Try Hack Me SOC Simulator Introduction to Phishing (Write-Up)

Hazırlayan : Kaan Akdeniz

Tarih : 27.02.2025

İçindekiler

1.ALARM (ID 1000) 4
1. Genel Bilgiler 4
2. Olayın Tanımı 4
3. Adım Adım Çözüm 5
2. ALARM (ID 1001) 5
1. Genel Bilgiler 5
2. Olayın Tanımı 5
3. Adım Adım Çözüm 6
3. ALARM (ID 1002) 6
1. Genel Bilgiler 6
2. Olayın Tanımı 7
3. Adım Adım Çözüm 7
5. Sonuç ve Değerlendirme ..... **Error! Bookmark not defined.**
1. Genel Bilgiler 8
2. Olayın Tanımı 8
3. Adım Adım Çözüm 9
5. Sonuç ve Değerlendirme ..... **Error! Bookmark not defined.**
5. ALARM (ID 1004) 10
1. Genel Bilgiler 10
2. Olayın Tanımı 10
3. Adım Adım Çözüm 11
5. Sonuç ve Değerlendirme ..... **Error! Bookmark not defined.**
6. ALARM (ID 1005) 11
1. Genel Bilgiler 11
2. Olayın Tanımı 11
3. Adım Adım Çözüm 12
5. Sonuç ve Değerlendirme ..... **Error! Bookmark not defined.**
7. ALARM (ID 1006) 12
1. Genel Bilgiler 12
2. Olayın Açıklaması 13
3. Adım Adım Analiz Süreci 13
5. Sonuç ve Değerlendirme ..... **Error! Bookmark not defined.**

8. ALARM (ID 1007) 14
1. Genel Bilgiler 14
2. Olayın Tanımı 14
3. Adım Adım Çözüm 15
5. Sonuç ve Değerlendirme 15

Incident Report: Suspicious External Email (Phishing Attempt)

1.ALARM (ID 1000)

1. Genel Bilgiler

- **Senaryo Adı:** Harici Etki Alanından Gelen Şüpheli E-Posta
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM,VirusTotal
- **Senaryo Amacı:** Kimlik avı girişiminin tespit edilmesi, analizi ve önleyici tedbirlerin belirlenmesi.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Alçak
- **Tehdit Türü:** Kimlik Avı (Phishing)
- **Zaman Damgası:** 28 Şubat 2025, 15:54:35.654
- **Veri Kaynağı:** E-postalar
- **Gönderen:** boone@hatventuresworldwide.online
- **Alıcı:** miguel.odonnell@tryhatme.com
- **Konu:** "Hat Harikalar Diyarı'na ücretsiz bir gezi kazandınız - talep etmek için buraya tıklayın"
- **Ek:** Hiç kimse
- **İçerik:** Hassas bilgileri korumak için kaldırılmıştır.
- **Yön:** Gelen

3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SIEM üzerinde bu e-postanın izleri incelendi ve alışılmadık bir üst düzey etki alanından geldiği belirlendi.
- VirusTotal platformunda yapılan sorgulamada **hatventuresworldwide.online** alan adı, kimlik avı girişimleriyle ilişkilendirilmemiki..
- E-posta gövdesinde şüpheli bir bağlantı olduğu tespit edilemedi.

4.Sonuç

False Positive bir alarm durumu

2. ALARM (ID 1001)

1. Genel Bilgiler

- **Senaryo Adı:** Harici Etki Alanından Gelen Şüpheli E-Posta
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM, VirusTotal
- **Senaryo Amacı:** Kimlik avı girişiminin tespit edilmesi, analizi ve önleyici tedbirlerin belirlenmesi.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Alçak
- **Tehdit Türü:** Kimlik Avı (Phishing)
- **Zaman Damgası:** 28 Şubat 2025, 15:55:35.654
- **Veri Kaynağı:** E-postalar
- **Gönderen:** maximillian@chicmillinerydesigns.de
- **Alıcı:** michelle.smith@tryhatme.com
- **Konu:** "VIP Hat Resort Konaklaması: Hayalinizdeki Tatil Sizi Bekliyor, Sadece Kargo Ücreti Ödeyin"
- **Ek:** Hiç kimse

