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

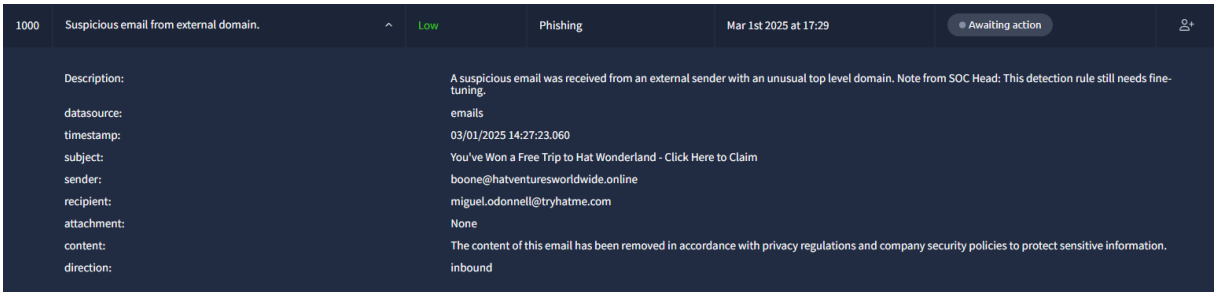
Cain Omoore, Sales cain.omoore@tryhatme.com Logged-in host: win-3452

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

False Positive Alert

ID 1000

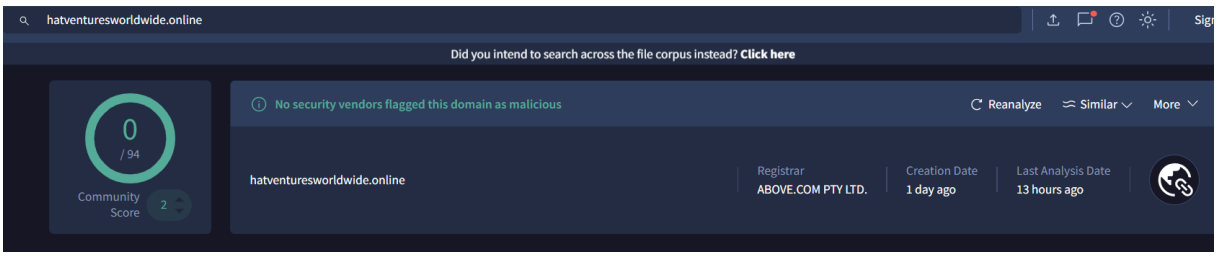
Senayonun ilk örneği olan 1000 ID'li alert ile analize başlayalım



Log içeriğini sender, subject, attachment olarak ele alacağız.

Sender : boone@hatventuresworldwide.online

Domain : hatventuresworldwide.online



Virüstotal 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.

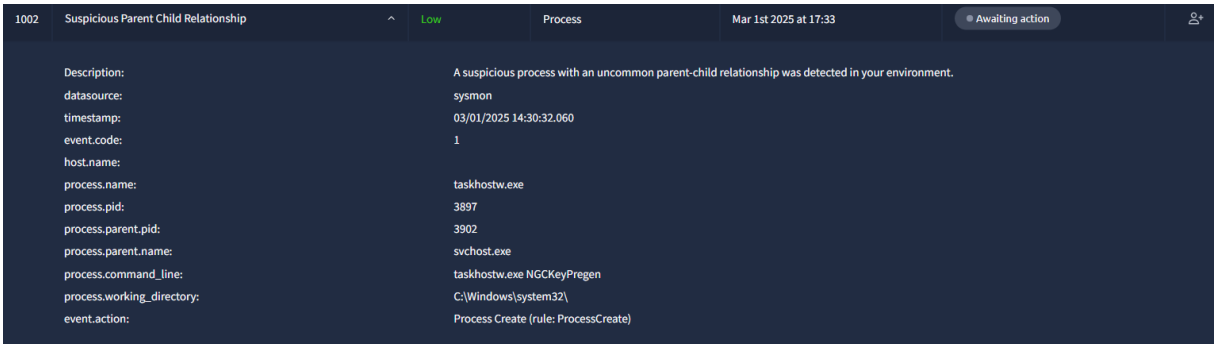
Suspicious Alert

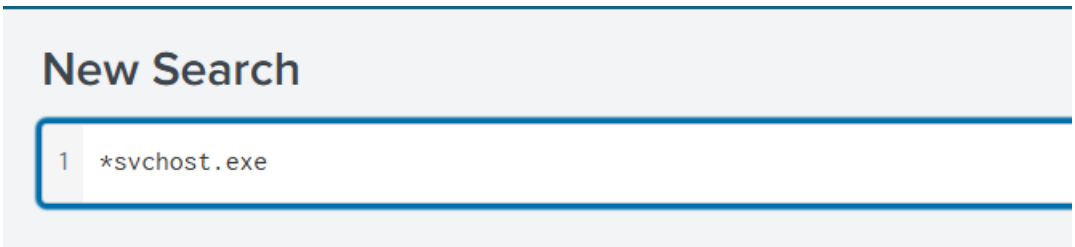
ID 1002

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.

