

INTRO TO PHISHING



Hazırlayan

Adı: Ayşe

Soyadı: BALCI

Tarih: 01/03/2025

Assigned alert(s) Write case report

1001

Suspicious email from external domain. ^

Low

Phishing

Mar 1st 2025 at 20:23

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 17:21:16.938

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

Göndericinin domaini ve ip adresi virustotal, abuseipdb gibi sitelerde aratıldıktan sonra herhangi bir şüpheli durumla karşılaşılmadı bu yüzden bu Alert False Positive.

1002 Suspicious Parent Child Relationship ^ Low Process Mar 1st 2025 at 20:25

Description:

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

datasource:

sysmon

timestamp:

03/01/2025 17:23:25.938

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, Windows'un görev yöneticisi olup genellikle DLL tabanlı görevleri çalıştırır. svchost.exe, sistem hizmetlerini yöneten bir süreçtir ve bazı durumlarda taskhostw.exe'nin ebeveyni olabilir. NGCKeypregen, Windows Hello ve TPM ile ilgili bir bileşen olup, şifreleme anahtarlarını yönetmek için çağrılabilir. Eğer Windows Hello aktifse, bu işlem normaldir. Ayrıca çalışma klasörü normal olduğu için alarm false pozitiftir.

Assigned alert(s) Write case report

1003	Reply to suspicious email. ^	Low	Phishing	Mar 1st 2025 at 20:27	👤-
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 17:24:42.938			
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			

Documentation kısmında şirket mailleri vardır ve sender maili şirketten gelen bir mail adresi olduğu için alarm false pozitiftir.

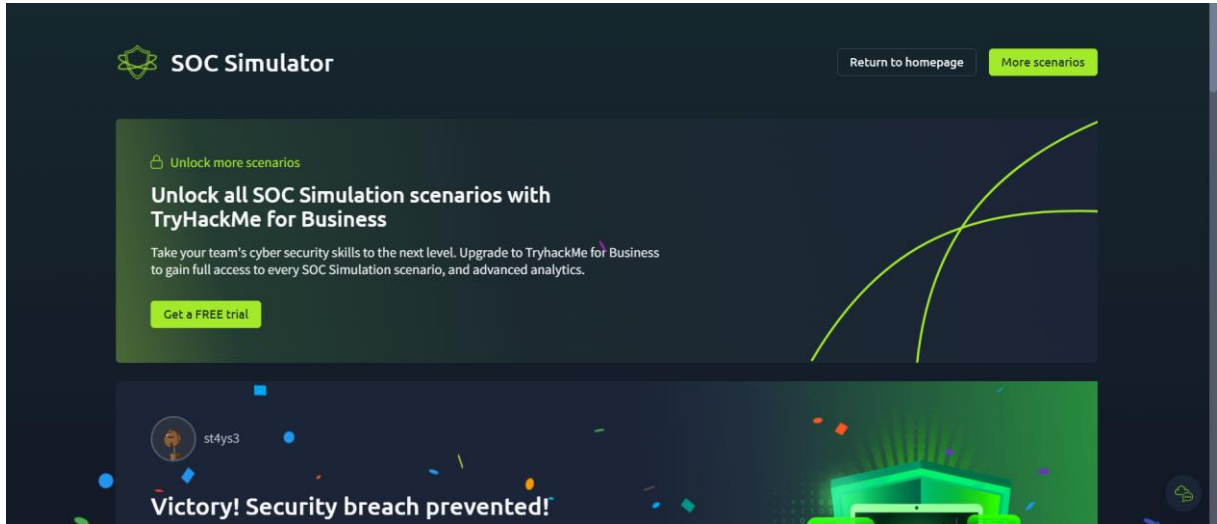
Assigned alert(s) Write case report

1004	Suspicious Attachment found in email ^	Low	Phishing	Mar 1st 2025 at 20:28	👤-
Description:		A suspicious attachment was found in the email. Investigate further to determine if it is malicious.			
datasource:		emails			
timestamp:		03/01/2025 17:26:20.938			
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			

Analyst VM kısmında forceupdate.ps1 dosyasının içeriği incelendi şüpheli bir durum görülmedi ayrıca sender maili şirketin IT yetkilisine atanmış bir mail olduğu için alarm false pozitiftir.

1007	Suspicious Attachment found in email ^	Low	Phishing	Mar 1st 2025 at 20:33	👤-
Description:		A suspicious attachment was found in the email. Investigate further to determine if it is malicious.			
datasource:		emails			
timestamp:		03/01/2025 17:31:00.938			
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			

Domain virustotal üzerinde kontrol edildiğine şüpheli olarak görüldü ayrıca analyst vm makinesinde attachments klasöründe zip dosyası bulundu içeriği çıkarıldığında ise bir lnk dosyası olarak görünüyor fakat uzantısı .pdf bu yüzden bu alarm true pozitiftir.



Alarmlar kapatıldıktan sonra ilk senaryo bitmiş oluyor ve simülâtör bu ekrana gitmiş oluyor.

