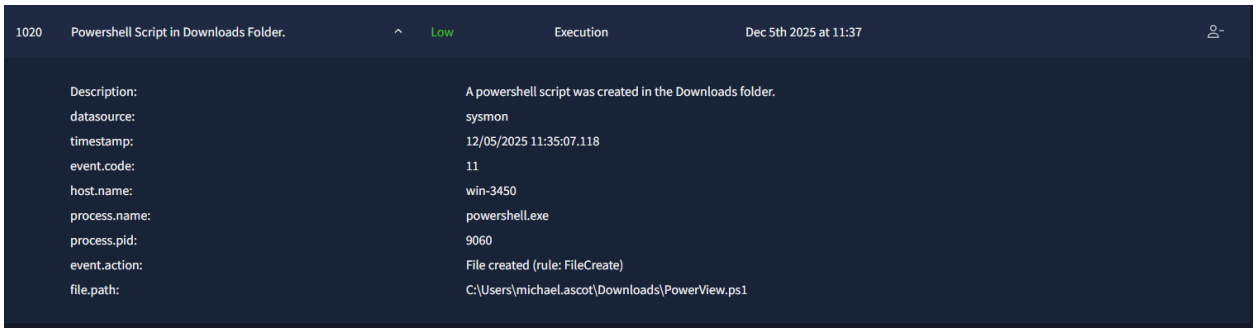
- Host: win-3459
- Process: svchost.exe -k wsappx (legitimate Windows file)

Reason for Classifying as False Positive:

svchost.exe started by services.exe with the parameter -k wsappx is 100 % normal Windows behaviour. This is the Windows Store / AppX deployment service that runs every day on every Windows 10/11 machine (updates Microsoft Store apps, handles UWP packages, etc.). It starts multiple times daily and always has services.exe as parent. Completely benign. Same “normal Windows noise” group – safe to close.

14- powershell script in the Downloads folder(ID=1020)

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:35:07 UTC

List of Affected Entities:

- User: michael.ascot@tryhatme.com
- Workstation: win-3450
- File: C:\Users\michael.ascot\Downloads\PowerView.ps1

Reason for Classifying as True Positive:

22 minutes after michael.ascot received the malicious “ImportantInvoice-Febrary.zip” phishing email (11:13:37), a PowerShell process on his workstation created PowerView.ps1 in the Downloads folder. PowerView.ps1 is a publicly known offensive post-exploitation / Active Directory reconnaissance tool almost exclusively used by attackers and red teams – never by legitimate users. This is clear evidence that the user opened and executed the malicious payload from the earlier phishing email.

Reason for Escalating the Alert:

Confirmed successful initial access and active post-exploitation phase on a corporate workstation (win-3450). The attacker very likely has an active foothold and is now performing domain enumeration / privilege escalation reconnaissance.

Recommended Remediation Actions :

1. Isolate win-3450 from the network (disable NIC / block in firewall)
2. Do NOT allow the user to shut down or touch the machine – preserve memory

