



A L T A Y

INTRODUCTION TO PHISHING WRITE - UP

THM SOC SIMULATOR

01.03.2025

MEHMET MERMER



ALERT ID 1000

← Case report for event ID: 1000

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1000	Suspicious email from external domain.	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.	Phishing	Low	Mar 2nd 2025 at 01:27

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:25:06.151

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

Bu alarm, Miguel O'Donnell adlı satış personeline ait olan, Şirkette win-3451 bilgisayarında oturum açılmış “miguel.odonnell@tryhatme.com” mail adresine, şirket dışı “boone@hatventuresworldwide.online” adlı mail adresi üzerinden, “You've Won a Free Trip to Hat Wonderland - Click Here to Claim” konu başlığıyla gönderilmiş olup incelendiğinde **Ücretsiz Seyahat Kazanıldığı** talep edilmektedir. Özellikle .online gibi çok kullanılmayan domain adresi üzerinden gönderilmiş olmakla birlikte insanı acele ettiren **Talep Etmek İçin Tıklayın** gibi aceleci başlıklar altında kullanılmış olması mailin phishing olduğunun göstergesidir. Bu sebepten ötürü bu alarm **True Pozitif** olarak kapatılabilir.

ALERT ID 1001

← Case report for event ID: 1001

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1001	Suspicious email from external domain.	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.	Phishing	Low	Mar 2nd 2025 at 01:28

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:26:06.151

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

Bu alarm, Michelle Smith adlı personele ait olan, Şirkette win-3459 bilgisayarında oturum açılmış “michelle.smith@tryhatme.com” mail adresine, şirket dışı “maximillian@chicmillinerydesigns.de” adlı mail adresi üzerinden, “VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping” konu başlığıyla gönderilmiş olup incelendiğinde Hayalinizdeki Tatilin Sizi Beklediğini söylemektedir. İnsanı cezbettiren , Sadece Nakliye Öde gibi dikkat çekici başlıklar altında kullanılmış olması mailin phishing olduğunun göstergesidir. Bu sebepten ötürü bu alarm **True Pozitif** olarak kapatılabilir.

ALERT ID 1002

← Case report for event ID: 1002

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1002	Suspicious Parent Child Relationship	A suspicious process with an uncommon parent-child relationship was detected in your environment.	Process	Low	Mar 2nd 2025 at 01:30

[Alert details](#) ^
datasource: sysmon
timestamp: 03/01/2025 22:28:15.151
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 NGCKKeyPregen
process.working_directory: C:\Windows\system32\
event.action: Process Create (rule: ProcessCreate)

Bu alarm, process oluşturma işlemi üzerine tetiklenmiştir. **taskhostw.exe** adlı bir işlemin **NGCKKeyPregen** argümanı ile çalıştırıldığını gösteriyor. **taskhostw.exe**, Windows’un yasal bir sistem sürecidir ve dinamik bağlantı kitaplıklarını (DLL) barındıran işlemleri çalıştırmak için kullanılır. **NGCKKeyPregen**, Windows Hello PIN ve biyometrik kimlik doğrulama ile ilgili anahtarların önceden oluşturulmasını (pre-generation) sağlayan bir bileşendir. **svchost.exe** ise Windows hizmetlerini çalıştıran bir sistem sürecidir. Bu sebepten ötürü alarm **False Pozitif** olarak kapatılabilir.

ALERT ID 1003

← Case report for event ID: 1003

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1003	Reply to suspicious email.	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.	Phishing	Low	Mar 2nd 2025 at 01:32

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:29:32.151

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

Bu alarm, şirkete ait destek maili olan, “support@tryhatme.com” maili üzerinden “**FWD: Convention Registration Now Open: Hat Trends and Insights**” konu başlığında şirkete ait olmayan “warner@yahoo.com” mail adresine gönderilmiş bir mail olup incelendiğinde Şapka Eğilimleri ve Analizleri kongresine kayıt olmasını anlatan bir bilgilendirme maili olduğu gösteren bir maildir. Bu sebepten ötürü **False Pozitif** olarak kapatılabilir.

ALARM ID 1004

← Case report for event ID: 1004

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1004	Suspicious Attachment found in email	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.	Phishing	Low	Mar 2nd 2025 at 01:33

