Incident Investigation Report — Suspicious Email Detection

— Suspicious email attachment detected

Infrastructure and Security - Cyber Security Incident Response Analyst

Prepared by: Ashraf Alaa Alkafury

Group Name : (AMIT-ONL2_ISS2_S1)

Incident Report: Suspicious Email Detection

Event ID: 1001
Date Analyzed: 12 May 2025
Direction: Inbound
Detection Source: Email
Reported By: SOC Monitoring System

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:	05/12/2025 15:32:55.770
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

---

1. Description

A suspicious inbound email was flagged by the detection system due to the presence of an *unusual top-level domain (TLD)* used by the sender's email address: chicmillinerydesigns.de.

🔎 **Note from SOC Head:** “This detection rule still needs fine-tuning.”

---

2. Email Metadata

- **Subject:** VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping
- **Sender:** maximillian@chicmillinerydesigns.de

- **Recipient:** michelle.smith@tryhatme.com
- **Timestamp:** 2025-05-12 15:32:55.770
- **Attachment:** None
- **Content:** Redacted per company policy to protect sensitive information.

---

3. Domain Reputation Check

Domain: chicmillinerydesigns.de
Top-Level Domain: .de (Germany – considered a valid TLD)

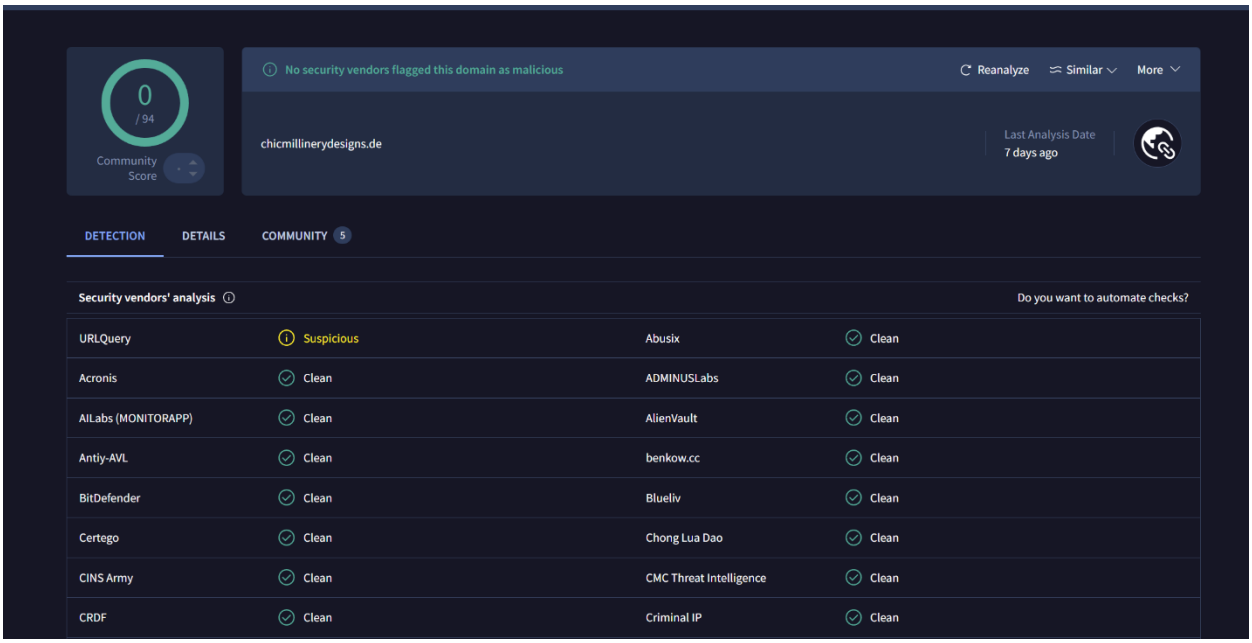
VirusTotal Analysis Summary

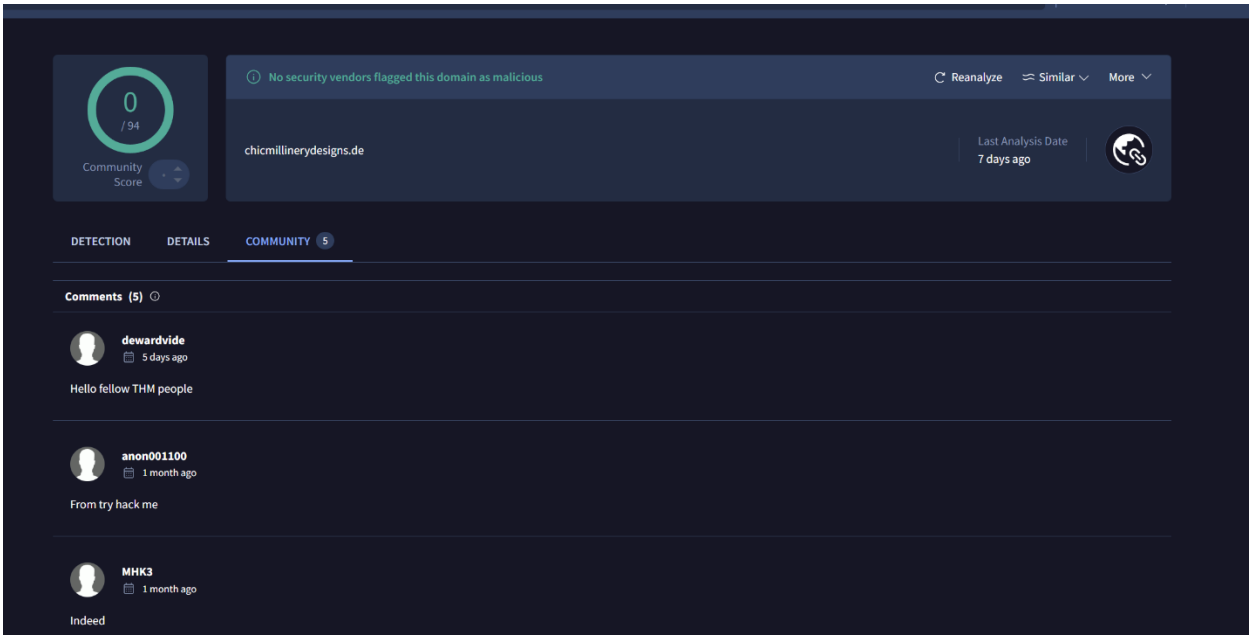
- **Vendors Flagged as Malicious:** 0 / 94
- **URLQuery Result:** Suspicious (Only 1 vendor flagged as “Suspicious”)
- **Community Score:** 0 (Neutral)
- **Last Scan:** 7 days ago
- **Detection Summary:** Majority of security vendors (93/94) marked the domain as clean.

---

4. Analysis

- Although the domain .de is not uncommon, it may have been flagged due to geographical targeting or unfamiliarity with the domain by the detection system.
- The subject line has hallmarks of a phishing attempt (e.g., “Your Dream Vacation”, “Just Pay Shipping”) — this raised suspicion.
- However, there was no attachment, and no links or payloads were analyzed due to redacted content.
