Introduction to Phishing

Hazırlayan: Sinan Kocagöz

Tarih: 28.02.2025

İçindekiler Tablosu

1. Giriş

Bu çalışmanın temel amacı, gerçek zamanlı phishing (oltalama) alarmlarını analiz etmek ve belirli bir zaman dilimi içinde bu alarmları doğru bir şekilde değerlendirmektir. Bu çalışmada:

- Gerçek zamanlı phishing girişimlerini tespit etmek ve analiz etmek.
- Gelen alarmların true positive (doğru pozitif) veya false positive (yanlış pozitif) olup olmadığını ayırt etmek.
- Log verilerini inceleyerek alarm kaynağını ve nedenini belirlemek.

2. Kapsam ve Yöntem

Bu simülasyon çalışması, 15 dakikalık bir zaman diliminde gerçekleştirilmiştir. Çalışma süresince aşağıdaki adımlar izlenmiştir:

- Splunk SIEM panelinde gelen alarmlar incelendi.
- Alarmların kaynağı ve ilgili log verileri detaylı bir şekilde analiz edildi.
- Elde edilen bulgulara göre alarmın true positive (gerçek tehdit) veya false positive (yanlış alarm) olduğu belirlen

3. Kullanılan Araçlar

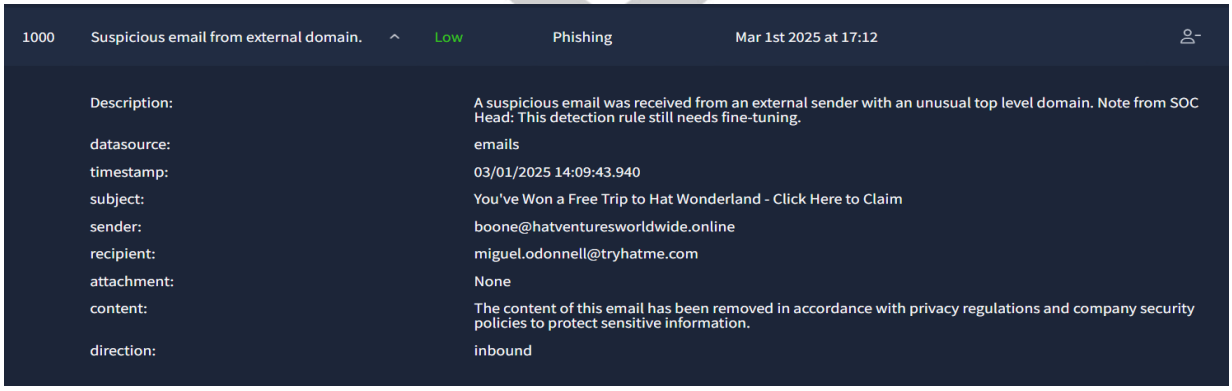
Splunk: Gerçek zamanlı alarm izleme ve log analizi için kullanılan SIEM aracı.
TryHackMe: SOC simülasyon ortamını sağlayan platformu.

4. Analiz Süreci

Alarmların kaynağına ait log verileri incelendi.
Ağ trafiği ve sistem kayıtları üzerinde anormallikler araştırıldı.
Şüpheli aktiviteler belirlenerek olası phishing girişimleri analiz edildi.