- **İçerik:** Hassas bilgileri korumak için kaldırılmıştır.
- **Yön:** Gelen

3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SIEM üzerinde e-postanın izleri incelendi ve alışılmadık bir üst düzey etki alanından geldiği belirlendi.
- Virus Total platformunda yapılan sorgulamada **chicmillinerydesigns.de** alan adının kimlik avı girişimleriyle ilişkilendirildiği görülemedi.
- E-posta gövdesinde şüpheli bir bağlantı olduğu tespit edilemedi

4.Sonuç

False Positive bir alarm durumu

3. ALARM (ID 1002)

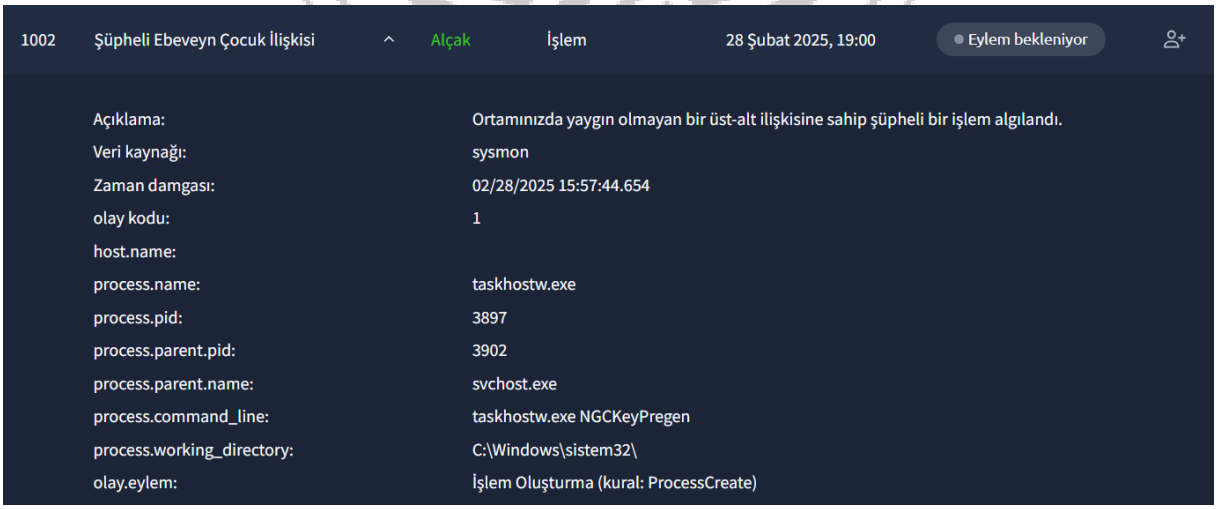
1. Genel Bilgiler

- **Senaryo Adı**: Ortamda Yaygın Olmayan Üst-Alt İlişkisine Sahip Şüpheli İşlem
- **Tarih:** 28 Şubat 2025

- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar**: SIEM, Sysmon, VirusTotal
- **Senaryo Amacı:** Şüpheli işlem yürütümünün tespit edilmesi, analizi ve önleyici tedbirlerin belirlenmesi.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Orta
- **Tehdit Türü:** Yetki Yükseltme / Süreç Manipülasyonu
- **Zaman Damgası:** 28 Şubat 2025, 15:57:44.654
- **Veri Kaynağı:** Sysmon
- **Olay Kodu:** 1
- **Olay Eylemi**: İşlem Oluşturma (ProcessCreate)
- **Etki Alanı:** Windows İşletim Sistemi
- **Etki Alanındaki Sistem:** [Belirtilmemiş]



3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SIEM ve Sysmon üzerinden taskhostw.exe sürecinin geçmişi incelendi.
- **taskhostw.exe** işleminin sistemde doğal olarak var olduğu ve belirli sistem görevlerini yönettiği doğrulandı.