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:31:10.151

subject: Force update fix

sender: yani.zubair@tryhatme.com

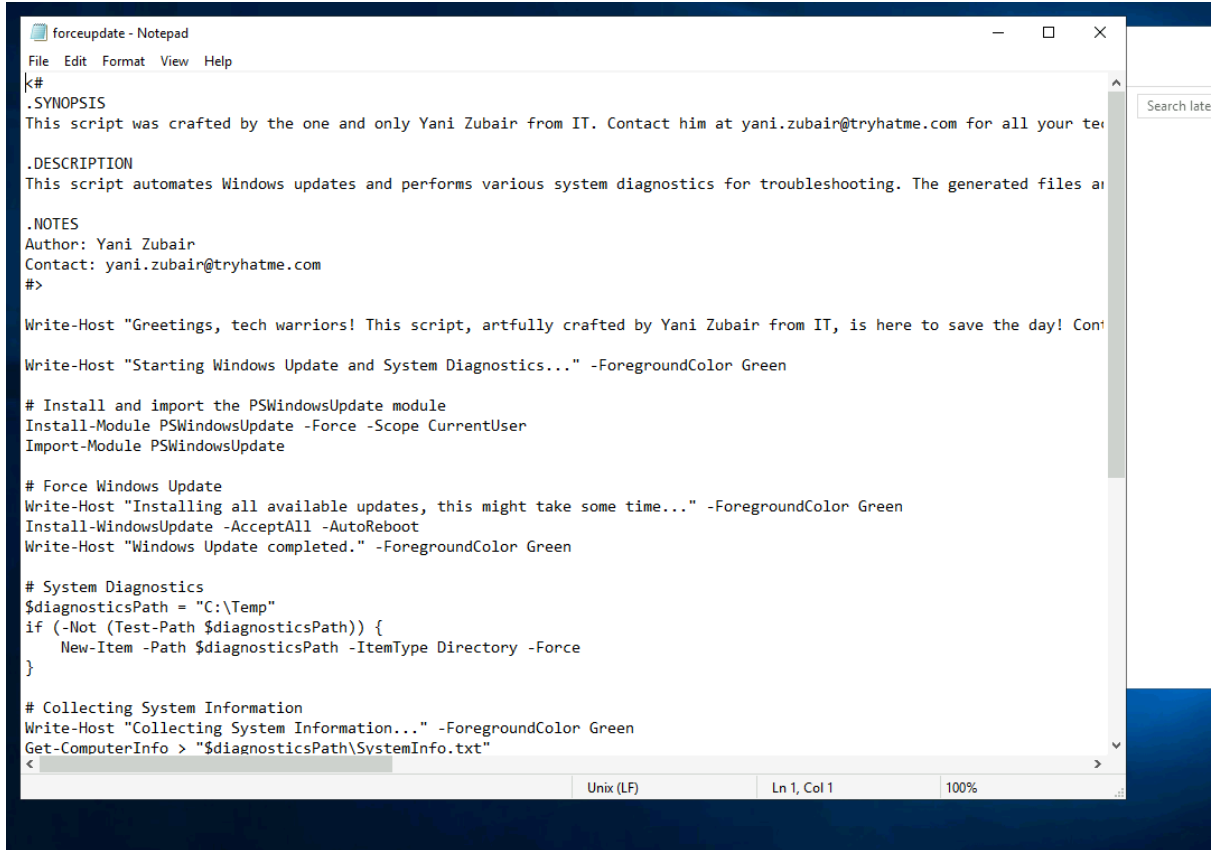
recipient: michelle.smith@tryhatme.com

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

Bu alarm, Yani Zubair, adlı IT personele ait olan, Şirkette win-3449 bilgisayarında oturum açılmış “**yani.zubair@tryhatme.com**” mail adresinden, yine şirket içerisinde Michelle Smith adlı personele ait olan, Şirkette win-3459 bilgisayarında oturum açılmış “**michelle.smith@tryhatme.com**” mail adresine “**Force update fix**” konu başlığında gönderilmiş olan maili içermektedir.



```
forceupdate - Notepad
File Edit Format View Help
k#
.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 located in the %TEMP% directory.

.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 me at yani.zubair@tryhatme.com for more info." -ForegroundColor Green

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
}

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

Ekte mevcut olan “**forceupdate.ps1**” powershell dosyası incelendiğinde şirket içi sistemsel bir güncelleme dosyası olduğu anlaşılmış olup alarm **False Pozitif** olarak kapatılabilir.

ALARM ID 1005

← Case report for event ID: 1005

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1005	Reply to suspicious email.	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.	Phishing	Low	Mar 2nd 2025 at 01:34

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:31:30.151

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

Bu alarm, Sophie J. adlı personele ait olan, Şirkette win-3461 bilgisayarında oturum açılmış “sophie.j@tryhatme.com” mail adresinden, “**Shrinking Hat Sale: Tiny Hats for Extraordinary People**” konu başlığında şirkete ait olmayan “eileen@gmail.com” mail adresine gönderilmiş bir mail olup incelendiğinde herhangi bir olumsuz durum tespit edilmemiştir, alarm **False Pozitif** olarak kapatılabilir.

ALARM ID 1006

← Case report for event ID: 1006

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1006	Suspicious email from external domain.	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.	Phishing	Low	Mar 2nd 2025 at 01:35

Alert details ^

datasource: emails

timestamp: 03/01/2025 22:33:27.151

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

Bu alarm, şirkete ait “invoice@tryhatme.com” maile, şirket dışı “tim@chicmillinerydesigns.de” adlı mail adresi üzerinden, “**Hats Off to Savings: Discounted Vacation Packages Just for You!**” konu başlığıyla gönderilmiş olup incelendiğinde **İndirimli Tatil Paketleri!** olduğunu söylemektedir. İnsanı cezbettiren, dikkat çekici başlıklar altında kullanılmış olması mailin phishing olduğunun göstergesidir. Bu sebepten ötürü bu alarm **True Pozitif** olarak kapatılabilir.

ALARM ID 1007

ID	Alert rule	Severity	Type	Date	Status
1007	Suspicious Attachment found in email	Low	Phishing	Mar 2nd 2025 at 04:43	Awaiting action
Description:		A suspicious attachment was found in the email. Investigate further to determine if it is malicious.			
datasource:		emails			
timestamp:		03/02/2025 01:41:08.748			
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			

Bu alarm, Michael Ascot adlı şirketin Ceo'suna ait olan, Şirketin win-3450 bilgisayarında oturum açılmış “**michael.ascot@tryhatme.com**” mail adresine, şirket dışı “**john@hatmakereurope.xyz**” adlı mail adresi üzerinden, “**Important: Pending Invoice!**” konu başlığıyla ekli zip dosyasıyla birlikte gönderilmiş olup incelendiğinde özellikle zip dosyasının içerisinde zararlı olabilecek bir pdf dosyasına rastlanmıştır. Konu başlığında **Önemli!** gibi dikkat çekici başlıklar ile birlikte dosyanın indirilmesi sağlanıp saldırının gerçekleşmesi hedeflenmektedir. Ayrıca ekli dosyada yapılan yazım yanlışları mailin phishing olduğunun göstergesidir. Bu sebepten ötürü bu alarm **True Pozitif** olarak kapatılabilir.