- No other domain reputation services flagged it as malicious.
- Therefore, the alert appears to be **non-malicious** based on available evidence.

- 

- 

---

5. Action Taken

- **Alert Classification:** False Positive
- **SOC Decision:** Closed the alert with no further action required.
- **Recommendation:**

- Add chicmillinerydesigns.de to the allowlist if legitimate communication is expected from this domain.
- Continue tuning the detection rule to reduce noise from non-malicious foreign TLDs.
- Monitor for any future patterns involving .de domains with suspicious subject lines.

Suspicious Email Attachment Detected – Documentation

Challenge Type: SOC Level 1 – Incident Response
Objective: Investigate a suspicious PowerShell script discovered in an email attachment and analyze its behavior to determine if it's malicious.

📜 1. Overview

During routine monitoring, a suspicious .ps1 PowerShell script was discovered as an email attachment. The email claimed to offer IT support but contained a script with system-wide access behaviors. Our task was to analyze the script and identify its functions, risks, and intent.

---

1. **Script Header – Metadata**

```
<#
.SYNOPSIS
This script was crafted by the one and only Yani Zubair from IT. Contact him at yani.zubair@tryhatme.com for all your tech needs!

.DESCRIPTION
This script automates Windows updates and performs various system diagnostics for troubleshooting. The generated files are saved in the output folder and can b

.NOTES
Author: Yani Zubair
Contact: yani.zubair@tryhatme.com
#>
```

- **Function: Introduces the script, its purpose, and the author's contact.**
- **Risk: Legitimate-looking metadata could be misleading in malicious contexts.**

---

2. Startup Message

```
Write-Host "Greetings, tech warriors! This script, artfully crafted by Yani Zubair from IT, is here to save the day! Contact him at yani.zubair@tryhatme.com for all your tech needs." -ForegroundColor Magenta
Write-Host "Starting Windows Update and System Diagnostics..." -ForegroundColor Green
```

