TryHackMe
SOC
SİMÜLATÖR

Hazırlayan: Şevval Kömeç
Tarih: 28.02.2025

Introduction to Phishing Simülatör

Phishing simülasyonuna giriş yapılmıştır. Sol menüden "Uyarı Kuyruğu" bölümüne girilmiş ve gelen uyarılar incelenmeye başlanmıştır. Burada, tüm vakaların güvenlik seviyesi sınıflandırması düşük olup, şüpheli ebeveyn çocuk ilişkisi dışında kalan tüm uyarılar phishing tipindedir. Sol menüde araştırmaların yapılabileceği SIEM ve Sanal Makine Analizi kategorileri bulunmaktadır. SIEM içerisinde Splunk kullanılmaktadır. Alarm kuyruğundaki vakaları kronolojik sırayla incelemek için en alttan yukarıya doğru bakılması gerekmektedir.

Vaka İncelemeleri

1. Vaka: Harici Etki Alanından Şüpheli E-posta

- Tanım: Harici bir göndericiden, alışılmadık bir üst düzey alan adına (TLD) sahip şüpheli bir e-posta alındı. SOC Başkanı'nın Notu: Bu tespit kuralı hâlâ ince ayar gerektiriyor.

Vakanın sahipliği alınarak incelemeye başlanır. Ek dosya mevcut değildir. Sadece herkesin çevrimiçi olarak kullanabileceği .online uzantılı bir domain bulunmaktadır.

1. Splunk arama çubuğuna "haventuresworldwide.online" yazılarak arama yapılır. Herhangi bir şüpheli durum görülmez.
2. VirusTotal üzerinde domain kontrol edilir ve negatif bir sonuç bulunmaz.

Bu alarmın false pozitif olduğu belirlenir. Vaka raporuna açıklama girilerek false pozitif olarak işaretlenir ve gönderilir. Alarm kapanarak "Kapalı Alarmlar" kategorisine taşınır.

2. Vaka: Harici Etki Alanından Şüpheli E-posta

- Tanım: Harici bir göndericiden, alışılmadık bir üst düzey alan adına (TLD) sahip şüpheli bir e-posta alındı.
- Konu: Tatil reklamı.

1. Ek dosya bulunmaz.
2. Domain VirusTotal üzerinden kontrol edilir ve herhangi bir giriş tespit edilmez.
3. Vaka, domain ve göndericinin kötü amaçlı olmadığı açıklanarak false pozitif olarak işaretlenir ve raporlanır.

3. Vaka: Şüpheli Ebeveyn-Çocuk İlişkisi

"Şüpheli Ebeveyn-Çocuk İlişkisi" terimi, bir işlem veya süreç hiyerarşisinde olağandışı veya beklenmedik bir ilişkiyi ifade eder. Bu, genellikle kötü amaçlı yazılım faaliyetleri veya yetkisiz erişim gibi güvenlik tehditlerinin göstergesi olabilmektedir.

Vakadaki işlemler:

- Process Name: taskhostw.exe
- Parent Process: svchost.exe

İşlem Açıklamaları:

- taskhost.exe, Windows'un arka planda çalışan ve DLL'leri yükleyerek çalışmasını sağlayan bir sistem işlemidir.
- svchost.exe, birden fazla Windows hizmetini çalıştıran sistem işlemidir.

1. Splunk üzerinde Process ID üzerinden arama yapılır, şüpheli bir durum tespit edilmez.
2. Daha spesifik aramalar yapılır, ancak işlemler normal gözükmektedir.

Vakanın false pozitif olduğu belirlenir ve "Belirtilen işlemler arasındaki ilişki normaldir." açıklaması ile vaka raporlanır.

4. Vaka: Şüpheli Maillere Cevap Verme

- Tanım: Bir çalışan, alışılmadık bir üst düzey alan adına sahip şüpheli bir göndericiye yanıt verdi.

1. Gönderici domaini Yahoo uzantılıdır ve yazım hatası bulunmamaktadır.
2. Ek dosya bulunmaz.
3. Alarm false pozitif olarak işaretlenerek raporlanır.

5. Vaka: Şüpheli E-posta Eki Bulundu

- Gönderen & Alıcı Domainleri: tryhateme uzantılı.
- Ek Dosya: "Güncellemeye Zorla" adlı bir dosya.

Dosya, Sanal Makine Analiz bölümünde incelenir.

- İçeriğinde, Windows'un güncellenmesi gerektiğini belirten açıklamalar bulunur.
- Bunun bir bilgilendirme e-postası olduğu anlaşılır.

Vaka false pozitif olarak işaretlenerek raporlanır.

6. Vaka: Şüpheli Maile Cevap Verme

- Konu: Küçülen Şapka Satışı: Olağanüstü İnsanlar için Minik Şapkalar Merkez Organizasyonu
- Gönderen Domainleri: Gmail ve tryhateme

1. Herhangi bir şüpheli durum görülmez.
2. Ek dosya bulunmaz.

Alarm false pozitif olarak işaretlenerek bildirilir.

7. Vaka: Harici Bir Domainden Şüpheli Mail

- Gönderen Domaini: tim@chicmillinerydesigns.de

  Gönderici domaini daha önce incelediğimiz yerden.

- Ek Dosya: Yok.

Vaka false pozitif olarak işaretlenerek gönderilir.

8. Vaka: Mailde Şüpheli Ek Bulundu

- Gönderen: john@hatmakereurope.xyz
- Alıcı: michael.ascot@tryhatme.com
- Konu: Bekleyen Fatura Maili.
- Ek Dosya: ImportantInvoice-Febrary.zip

İnceleme Süreci:

1. Dosya Sanal Makine Analiz bölümünde incelenir.
2. PowerShell üzerinden SHA-256 ve MD5 hash değerleri alınarak VirusTotal üzerinde kontrol edilir. Şüpheli bir sonuç bulunmaz.
3. Splunk üzerinde dosya ismi ve gerçek adıyla arama yapılır, sonuç bulunamaz.

Ancak dosya hâlâ şüpheli olduğu için zaman taramalı araştırma yapılır:

- Mailin gönderilme zamanından itibaren olaylar incelenir.
- PowerShell başlatan bir olay tespit edilir.
- explorer.exe, fatura dosyasını açmıştır.
- outlook.exe çalıştırıldıktan sonra powershell.exe başlatılmıştır.
- PowerShell komutunda şüpheli bir kod tespit edilir:
    - GitHub'dan powercat.ps1 indirilmiş.
    - ngrok.io üzerinden C2 bağlantısı kurulmuş.

Vaka Değerlendirmesi:

- True Pozitif olarak işaretlenir.
- Durum Raporu:

Saldırgan, GitHub'dan powercat.ps1 indirdi ve ardından ngrok kullanarak bir C2 (Command and Control) kurdu. whoami.exe ve systeminfo.exe gibi komutları çalıştırarak sistemi numaralandırdı. Ele geçirilen makinedeki dosya paylaşımlarını haritaladı ve finansal kayıtların bulunduğu bir paylaşım keşfetti. robocopy.exe kullanarak bu paylaşımı ediltsime.zip adlı bir dosyaya aktardı. Son olarak, videokap.exe kullanarak DNS veri toplama işlemlerini gerçekleştirdi.