- **NGCKeyPregen** parametresinin Windows Hello ve kimlik doğrulama süreçleriyle ilgili olduğu tespit edildi.
- Üst süreç olan **svchost.exe**, Windows servislerini çalıştırmak için kullanılan meşru bir işlem olarak tanımlandı.

3.2. Tehdit Avcılığı ve Olay Analizi

- **taskhostw.exe** işlemiyle ilgili imzalı kötü amaçlı yazılım verileri tehdit istihbarat veritabanlarında (VirusTotal da) araştırıldı ve herhangi bir kötü amaçlı etkinlik tespit edilmedi.
- Çalıştırılan komutun, Microsoft'un kimlik doğrulama yönetim sürecinin bir parçası olduğu belirlendi.
- Aynı olayın daha önce benzer sistemlerde de meydana geldiği görüldü.

3.3. False Positive Olduğunun Belirlenmesi

- **taskhostw.exe**, Windows'un standart bir bileşeni olup, kötü amaçlı bir faaliyet göstermediği için False Positive olarak değerlendirildi.
- Bu olayın, alarm tetikleme kurallarının fazla duyarlı olması nedeniyle ortaya çıktığı tespit edildi.

4.Sonuç

False Positive bir alarm durumu

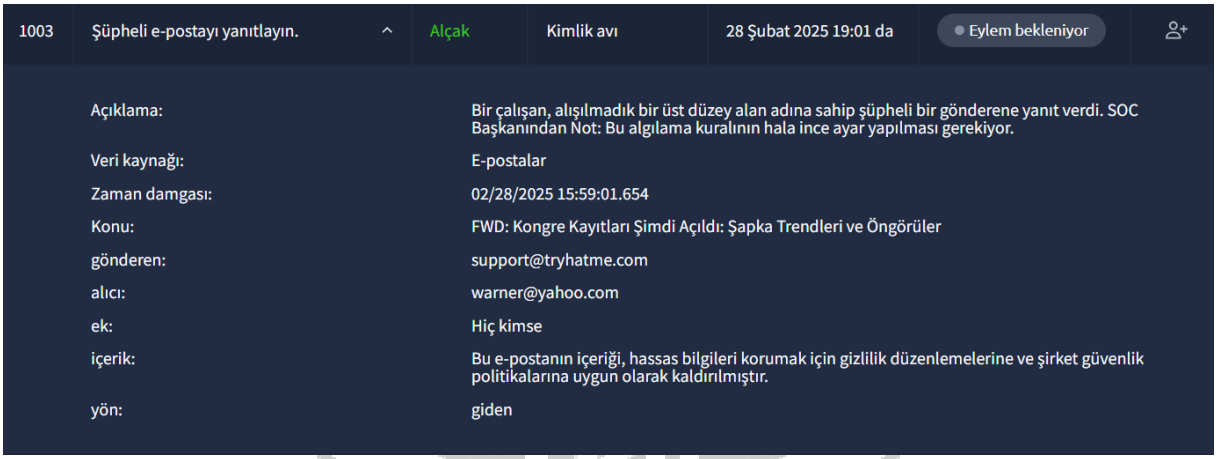
1. Genel Bilgiler

- **Senaryo Adı:** Şüpheli Gönderene Yanıt Verilmesi
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM, VirusTotal, Threat Intelligence Platform
- **Senaryo Amacı:** Potansiyel kimlik avı saldırısının tespiti, analizi ve önleyici tedbirlerin belirlenmesi.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Orta
- **Tehdit Türü:** Kimlik Avı / Sosyal Mühendislik
- **Zaman Damgası:** 28 Şubat 2025, 15:59:01.654

- **Veri Kaynağı:** E-postalar
- **Olay Yönü:** Giden
- **Konu:** FWD: Kongre Kayıtları Şimdi Açıldı: Şapka Trendleri ve Öngörüler
- **Gönderen:** support@tryhatme.com
- **Alıcı:** warner@yahoo.com
- **Ek Durumu:** Hiç kimse
- **İçerik:** Gizlilik düzenlemeleri ve güvenlik politikalarına uygun olarak kaldırılmıştır.