- **Function: Displays welcoming messages in green text.**

- **Purpose: Signals the start of the script for user feedback.**

---

3. Module Installation

```
# Install and import the PSWindowsUpdate module
Install-Module PSWindowsUpdate -Force -Scope CurrentUser
Import-Module PSWindowsUpdate
```

- **Function: Installs and imports a PowerShell module for managing Windows updates.**
- **Note: Requires internet and PowerShell gallery access.**

---

4. System Update Execution

```
# Force Windows Update
Write-Host "Installing all available updates, this might take some time..." -ForegroundColor Green
Install-WindowsUpdate -AcceptAll -AutoReboot
Write-Host "Windows Update completed." -ForegroundColor Green
```

- **Function: Installs all available updates and may reboot the system.**
- **Risk: May disrupt active sessions or tasks if executed unknowingly.**

---

5. Create Diagnostics Directory

```
# System Diagnostics
$diagnosticsPath = "C:\Temp"
if (-Not (Test-Path $diagnosticsPath)) {
    New-Item -Path $diagnosticsPath -ItemType Directory -Force
}
```

- **Function: Creates C:\Temp to store diagnostic outputs.**
- **Purpose: Ensures all logs and reports are organized in one directory.**

---

6. System Information Collection

```
# Collecting System Information
Write-Host "Collecting System Information..." -ForegroundColor Green
Get-ComputerInfo > "$diagnosticsPath\SystemInfo.txt"
Write-Host "System Information collected."
```

- **Function: Saves detailed hardware and OS info.**
- **Output: SystemInfo.txt contains CPU, RAM, BIOS, OS version, etc.**

---

7. Network Configuration Collection

```
# Collecting Network Configuration
Write-Host "Collecting Network Configuration..." -ForegroundColor Green
ipconfig /all > "$diagnosticsPath\NetworkConfig.txt"
Write-Host "Network Configuration collected."
```

- **Function: Logs full network adapter and IP config details.**
- **Use: Useful for diagnosing connectivity issues or mapping infrastructure.**

---

8. Installed Programs Inventory

```
# Collecting Installed Programs
Write-Host "Collecting Installed Programs..." -ForegroundColor Green
Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate >
Write-Host "Installed Programs collected."
```

- **Function: Queries the registry to extract installed software info.**
- **Details Logged: App name, version, publisher, and install date.**

---

9. Top Running Processes

```
# Collecting Running Processes
Write-Host "Collecting Running Processes..." -ForegroundColor Green
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 > "$diagnosticsPath\RunningProcesses.txt"
Write-Host "Running Processes collected."

Write-Host "All tasks completed. Diagnostics files are saved in $diagnosticsPath." -ForegroundColor Green
```

- **Function: Lists top 10 CPU-heavy processes.**
- **Purpose: Detects performance drains or potential suspicious activity.**

---

10. Completion Message

```
Write-Host "All tasks completed. Diagnostics files are saved in $diagnosticsPath." -ForegroundColor Green
```

- **Function: Confirms successful execution and diagnostics saved.**
- **Output: Confirms location of diagnostic files.**

---

11. Send Data via Email

- **Function: Emails all diagnostics files to an external address.**
- **⚠️ Risk: This is a critical red flag. Exfiltration of internal data without user consent is a clear security threat.**

🛡️ Incident Documentation: Suspicious File Stream Creation on Host win-3450

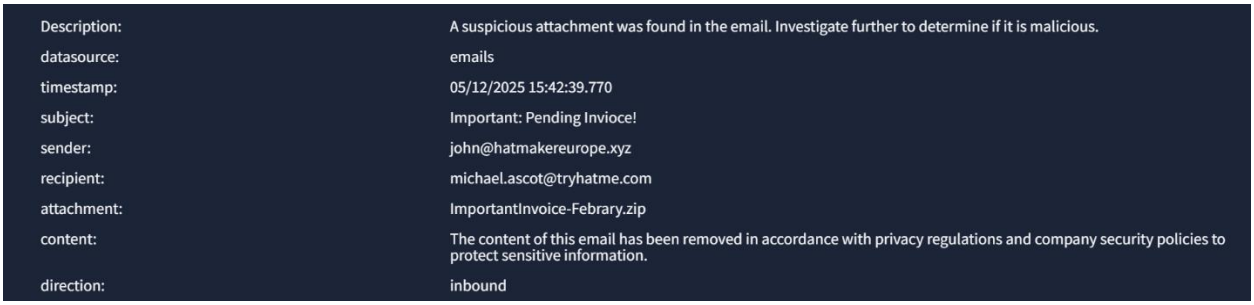
📜 Executive Summary

On May 12, 2025, at 15:02:57.770, a suspicious shortcut file named invioce.pdf.lnk was created in the Temp directory of user michael.ascot (CEO of TryHatMe). This was detected by Sysmon event ID 15 (FileCreateStreamHash) and logged via Splunk from host win-3450. Multiple indicators suggest this is a malicious LNK file potentially linked to a phishing or malware attack.