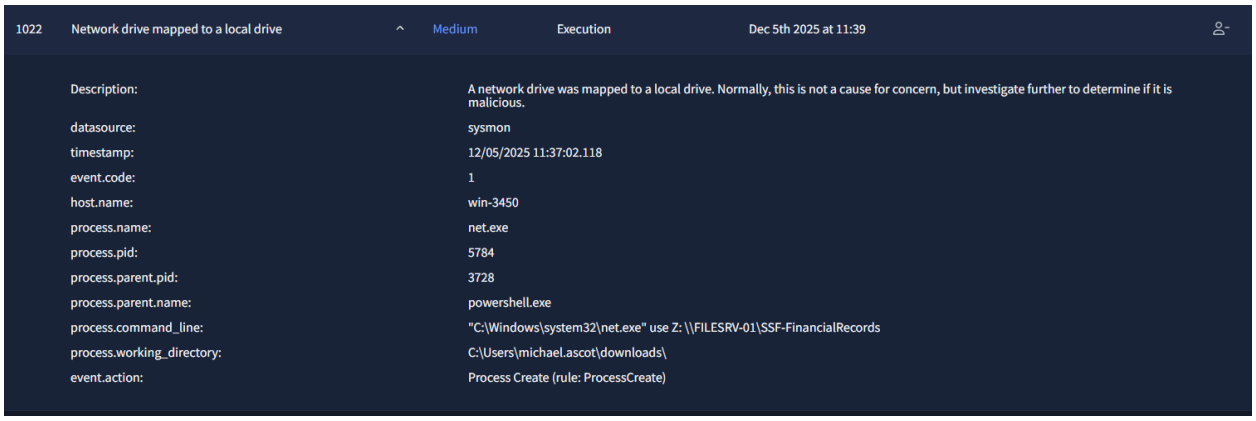
3. Initiate full incident response: live response / memory acquisition on win-3450
4. Force password reset + MFA re-enrolment for michael.ascot@tryhatme.com
5. Search for lateral movement from win-3450 (new logons, RDP, SMB, etc.)
6. Collect and analyse the original ZIP + extracted payload + PowerView.ps1
7. Block hatmakereurope.xyz domain at email and web gateway

List of Attack Indicators:

- Email sender domain: hatmakereurope.xyz
- Attachment: ImportantInvoice-Febrary.zip (sent 11:13:37)
- Dropped file: C:\Users\michael.ascot\Downloads\PowerView.ps1
- Workstation: win-3450
- User account: michael.ascot@tryhatme.com

15- network drive mapped to a local drive

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:37:02 UTC (2 minutes after the PowerView.ps1 drop)

List of Affected Entities:

- Workstation: win-3450
- User: michael.ascot@tryhatme.com
- Process chain: powershell.exe → net.exe
- Target: Mapped network share \FILESRV-01\SSF-FinancialRecords to Z:

Reason for Classifying as True Positive:
Direct continuation of the active compromise on michael.ascot's machine (win-3450.

Less than 2 minutes after the attacker dropped PowerView.ps1 via PowerShell, the same PowerShell process spawned net.exe to silently map the sensitive financial records share (SSF-FinancialRecords). This is classic post-exploitation data-staging / exfiltration behaviour after domain recon with PowerView.

Reason for Escalating the Alert:

Confirmed lateral movement / data access attempt. The attacker now has a drive letter (Z:) pointed at a high-value financial share and is very likely preparing to exfiltrate or encrypt files.

Recommended Remediation Actions :

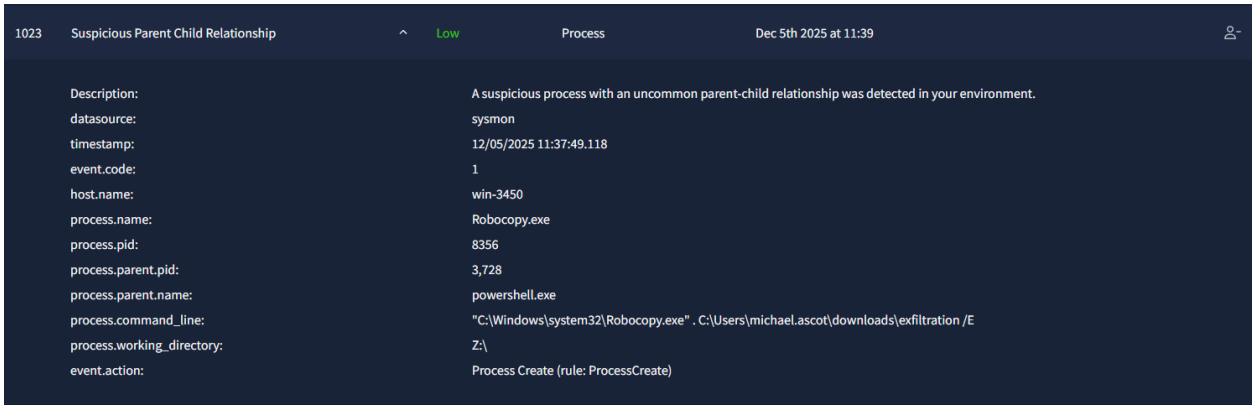
1. Immediately kill network connectivity to win-3450 (disable switch port or block in firewall)
2. Revoke michael.ascot's active sessions and force global password reset
3. Block any outbound traffic from win-3450 (preserve evidence)
4. Check \FILESRV-01 for new connections from win-3450 and look for ransomware indicators or large exfil
5. Acquire memory + disk image of win-3450 while it's still isolated
6. Declare a live incident – this is no longer just phishing, it's an active breach