3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SOC ekibi, SIEM üzerinden bu olayla ilgili e-posta trafiğini inceledi.
- Gönderen alan adı ve e-posta içeriği analiz edildi.
- **support@tryhatme.com** adresinden gelen e-postanın önceki tehdit istihbaratıyla eşleştirilip eşleştirilmediği kontrol edildi.
- Kullanıcının bilinçli bir şekilde mi yoksa yanlışlıkla mı yanıt verdiği değerlendirildi.

3.2. Tehdit Avcılığı ve Olay Analizi

- Alıcı adresi **warner@yahoo.com** sorgulandı ve potansiyel kötü niyetli bir alan adı olup olmadığı incelendi.
- E-posta içeriğinde kimlik avı belirtileri olup olmadığı araştırıldı.
- Kullanıcının gönderdiği yanıtın hassas bilgileri içerip içermediği değerlendirildi.

4.Sonuç

False Positive bir alarm durumu

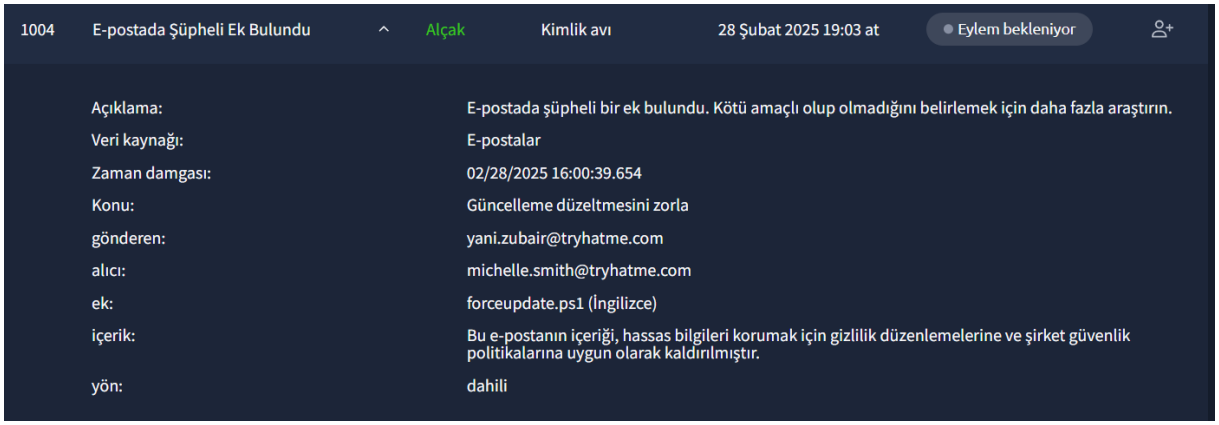
5. ALARM (ID 1004)

1. Genel Bilgiler

- **Senaryo Adı:** Şüpheli Ek İçeren E-Posta
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM, VirusTotal, Sandboxing
- **Senaryo Amacı:** Şüpheli bir e-posta ekinin kötü amaçlı olup olmadığının belirlenmesi ve önleyici tedbirlerin alınması.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Yüksek
- **Tehdit Türü:** Kötü Amaçlı Yazılım / Kimlik Avı
- **Zaman Damgası:** 28 Şubat 2025, 16:00:39.654
- **Veri Kaynağı:** E-postalar
- **Olay Yönü:** Dahili
- **Konu:** Güncelleme Düzeltmesini Zorla
- **Gönderen:** yani.zubair@tryhatme.com
- **Alıcı:** michelle.smith@tryhatme.com
- **Ek:** forceupdate.ps1
- **İçerik:** Gizlilik düzenlemeleri ve güvenlik politikalarına uygun olarak kaldırılmıştır.