🔎 Event Details

Field	Value
Username	Michael Ascot
Email	michael.ascot@tryhatme.com

Field	Value
Host Name	win-3450
IP Address	10.10.253.241
Process	Explorer.EXE (PID 3180)
Event Code	15 – FileCreateStreamHash
Timestamp	05/12/2025 16:02:57.770
File Path	C:\Users\michael.ascot\AppData\Local\Temp\ImportantInvoice-Febrary.zip\ImportantInvoice-Febrary\invioce.pdf.lnk
File Type	Shortcut (.lnk), 1 KB
Detected By	Sysmon, forwarded by eventcollector



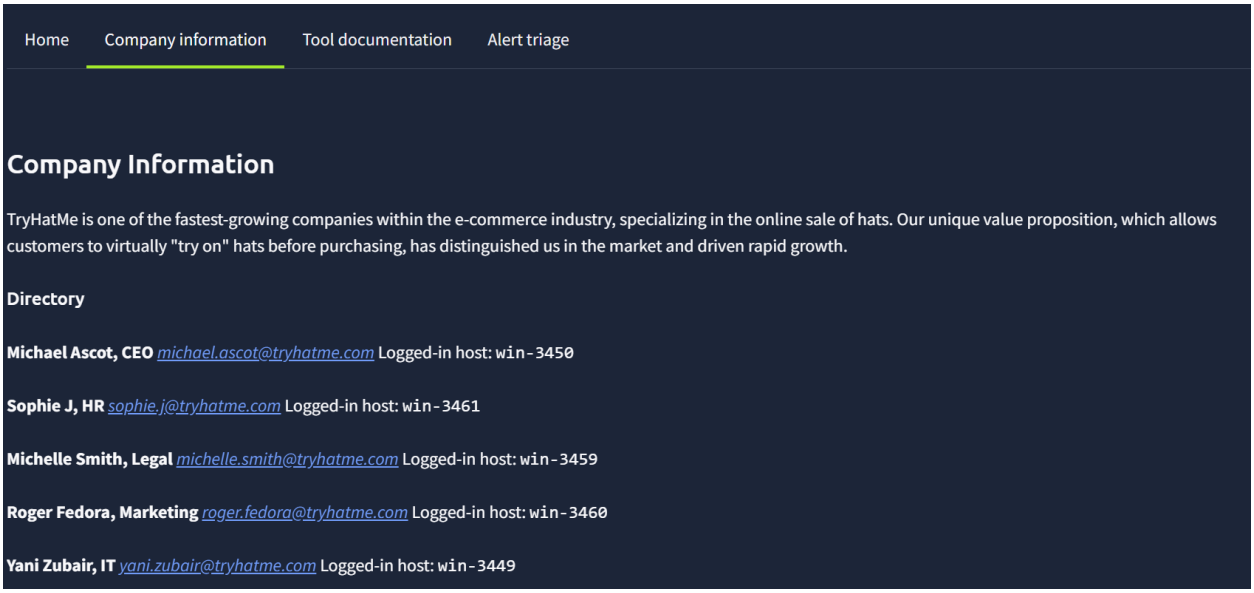
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
datasource:	emails
timestamp:	05/12/2025 15:42:39.770
subject:	Important: Pending Invioce!
sender:	john@hatmakereurope.xyz
recipient:	michael.ascot@tryhatme.com
attachment:	ImportantInvoice-Febrary.zip
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

🚩 Indicators of Suspicion

1. **Filename: invioce.pdf.lnk – misspelled “invoice,” common in phishing.**
2. **Location: Stored in the Temp directory inside a suspiciously named .zip file.**
3. **File Size: 1 KB, suggesting it’s a shortcut pointing to hidden/external content.**
4. **Triggered Process: Explorer.EXE, suggesting user interaction (clicked/opened).**
5. **Event Frequency: Host win-3450 generated 63.158% of all monitored Sysmon events — indicates it was the most active machine in the incident window.**

🏢 User and Device Context

From the internal TryHatMe company directory:

- **Michael Ascot (CEO) is the user tied to host win-3450.**
- **The email michael.ascot@tryhatme.com is officially associated with that host.**
- **Device is confirmed online and active during the time of incident.**
- 