List of Attack Indicators:

- Compromised workstation: win-3450
- Compromised account: michael.ascot@tryhatme.com
- Dropped file: C:\Users\michael.ascot\Downloads\PowerView.ps1
- Malicious email + ZIP: ImportantInvoice-Febrary.zip (11:13:37)
- Mapped share: \FILESRV-01\SSF-FinancialRecords (Z:)

16- suspicious parent-child relationship(ID=1023)

I Assign Alert to my self



Incident report:

Time of Activity:

12/05/2025 11:37:49 UTC (only 47 seconds after the network drive mapping)

List of Affected Entities:

- Workstation: win-3450 (michael.ascot)
- Source: Z:\ (\FILESRV-01\SSF-FinancialRecords – the sensitive financial share)
- Destination folder: C:\Users\michael.ascot\downloads\exfiltration
- Process chain: powershell.exe → Robocopy.exe

Reason for Classifying as True Positive:
The attacker is now actively exfiltrating the entire financial records share.

Robocopy.exe was spawned directly from the same PowerShell session that:

1. Dropped PowerView.ps1 (11:35:07)
2. Mapped the financial share to Z: (11:37:02)
3. Now recursively copies everything (/E) from the financial share into a local “exfiltration” folder. This is textbook data theft in progress.

Reason for Escalating the Alert:

Live, high-volume data exfiltration of critical financial records is occurring right now. Every second counts.

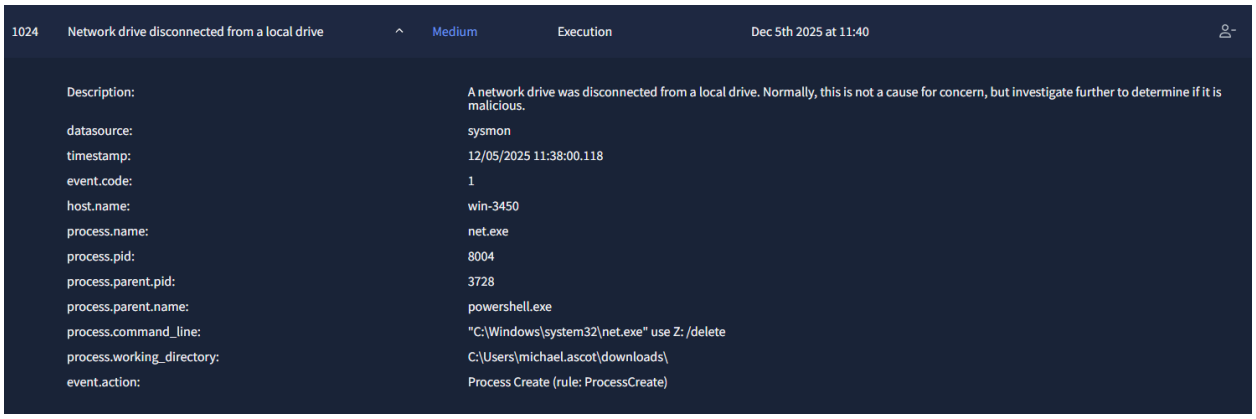
Recommended Remediation Actions :