3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SIEM üzerinden e-posta loglarını inceledi.
- **forceupdate.ps1** ekinin kötü amaçlı olabileceği ihtimali değerlendirildi.
- Gönderen e-posta adresi analiz edilerek tehdit istihbaratı veritabanlarıyla karşılaştırıldı.

3.2. Tehdit Avcılığı ve Olay Analizi

- **forceupdate.ps1** eki izole bir ortamda (sandbox) çalıştırılarak davranış analizi yapıldı.
- Ekte zararlı komutlar olup olmadığı incelendi.
- Ek, virüs tarama ve dinamik analiz araçları ile değerlendirildi.

4.Sonuç

False Positive bir alarm durumu

6. ALARM (ID 1005)

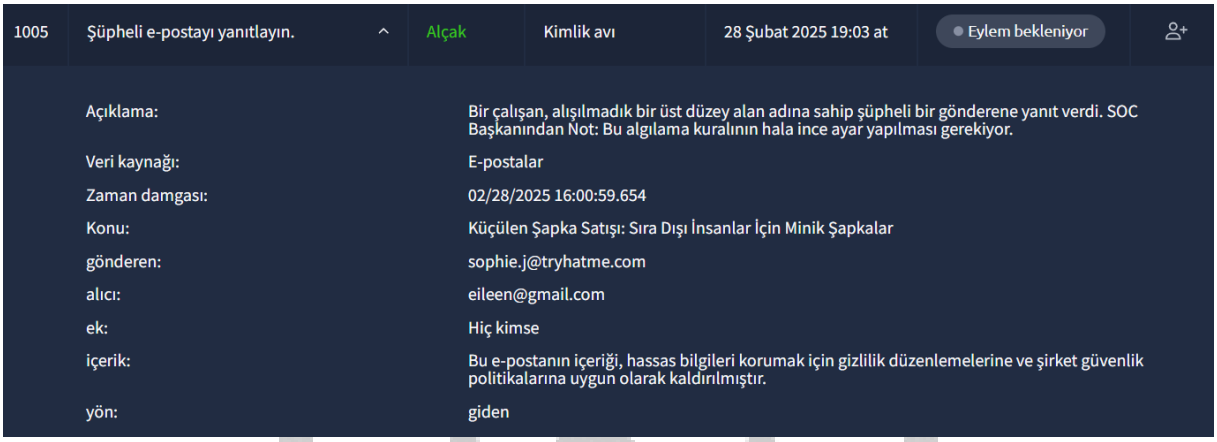
1. Genel Bilgiler

- **Senaryo Adı:** Şüpheli Ek İçeren E-Posta
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM, VirusTotal, Threat Intelligence Platform, Sandboxing
- **Senaryo Amacı:** Şüpheli bir e-posta ekinin kötü amaçlı olup olmadığının belirlenmesi ve önleyici tedbirlerin alınması.

2. Olayın Tanımı

- **Tehdit Seviyesi:** Yüksek
- **Tehdit Türü:** Kötü Amaçlı Yazılım / Kimlik Avı
- **Zaman Damgası:** 28 Şubat 2025, 16:00:39.654
- **Veri Kaynağı:** E-postalar

- **Olay Yönü:** Dahili
- **Konu:** Güncelleme Düzeltmesini Zorla
- **Gönderen:** yani.zubair@tryhatme.com
- **Alıcı:** michelle.smith@tryhatme.com
- **Ek:** forceupdate.ps1 (İngilizce)
- **İçerik:** Gizlilik düzenlemeleri ve güvenlik politikalarına uygun olarak kaldırılmıştır.



3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SOC ekibi, SIEM üzerinden e-posta loglarını inceledi.
- **forceupdate.ps1** ekinin kötü amaçlı olabileceği ihtimali değerlendirildi.
- Gönderen e-posta adresi analiz edilerek tehdit istihbaratı veritabanlarıyla karşılaştırıldı(VirusTotal da).

