

Introduction to Phishing

İREM GÜZEL
01.03.2025

İçindekiler

Company Information.....	2
False Positive Alert.....	2
ID 1000	2
Suspicious Alert	3
ID 1002	3
ID 1004	3
True Positive Alert	4
ID 1007	4

Company Information

Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450

Sophie J, HR sophie.j@tryhatme.com Logged-in host: win-3461

Michelle Smith, Legal michelle.smith@tryhatme.com Logged-in host: win-3459

Roger Fedora, Marketing roger.fedora@tryhatme.com Logged-in host: win-3460

Yani Zubair, IT yani.zubair@tryhatme.com Logged-in host: win-3449

Miguel O'Donnell, Sales miguel.odonnell@tryhatme.com Logged-in host: win-3451

Cain Omoore, Sales cain.omoore@tryhatme.com Logged-in host: win-3452

Kyra Flores, Sales kyra.flores@tryhatme.com Logged-in host: win-3453

False Positive Alert

ID 1000

Senayonun ilk örneği olan 1000 ID'li alert ile analize başlayalım

1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 17:29	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 14:27:23.060					
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					

Log içeriğini sender, subject, attachment olarak ele alacağız.

Sender : boone@hatventuresworldwide.online

Domain : hatventuresworldwide.online

hatventuresworldwide.online

Did you intend to search across the file corpus instead? [Click here](#)

0 / 94
Community Score 2

No security vendors flagged this domain as malicious

Reanalyze Similar More

hatventuresworldwide.online

Registrar ABOVE.COM PTY LTD. Creation Date 1 day ago Last Analysis Date 13 hours ago

Virüstopal analizinde domain kısmı temiz çıktı. Herhangi bir uyarı bulunmamaktadır.

Subject : You've Won a Free Trip to Hat Wonderland - Click Here to Claim

Attachment : None

Dosyada bir ek bulunmuyor. Mail phishing başlığında olsa bile genel olarak içeriğinde zararlı bir link ve obje bulunmadığı için FP olarak sınıflandırılmıştır.

Senaryonun diğer ‘Suspicious email from external domain’ alertlerinde de aynı mantıkla FP olarak Case yazılmıştır.

Suspicious Alert

ID 1002

Bu alertte process taskhostw.exe ve process’in parent_name’i : svchost.exe

Süreçler araştırıldığında Windows sistem süreçlerini yönetmek için olan bir işlem olduğu belirtiliyor.

Olayın ilgili kötü amaçlı yazılım bağlamında olup olmadığı ve bir korelasyonun başlangıcı olup olmadığı henüz belirlenemediği için işlem Splunk tarafında takibe alındı.Şu an FP olarak işaretlendi ve ilgili Case yazıldı.

1002	Suspicious Parent Child Relationship	Low	Process	Mar 1st 2025 at 17:33	Awaiting action	
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 14:30:32.060					
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)					

New Search

1 *svchost.exe

ID 1004

Bu alertin şüpheli olarak belirtilmesindeki en büyük kısım ek olarak bir powershell script dosyası içermesidir. Dosya indirilemediği için dosyanın statik veya dinamik analizi

yapılamamaktadır. Ancak Alert IT departmanının bir şirket çalışanına atılmış. Bundan dolayı genel olarak FP olarak Case'lenmiştir.

1004	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 17:35	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 14:33:27.060				
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				

True Positive Alert

ID 1007

Senaryonun tek TP alertinin detaylarına bakalım :

1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 17:40	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 14:38:07.060				
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				

Sender : john@hatmakereurope.xyz

Domain : hatmakereurope.xyz

hatmakereurope.xyz

0
/ 94
Community Score

No security vendors flagged this domain as malicious

hatmakereurope.xyz

elevated exposure Suspicious (alphaMountain.ai)

Last Analysis Date
3 days ago

DETECTION

DETAILS

COMMUNITY 1

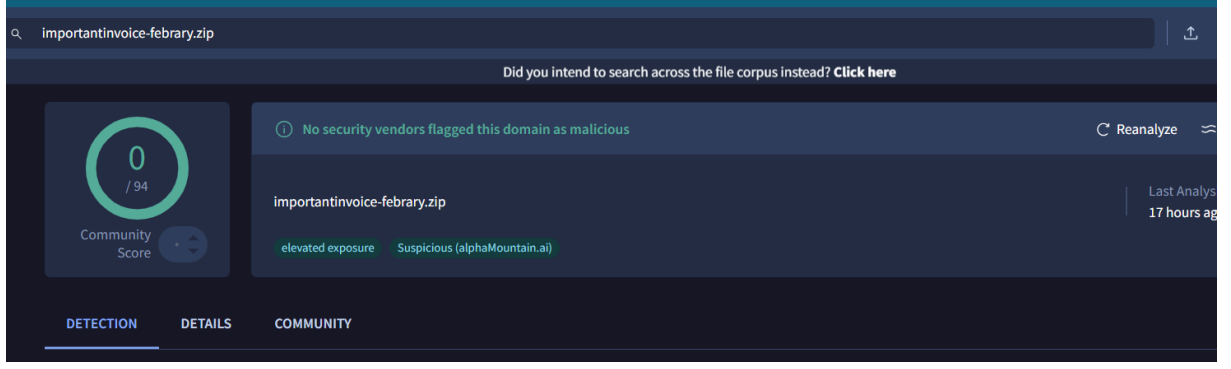
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Suspicious	Forcepoint ThreatSeeker	Suspicious
Trustwave	Suspicious	Abusix	Clean

Attachment : ImportantInvoice-February.zip



İlgili mail şirket dışından gelmiştir, .zip eki indirilemediği için Hash değeriyle bir sorgu yapılamıyor. Virütotal sonuçları temiz gelse dahi ek'ten dolayı şüpheli bulunduğu için TP olarak işaretlendi.