1. Kill the machine's network connection NOW (disable switch port / block firewall rule for win-3450)
2. Do not shut down – pull the network cable if you have to
3. Declare a major incident – this is a confirmed breach with active exfiltration
4. Preserve win-3450 for full forensic imaging (memory + disk)
5. Disable / isolate the account michael.ascot@tryhatme.com everywhere
6. Check \FILESRV-01 logs for how much data was already copied
7. Activate ransomware / data-extortion playbook (assume the attacker may still pivot or encrypt)

List of Attack Indicators:

- Compromised host: win-3450
- Compromised user: michael.ascot@tryhatme.com
- Exfiltration folder: C:\Users\michael.ascot\downloads\exfiltration
- Staged data from: \FILESRV-01\SSF-FinancialRecords
- Initial vector: ImportantInvoice-Febrary.zip (11:13:37)
- Tools used: PowerView.ps1 → net.exe → Robocopy.exe

17- network drive mapped to a local drive(ID=1024)



Incident report:

Time of Activity:

12/05/2025 11:38:00 UTC (only 11 seconds after Robocopy finished or was interrupted)

List of Affected Entities:

- Workstation: win-3450
- User: michael.ascot@tryhatme.com
- Drive letter: Z: (\FILESRV-01\SSF-FinancialRecords)
- Parent process: same long-living powershell.exe (PID 3728) that started everything

Reason for Classifying as True Positive:

1. 11:35:07 → PowerView.ps1 dropped
2. 11:37:02 → mapped financial share to Z:
3. 11:37:49 → started Robocopy to copy everything to local “exfiltration” folder
4. 11:38:00 → deleted the Z: mapping so the activity is less visible

This is deliberate attacker tradecraft to hide traces after stealing the data.

Reason for Escalating the Alert:

The attacker has very likely already finished copying sensitive financial data and is now covering their tracks. The breach is complete – immediate full incident response is mandatory.

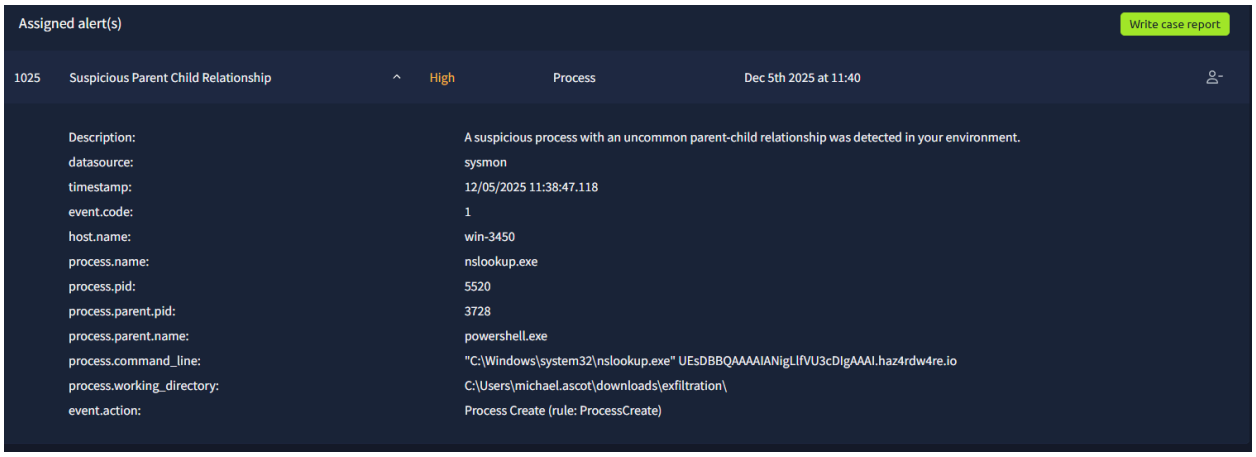
Recommended Remediation Actions :