🕒 Timeline

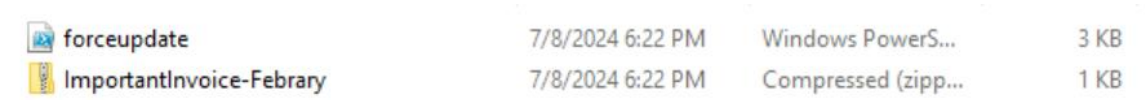
Time	Event
15:20	invioce.pdf.lnk file appears on disk (seen in File Explorer snapshot).
15:42:39.770	General timestamp log of surrounding activity.
16:02:57.770	Sysmon logs FileCreateStreamHash event for the suspicious .lnk file.

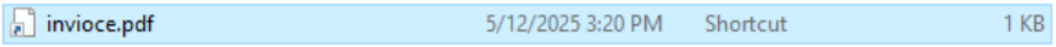
```
timestamp:                                05/12/2025 15:42:39.770
```

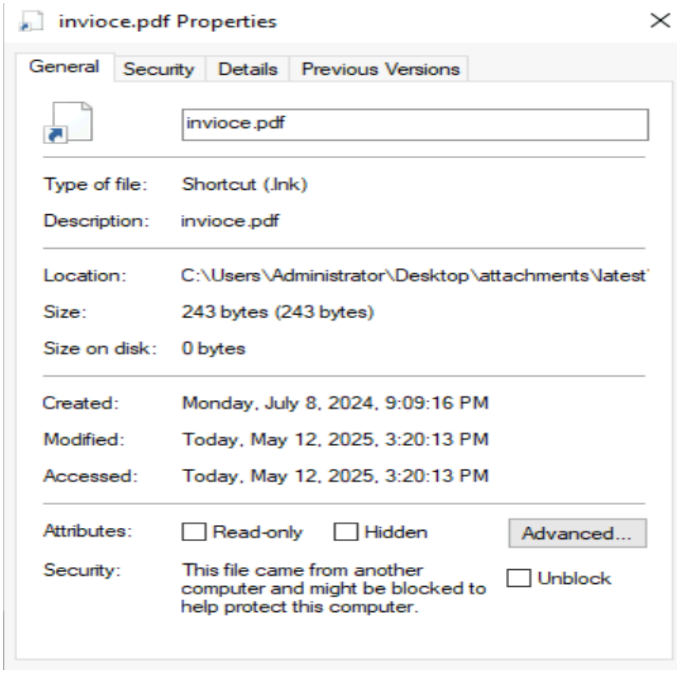
📌 Technical Implications

- **Sysmon Event ID 15 logs creation of alternate data streams or .lnk file activity — often used in living-off-the-land attacks (LOTL).**

- **.lnk files are known vectors for code execution or dropping payloads from remote sources.**







🧩 Possible Attack Vector

The file appears to be embedded in a ZIP archive titled:

ImportantInvoice-Febrary.zip\ImportantInvoice-Febrary\invioce.pdf.lnk

This matches classic phishing delivery methods:

- **ZIP attachment in email → user unzips → sees deceptive filename → clicks → executes hidden malicious payload.**

✅ Recommended Actions

1. Immediate Containment

- **Isolate host win-3450 from internal network.**
- **Revoke CEO's credentials if compromised.**
- **Disable Explorer autorun for .lnk files (Group Policy).**

2. Forensics

- **Dump memory of win-3450.**
- **Search for persistence mechanisms (registry run keys, scheduled tasks).**
- **Extract and analyze .lnk file in sandbox (e.g., AnyRun, Cuckoo).**

3. Detection & Response

- **Correlate this event with outbound connections from win-3450.**
- **Look for similar .lnk files in AppData\Temp on other hosts (e.g., win-3454, win-3461).**
- **Enhance SIEM rules for Sysmon Event ID 15 + .lnk + Temp.**

4. Awareness & Training

- **Alert users about recent phishing emails with "Important Invoice" themes.**
- **Conduct simulated phishing test.**

📦 Log Evidence Snapshot

{

"datasource": "sysmon",

"event.action": "File stream created (rule: FileCreateStreamHash)",

"event.code": 15,

"file.path": "C:\\Users\\michael.ascot\\AppData\\Local\\Temp\\ImportantInvoice-Febrary.zip\\ImportantInvoice-Febrary\\invioce.pdf.lnk",

"host.name": "win-3450",

"process.name": "Explorer.EXE",

"process.pid": 3180,

"timestamp": "05/12/2025 16:02:57.770"

}