5. Bulgular

Alarm 1000: Suspicious email from external domain



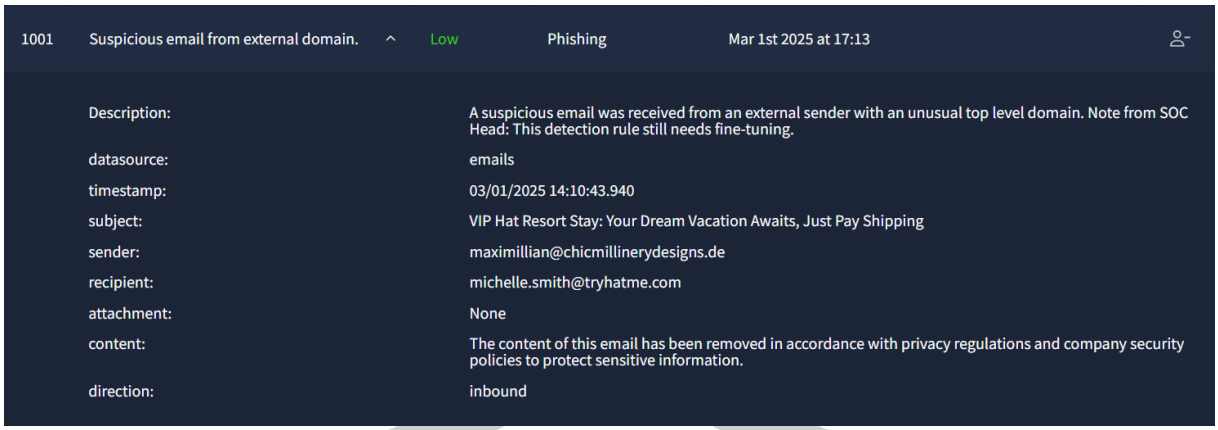
Severity: Low

Type: Phishing

Time to Resolve: 1.07 dakika

Sınıflandırma: False Positive, Harici bir alan adından gelen e-posta, ilk bakışta şüpheli görünse de yapılan analizde herhangi bir zararlı içerik veya kötü niyetli bağlantı tespit edilmemiştir. Bu nedenle alarm yanlış pozitif olarak değerlendirilmiştir.

Alarm 1001: Suspicious email from external domain



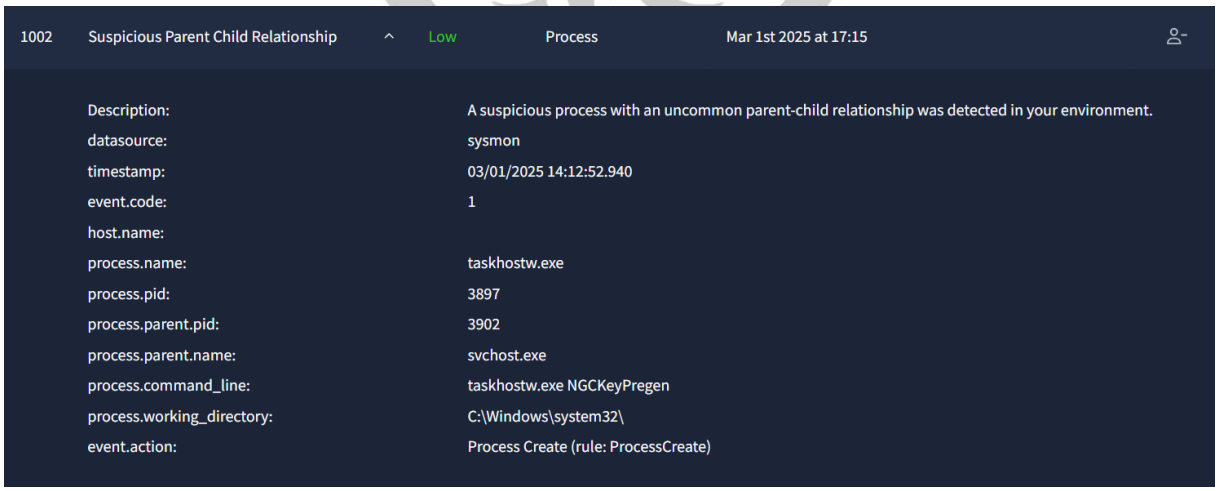
Severity: Low

Type: Phishing

Time to Resolve: 0.92 dakika

Sınıflandırma: False Positive, E-postanın geldiği alan adı incelenmiş ve güvenilir bir kaynağa ait olduğu doğrulanmıştır. İçerikte herhangi bir phishing göstergesi tespit edilmemiştir.