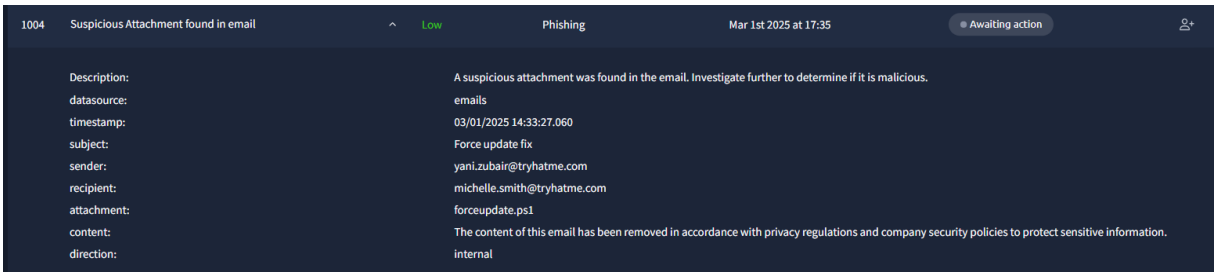




ID 1004

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

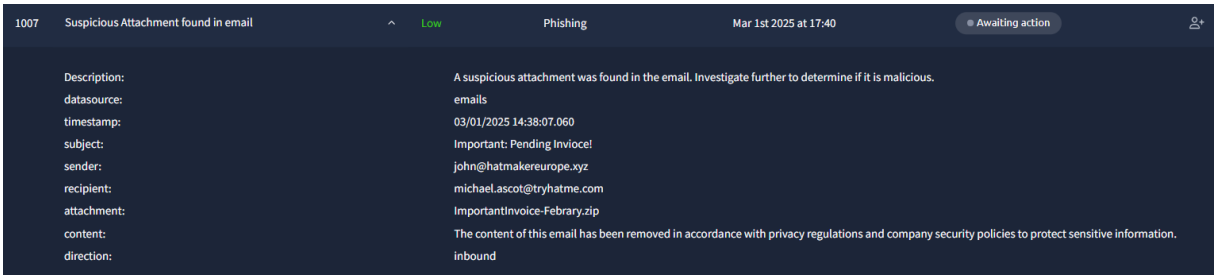
yapılamamaktadır.Ancak Alert IT departmanınan bir şirket çalışanına atılmış. Bundan dolayı genel olarak FP olarak Case'lenmiştir.



True Positive Alert

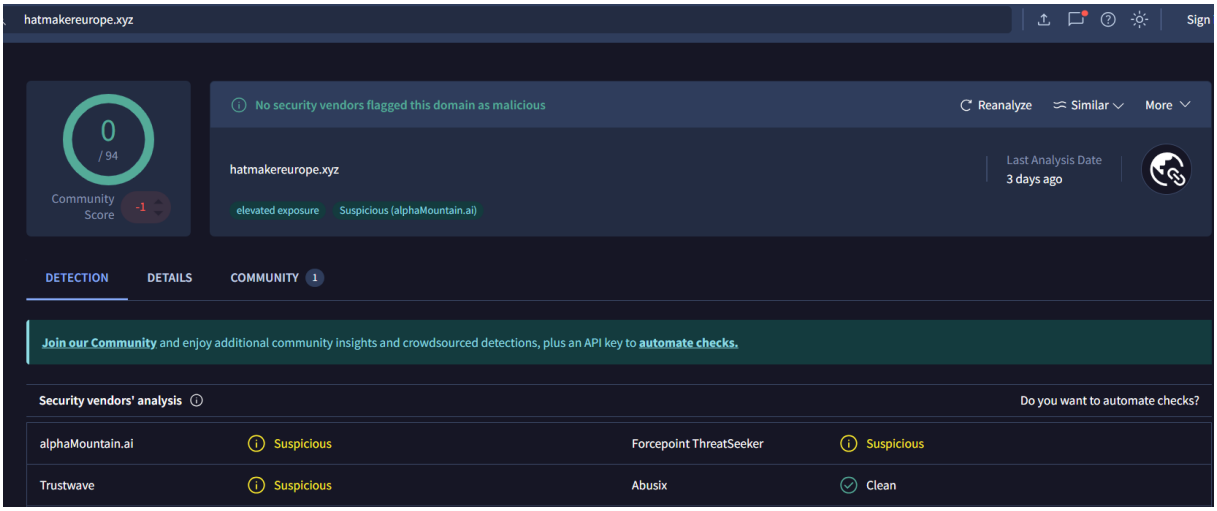
ID 1007

Senaryonun tek TP alertinin detaylarına bakalım :

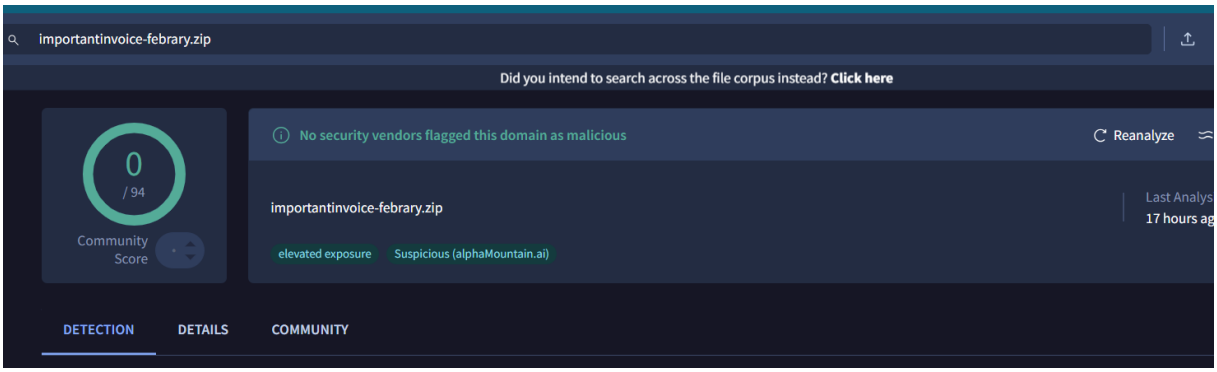


Sender : john@hatmakereurope.xyz

Domain : hatmakereurope.xyz



Attachment : ImportantInvoice-Febrary.zip



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