4.Sonuç

False Positive bir alarm durumu

7. ALARM (ID 1006)

1. Genel Bilgiler

- **Olay Adı:** Şüpheli Harici E-Posta Alımı
- **Tarih:** 28 Şubat 2025

- **Hazırlayan:** Kaan Akdeniz
- **Veri Kaynağı:** VirusTotal, SIEM
- **Tehdit Seviyesi:** Düşük
- **Tehdit Türü:** Potansiyel Kimlik Avı (Phishing)

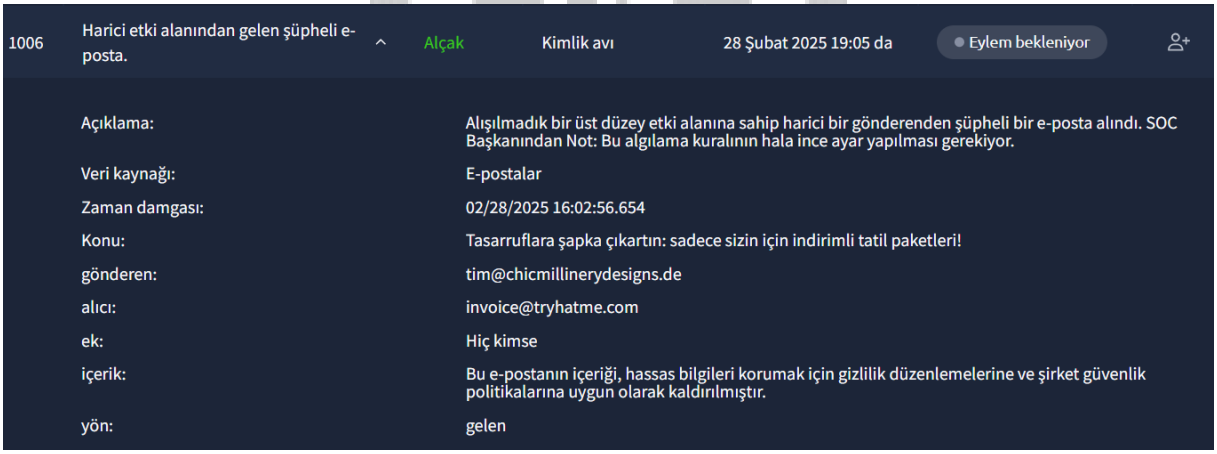
2. Olayın Açıklaması

2.1. Olay Detayları

- **Zaman Damgası:** 28 Şubat 2025, 16:02:56.654
- **Konu:** Tasarruflara Şapka Çıkartın: Sadece Sizin İçin İndirimli Tatil Paketleri!
- **Gönderen:** tim@chicmillinerydesigns.de
- **Alıcı:** invoice@tryhatme.com
- **Ek:** Yok
- **Yön:** Gelen

2.2. Olası Tehditler

- Gönderen, bilinmeyen bir üst düzey alan adına (.de – Almanya) sahip ve şirket içinden bir çalışana e-posta göndermiş.
- Konu satırı, sosyal mühendislik kullanarak alıcıyı kandırmaya yönelik gibi görünüyor.
- Ek içermese de, gövde içeriği şüpheli bağlantılar içerebilir.



3. Adım Adım Analiz Süreci

3.1. İlk İnceleme

- SIEM üzerinde e-posta logları tarandı ve olayın kaydı doğrulandı.
- Gönderen adresi tehdit istihbarat veri tabanlarında arandı.

- E-postanın içeriği, kimlik avı unsurları açısından incelendi.

3.2. Risk Değerlendirmesi

- Kullanıcı bu e-postaya tıklamış mı veya yanıt vermiş mi kontrol edildi.
- Bu alan adına daha önce benzer e-postalar gönderilmiş mi araştırıldı.
- İçerikte herhangi bir kötü amaçlı bağlantı olup olmadığı tespit edilmeye çalışıldı.