Alarm 1002: Suspicious Parent Child Relationship



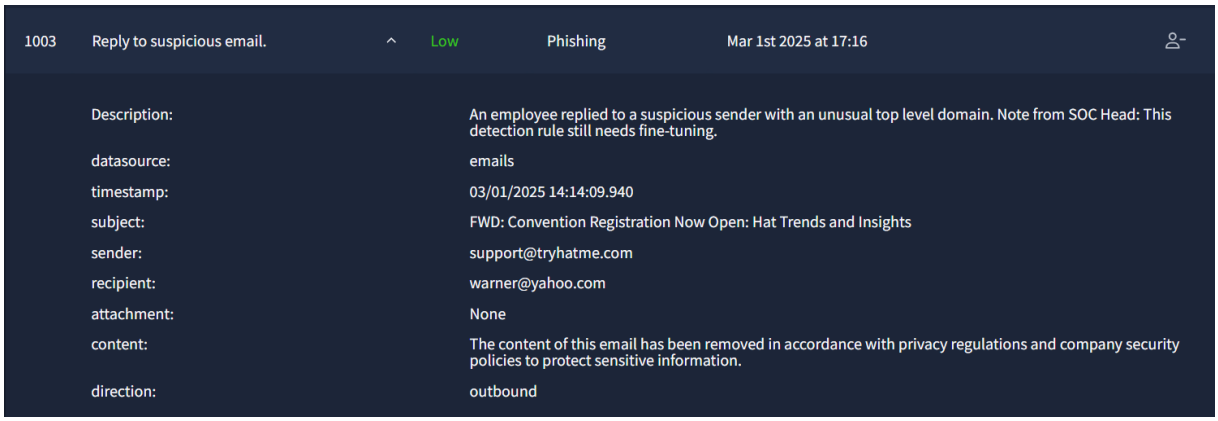
Severity: Low

Type: Process

Time to Resolve: 0.58 dakika

Sınıflandırma: False Positive Bir işlem ilişkisine dayalı bu alarm, güvenlik politikalarına uygun bir sistem sürecinden kaynaklanmıştır. Bu nedenle yanlış pozitif olarak değerlendirilmiştir.