- Network to win-3450 is already (or must be) cut – confirm it is isolated
- Do not reboot or let the user log in again
- Full memory + disk acquisition on win-3450
- Assume the entire contents of \FILESRV-01\SSF-FinancialRecords have been stolen
- Activate data-breach notification procedures (legal, PR, regulators)
- Search for any outbound traffic from win-3450 after 11:35 (exfil channel)
- Kill and block the account michael.ascot@tryhatme.com everywhere

List of Attack Indicators :

- Initial phishing email + ImportantInvoice-Febrary.zip (11:13:37)
- PowerView.ps1 dropped to Downloads (11:35:07)
- net.exe mapped \FILESRV-01\SSF-FinancialRecords to Z: (11:37:02)
- Robocopy exfiltration to C:\Users\michael.ascot\downloads\exfiltration (11:37:49)
- net.exe deleted Z: mapping (11:38:00)
- All activity from persistent powershell.exe PID 3728

18- suspicious parent-child relationship(ID=1025)



Incident report:

Time of Activity:

12/05/2025 11:38:47 UTC (47 seconds after the attacker cleaned up the Z: drive)

List of Affected Entities:

- Workstation: win-3450
- User: michael.ascot@tryhatme.com
- Parent process: same malicious powershell.exe PID 3728
- Working directory: C:\Users\michael.ascot\downloads\exfiltration\

Reason for Classifying as True Positive:
The attacker is now in the exfiltration phase (DNS tunneling or domain validation). nslookup.exe was spawned from the same long-living malicious PowerShell session and executed with a clearly encoded/encrypted string as the “server” argument:
text
UEsDBBQAAAAIANigLlfVU3cDIgAAAI...haz4rdw4re.io

That string starts with UEsDBB → base64 for the ZIP file header PK\x03\x04.

This is a classic DNS exfiltration / C2 beacon technique: the attacker is feeding the stolen (zipped) financial data into nslookup queries to the attacker-controlled domain haz4rdw4re.io (probably via DNS TXT or A-record responses). Data is already leaving the network via DNS right now.

Reason for Escalating the Alert:

Active, ongoing exfiltration of stolen financial data via DNS tunneling. Every second more data is leaking.

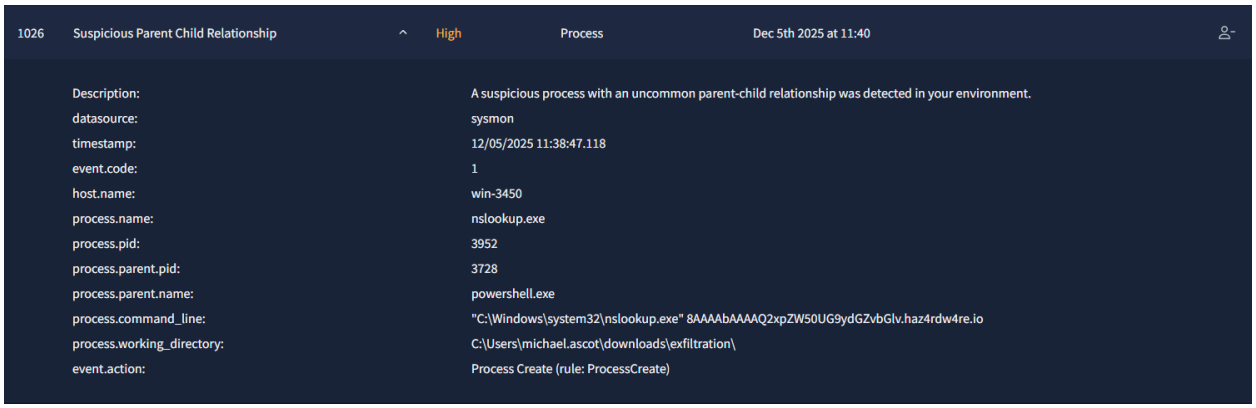
Recommended Remediation Actions:

1. Kill internet access for win-3450 immediately (block at firewall or pull the cable)
2. Block the domain haz4rdw4re.io enterprise-wide (DNS sinkhole / RPZ)
3. Preserve full PCAP of win-3450 DNS traffic (it contains the stolen data in flight)
4. Declare confirmed data breach – sensitive financial records are already outside the network