4.Sonuç

False Positive bir alarm durumu

8. ALARM (ID 1007)

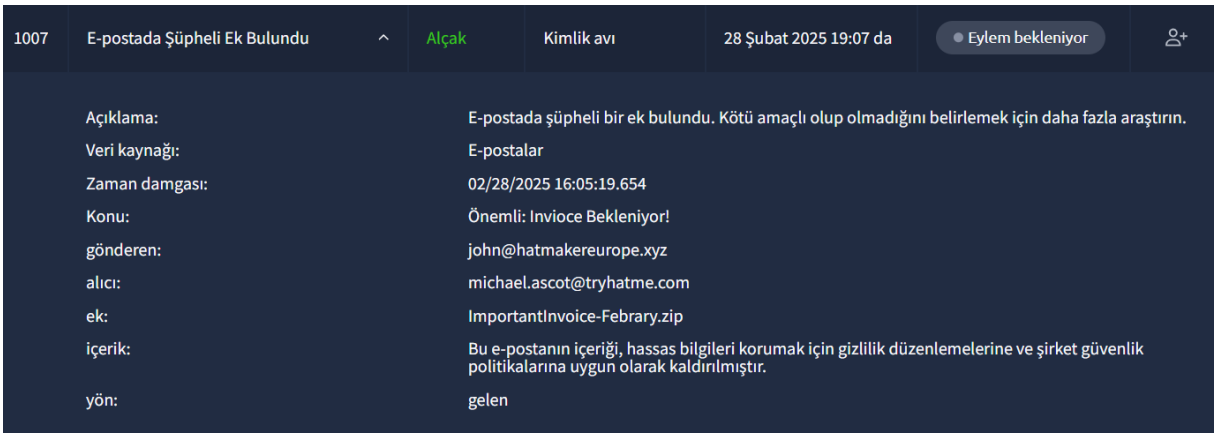
1. Genel Bilgiler

- **Senaryo Adı:** Şüpheli Ek İçeren E-Posta
- **Tarih:** 28 Şubat 2025
- **Hazırlayan:** Kaan Akdeniz
- **Kullanılan Araçlar:** SIEM, VirusTotal, Threat Intelligence Platform, Sandboxing
- **Senaryo Amacı:** Şüpheli ek içeren e-postaların incelenmesi ve zararlı olup olmadıklarının belirlenmesi.

2. Olayın Tanımı

Olay: Şüpheli Ek İçeren E-Posta

- **Tehdit Seviyesi:** Yüksek
- **Tehdit Türü:** Kötü Amaçlı Yazılım / Kimlik Avı
- **Zaman Damgası:** 28 Şubat 2025, 16:05:19.654
- **Veri Kaynağı:** E-postalar
- **Olay Yönü:** Gelen
- **Konu:** Önemli: Invoice Bekleniyor!
- **Gönderen:** john@hatmakereurope.xyz
- **Alıcı:** michael.ascot@tryhatme.com
- **Ek:** ImportantInvoice-Febrary.zip
- **İçerik:** Gizlilik düzenlemeleri ve güvenlik politikalarına uygun olarak kaldırılmıştır.



3. Adım Adım Çözüm

3.1. İlk Analiz ve Log İnceleme

- SOC ekibi, SIEM üzerinden e-posta loglarını inceledi.
- **ImportantInvoice-Febrary.zip** ekinin kötü amaçlı olabileceği ihtimali değerlendirildi.
- Gönderen e-posta adresi tehdit istihbaratı veritabanlarıyla karşılaştırıldı.

3.2. Tehdit Avcılığı ve Olay Analizi

- Ek, virüs tarama ve dinamik analiz araçları ile değerlendirildi.
- ZIP dosyası içeriğindeki herhangi bir çalıştırılabilir dosya olup olmadığı incelendi.

5. Sonuç

Positive bir alarm durumu