Alarm 1003: Reply to Suspicious Email



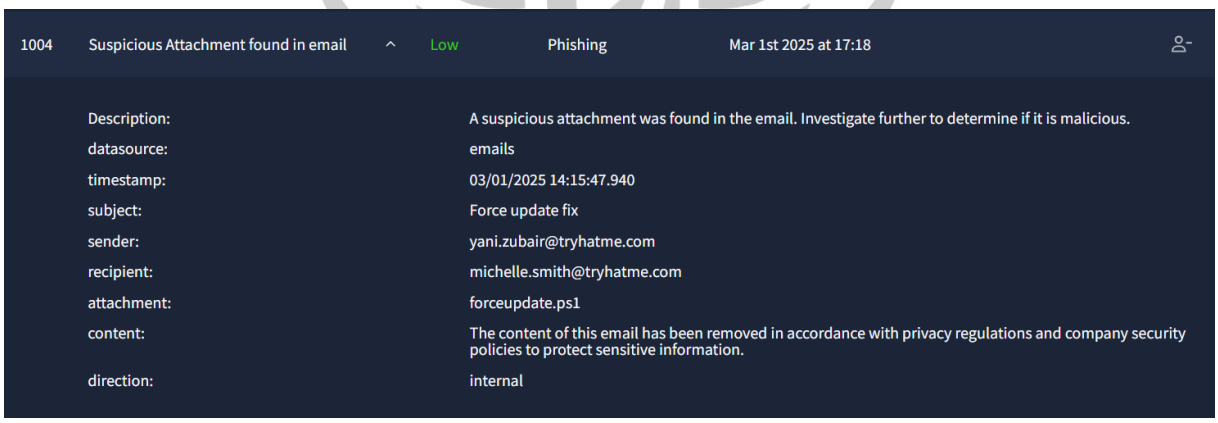
Severity: Low

Type: Phishing

Time to Resolve: 0.62 dakika

Sınıflandırma: False Positive, Bu alarm, bir kullanıcının şüpheli olarak işaretlenmiş bir e-postaya yanıt verdiğini göstermektedir. Yapılan analiz sonucunda, orijinal e-postanın güvenli olduğu belirlenmiştir, dolayısıyla bu alarm yanlış pozitif olarak sınıflandırılmıştır.

Alarm 1004: Suspicious Attachment Found in Email



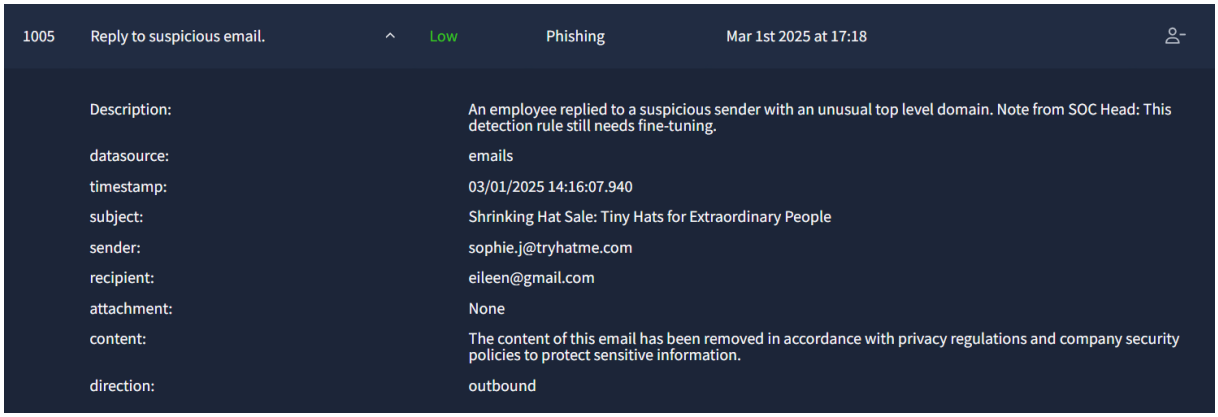
Severity: Low

Type: Phishing

Time to Resolve: 0.98 dakika

Sınıflandırma: False Positive, E-postaya eklenmiş dosya analiz edilmiş ve herhangi bir zararlı yazılım belirtisine rastlanmamıştır. Dosyanın meşru bir iş iletişiminin parçası olduğu anlaşılmıştır.

Alarm 1005: Reply to Suspicious Email



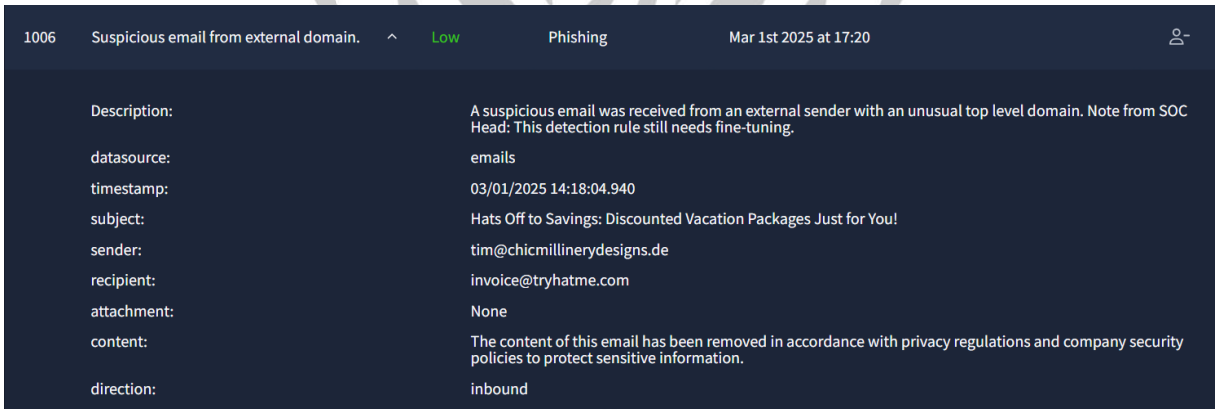
Severity: Low

Type: Phishing

Time to Resolve: 0.58 dakika

Sınıflandırma: False Positive, Kullanıcının yanıt verdiği e-posta incelenmiş ve güvenilir bir kaynaktan geldiği anlaşılmıştır. Phishing göstergesi bulunmamaktadır.

Alarm 1006: Suspicious Email from External Domain



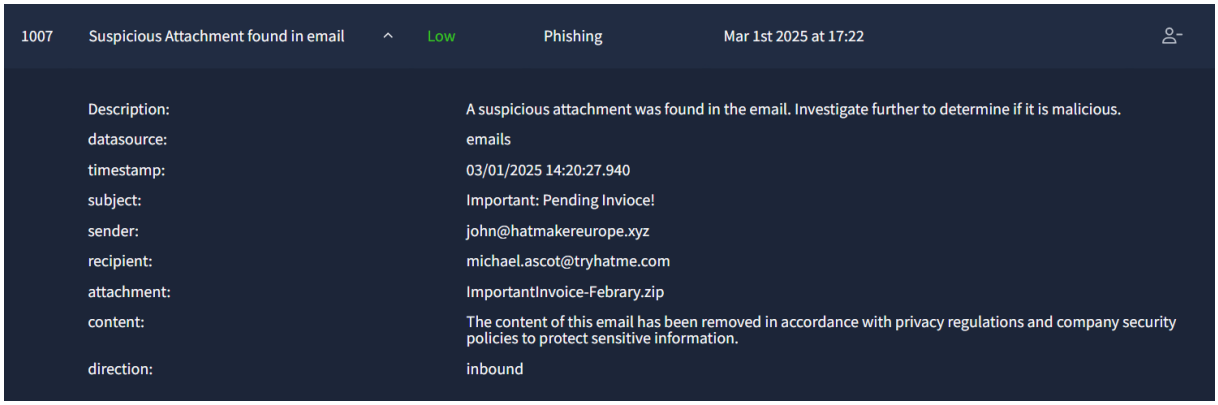
Severity: Low

Type: Phishing

Time to Resolve: 0.47 dakika

Sınflandırma: False Positive, E-posta, dış bir kaynaktan gelmiş olmasına rağmen yapılan analiz sonucunda herhangi bir tehdit unsuru taşımadığı belirlenmiştir.

Alarm 1007: Suspicious Attachment Found in Email



Severity: Low

Type: Phishing

Time to Resolve: 0.8 dakika

Sınıflandırma: True Positive, Bu alarmda, bir e-postaya eklenmiş şüpheli bir dosya tespit edilmiştir. Dosya, bilinen zararlı yazılım göstergelerine sahip olduğundan ve daha önce kara listeye alınmış bir kaynaktan geldiği için alarm doğru pozitif olarak sınıflandırılmıştır.

6. Sonuç

SOC simülasyonu, gerçek zamanlı phishing alarm analizine yönelik pratik kazandırdı ve Splunk aracı ile etkin bir şekilde güvenlik izleme yapılmasına katkı sağladı. True positive ve false positive alarmların ayırt edilmesi ve bu sınıflandırmanın log verileri ile desteklenmesi sayesinde, bir SOC analistinin sahip olması gereken araştırma ve analiz becerileri geliştirmiş oldum.