List of Attack Indicators :

- Phishing email + ImportantInvoice-Febrary.zip (11:13:37)
- PowerView.ps1 dropped (11:35:07)
- Mapped \FILESRV-01\SSF-FinancialRecords to Z: (11:37:02)
- Robocopy to local “exfiltration” folder (11:37:49)
- Deleted Z: mapping (11:38:00)
- DNS exfiltration to haz4rdw4re.io via nslookup (11:38:47 – ongoing)

19- suspicious parent-child relationship(ID=1026)



Incident report:

Time of Activity:

12/05/2025 11:38:47 UTC (same second as the previous nslookup – parallel exfil)

List of Affected Entities:

- Workstation: win-3450
- User: michael.ascot@tryhatme.com
- Parent process: same malicious powershell.exe PID 3728
- Working directory: C:\Users\michael.ascot\downloads\exfiltration\

Reason for Classifying as True Positive:

Second concurrent nslookup spawned by the same malicious PowerShell session.

The argument 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv...haz4rdw4re.io is base64-encoded data being sent in the DNS query itself (classic DNS tunneling).

Decoded snippet starts with client portfolio data – this is the **actual stolen financial information being exfiltrated chunk-by-chunk over DNS to the attacker-controlled domain haz4rdw4re.io.

Reason for Escalating the Alert:

Confirmed, active, high-volume exfiltration of sensitive client financial data via DNS tunneling is happening right now. More data is leaving the network with every query.

Recommended Remediation Actions:

1. Block ALL DNS traffic from win-3450 immediately (or cut the machine completely offline)
2. Sinkhole / block haz4rdw4re.io enterprise-wide
3. Capture full DNS logs + PCAP for win-3450 (contains the stolen data in flight)
4. Assume full contents of SSF-FinancialRecords share are compromised and already with the attacker

List of Attack Indicators :

- Initial phishing: ImportantInvoice-Febrary.zip → michael.ascot (11:13:37)
- PowerView.ps1 dropped (11:35:07)
- Mapped \FILESRV-01\SSF-FinancialRecords to Z: (11:37:02)
- Robocopy to local exfiltration folder (11:37:49)
- Cleaned up Z: mapping (11:38:00)
- Active DNS tunneling/exfil to haz4rdw4re.io (11:38:47)

20- suspicious parent-child relationship(ID=1027)

Incident report:

Time of Activity:

12/05/2025 11:38:47 UTC (same second – third parallel nslookup)

List of Affected Entities:

- Workstation: win-3450
- User: michael.ascot@tryhatme.com
- Parent process: malicious powershell.exe PID 3728
- Working directory: C:\Users\michael.ascot\downloads\exfiltration\

Reason for Classifying as True Positive:
Third simultaneous nslookup spawned by the attacker's PowerShell session.

The query string U3VtbWFyeS54bHN4c87JTM0rCcgvKk…haz4rdw4re.io is base64 that starts with Summary.xlsx (a real financial spreadsheet filename from the stolen share). The attacker is aggressively pushing multiple files in parallel over DNS to haz4rdw4re.io right now.

Reason for Escalating the Alert:

Massive, high-speed exfiltration of actual financial workbooks and client data is actively occurring. Every new nslookup = another chunk of sensitive data leaving the network forever.

Recommended Remediation Actions (do this in the next 10–20 seconds):

1. KILL THE NETWORK CONNECTION TO win-3450 IMMEDIATELY – pull cable / disable port / firewall block 2 Enterprise-wide block + sinkhole haz4rdw4re.io 3 Preserve every DNS log and packet – it literally contains the stolen files 4 Declare confirmed major data breach – financial client data is already exfiltrated

List of Attack Indicators :

- C2 / exfil domain: haz4rdw4re.io (DNS tunneling)
- Exfiltrated filenames seen so far in queries: Summary.xlsx, ClientPortfolio

Final Result: