Siber Güvenlik Saldırılarına Dair

Siber güvenlik saldırılarını ve çeşitlerini kapsamaktadır.

Ümmü Gülsüm Varlı

İçindekiler

Siber Güvenlik Saldırıları:

1. Siber Güvenlik Saldırısı Nedir?

Siber Güvenlik saldırısı bir ya da birden fazla makineye saldırı yöntemine göre savaş açmak datalarını bozmak, verilerini çalmak ya da üzerinde yapılan en ufak değişikliklerin tamamıdır. Siber Güvenlik saldırıları çok çeşitli olup sınıflandırılmaya müsait kapsamlı bir disiplindir. Her ne kadar çok fazla güvenlikli olduğuna inandığınız makinelerde de olsanız siber güvenlik saldırısı başarılı ya da başarısız şekilde her zaman denenmeye müsaittir. Sistemin olduğu her yerde açıkta mevcuttur. Siber güvenlik saldırıları da sistemlerin açıklarını kullanarak, bularak çeşitli toollar, yöntemler, kötü amaçlı yazılımlar ile saldırılmasıdır. Unutmamalıyız ki her zaman potansiyel hedefler mevcuttur ve mevcut olmaya devam edecektir.

Peki nedir bu siber güvenlik saldırı çeşitleri ve biz bunlardan korunamaz mıyız?

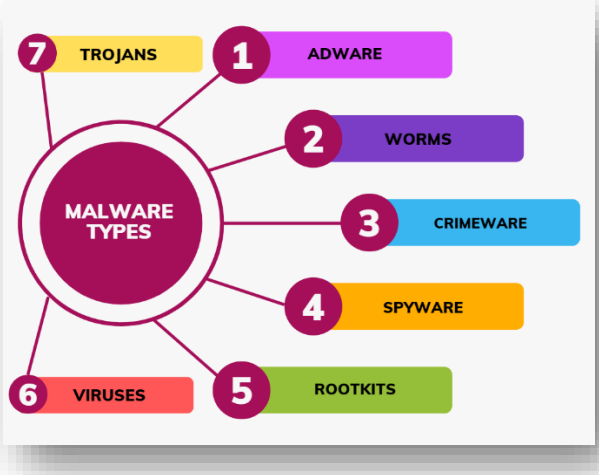
Elbette bir sürü saldırı çeşidi ve korunma yöntemi mevcuttur.

2. Siber Güvenlik Saldırı Çeşitleri:

Siber güvenlik saldırı çeşitleri çok çeşitli olmasına karşın en önemlileri şeklinde sıralanmaya çalışıldığında *Malware (kötü amaçlı yazılım), Phishing (oltalama), DDoS ve DoS, SQL Injection ,* Cryptojacking , Password Attacks (şifre saldırısı) , Supply Chain Attack – Tedarik Zinciri Saldırısı, *Eavesdropping Attack – Telekulak / Gizli Dinleme Saldırısı, Zero Day Exploit - Sıfır Gün Açığı,* Man in the Middle olarak sıralanabilir.

2.1. Malware (kötü amaçlı yazılım):

Dünya genelinde en kötü amaçlı yazılım olarak bilinen türdür. Farklı sızma yöntemleri ile elektronik cihazlarınıza sızarak cihazları etkisiz hale ya da sizi etkisiz hale getirmede yeterince başarılı bir türdür. Gerek reklam yoluyla gerek dosya ya da link yoluyla gerek kendini kopyalayarak cihazınızı etkisiz hale getirme yoluyla ya da tüm özel bilgilerinizi sizi ciddi manada tehlikeye sokabilir. Bu yüzden *malware* yazılımları kesinlikle kaçınılması gereken yazılım türlerindendir.



2.1.1. Adware Yazılım*:*

Saldırganın kullanıcıdan izin almadan yetkisiz girmesi ya da girmemesi gereken yerlere bilgisayar ya da mobil cihazlar yoluyla sızarak arka planda aktif olarak çalışan reklam yazılımları olarak tanımlanır. Adware yazılımları sadece kuruldukları makinede aktif olarak işlem yapabileceğinden virüs olarak değerlendirilmez. Arka planda çalışarak sisteme ağır hasarlar yükleyebilen kötü amaçlı yazılım türüdür. Web sayfaları ya da ücretsiz yazılım indirme yolu ile bulaşabilir. Bu nedenle güvenmediğiniz sitelerden bir şey indirmemeniz tavsiye edilir.

Adware yazılımdan korunmak için güvenilir web sitelerini tercih etmek ve kullandığınız cihazlarda anti-virüs yazılımı kullanmak korunmanıza yardımcı olacaktır.

2.1.2. Worms:

Worms, yani solucanlar virüslerden farklı olarak kendini kopyalayıp çoğalabilen kötü amaçlı yazılım türlerindendir. Solucanlar, bir bilgisayardan başka bilgisayara kopyalanmak için kullanılırlar. Solucanlar çok kısa sürede herhangi bir eyleme gerek duymadan çok hızlı bir şekilde yayılabilirler. Bu da DDoS saldırısına benzer olarak trafiği yavaşlatır ve cihazınızı işlevsiz hale getirebilir. Sunucular(servers) bu trafiği kaldıramayabilir bu da sistemi etkisiz hale getirir. Solucanlar genelde e-posta yoluyla ya da güvenilir olmayan, belirsiz sitelerden bulaşabilir.

Örneğin internetteki solucan örneklerine değinecek olursak;

- Tebrikler! Amerika'ya ücretsiz vize hakkı hazandınız.
- Sitemize giren 10.000. kişisiniz bu yüzden size İPhone hediye ediyoruz.

Genelde sosyal medya hesaplarınıza gelen linklerde solucanlar bulunur ve siz bu linklere tıkladığınızda arka planda URL ya da IP adresine gönderir ve oradan bilgilerinizi ele geçirebilir ya da üstünüzden para kazanabilirler-aklayabilirler.

2.1.3. Crimeware:

Crimewareler, siber suçları otomatikleştirmek için tasarlanan yazılımlardandır. Daha çok sosyal mühendislik ile ilgilenen kişilerin kullandığı kötü amaçlı yazılımlardandır. Ağ güvenliğini sarsabilir, verilerinizi ele geçirebilir ve banka hesaplarınıza erişerek size büyük kayıplar yaşatabilir. Kötü amaçlarla girilmemesi gereken ağlara uzaktan erişim sağlayabilir, hassas verilerinize ulaşarak değiştirebilir, fidye ödemesi isteyerek şantaj yaptırılabilir yani ciddi manada dikkat edilmesi gereken kötü amaçlı yazılım türlerindendir.

Bu tarz durumlardan kendinizi koruyabilmek için güvenlik yazılımı yükleyebilir, işletim sisteminize güvenlik yamaları ekleyebilir ve sitelerdeki kişisel metinleri okuyarak onaylayabilirsiniz.

2.1.4. Spyware:

Casus yazılımlar, şirketlerin, kurum-kuruluşların neredeyse en çok canını sıkan kötü amaçlı yazılımlardandır. Casus yazılımlar, cihazlarınızdan gizlice veri toplayabilirler. Bilgisayarınızdaki şifreleri kaydedebilir, ekran görüntüsü alabilirler. Ayrıca bu yazılımlar sadece Windows ile sınırlı kalmayıp Mac bilgisayarlarınıza da sızabilirler. Sitenizi hackleyerek siteyi kapalı hale getirerek kötü hizmet sunabilirler. Kullanıcı verilerini sızdırarak çok daha büyük hasarlar bırakabilirler. Aslına bakılırsa korunma noktasında henüz güçlü bir şey yok denebilir çünkü çok fazla potansiyel spyware aracı-toolu mevcut olup potansiyel minimum düzeyden fazladır. O yüzden her zaman verilerinizi bir yerde yedekli bir şekilde saklayın.

2.1.5. Rootkits:

Root, "ayrıcalıklı kontrol sistem yetkisine" sahip olan Linux ve Unix'ten gelmekte olup kit "yönetici düzeyinde erişim" anlamını karşılar. Yani her şeye sahip olabilir ağlara erişerek verilere erişebilir DDoS saldırısı başlatabilirler.

Kök kullanıcı tanımı, adından yola çıkıldığı üzere bir şeyin kökünde var olmuş gibi göstererek gizlenerek o cihazda yaşamaya çalışır. Amacı kendini kopyalamak ya da çoğalmak değildir, bulunduğu cihazda gizli bir şekilde yaşayabilmektir. En güçlü kötü yazılım türlerindendir. Sistem çekirdeğine kadar ulaşıp kendilerini yamalayabilirler.

Ayrıca sistem çekirdeğine kadar ulaşabildiği için de sadece yazılımsal veri anlamda çöküşle yetinmeyip donanımsal hasarlarda bırakır. Kaynağından emin olmadığınız belge, dosya, linkler rootkit bulaştırabilirler. Sosyal mühendislik avında olanlar kimlik bilgilerinize erişmek isteyerek rootkit yazılımını kullanabilirler, bu yüzden kurum-kuruluşların kullandığı her şeyde penetrasyon testlerini düzenli olarak takip etmesi gerekmektedir.

3 tip rootkit bulunmaktadır. Bunlar kernel (çekirdek), bootloader (önyükleyici) ve memory (bellek) sıralanalabilir.

a) Kernel(çekirdek): Bilgisayarınızın çekirdeğine ulaşıp işletim sisteminizin işleyişini ve çalışma düzenini değiştirir.
b) Bootloader(önyükleyici): Bootloader rootkit, önyükleyiciden önce sahte bir işletim sistemi yükler ve ardından normal işletim sistemi ile değiştirir. Bu şekilde aktif hale gelerek işletim sistemini ele geçirir.
c) Memory(bellek): Bilgisayarın ROM yani kalıcı bölgesine değil de RAM bölgesinde yer almaya çalıştığından kalıcı olarak bilgisayarda yer alamaz. ROM belleğinde silinecektir. Bilgisayarın arka planında ROM bölgesinde çalıştığından bilgisayarın performansını düşürür fakat bilgisayar yeniden başlatınca ROM kendini yenilendiğinden yok olacaktır.

2.1.6. Viruses(Virüsler):

Kullanıcı izni olmadan cihaza erişim sağlayıp çalışma şeklini değiştirip, saklanan kötü amaçlı yazılım programlamalarıdır denilebilir. Kötü amaçlı yazılımların virüs kategorisinde olması için kendi kendini kopyalayabilmeli ve kendini çalıştırabilmelidir.

Virüsleri kendi aralarında kategorize etmeye çalışırsak önemlileri bakımından makro-virüsler, dosya-virüsleri, ağ-virüsleri, yazılım bombaları, xss/cross site scripting virüsleri şeklinde ayrılabilirler.

- Makro-virüsler, makro program içeren yerlerde bulunabilirler. Office programları gibi.
- Dosya-virüsleri, yürütülebilir dosyalara konak şeklinde tutunup çalıştırıldığında aktifleşip çalışan virüslerdir.
- Ağ-virüsleri, önce ağa sızmaya çalışır ardından potansiyel hedeflere de sızmaya çalışırlar. Yerel ağlarda, internette hızla yayılabilirler.
- Yazılım-bombaları, kodlamaya göre gerekli şartlar oluştuğunda uygun ortamda harekete geçip aktifleşirler.

2.1.7. Trojan:

Trojanlar, veri silebilir, engelleyebilir, değiştirebilir, kopyalayabilir, cihazların performansını düşürebilirler. Kendi kendilerine çoğalamazlar, kendi başlarına işlem yapılamazlar. Saldırgan ya da bir kullanıcı tarafından başlatılmayı beklerler. Truva atı zararlı yazılım yükleyen bir bilgisayar programıdır.

En basit örneklerinden biri “Waterfalls.scr” isimli programdır. Bu program çalıştırıldığında truva atı aktif hale gelir. Program ise size başta yüklediğinizde bedava ekran koruyucu vereceğini vadeder.

Truva atları, sistemde nasıl hasar açabildiklerine göre sınıflandırılırlar. Bu şekilde sınıflandırma sağlandığında 7 ana tür truva atı ortaya çıkıyor.

1. Remote Access- Uzaktan Erişim
2. Email Sending – E-posta gönderme
3. Data destruction – Veri Yıkımı
4. Proxy Trojan – Proxy Truva: Zararlı bulaşmış sistemi saklar.
5. Ftp Trojan – Ftp Truva: Zararlı bilgisayardan dosya ekleme ya da yakalama işlemini yapar.
6. Güvenlik yazılımlarını devre dışı bırakma
7. DDoS Attacks – DDoS Saldırıları
8. URL Trojan – URL Truva olarak sınıflandırılırlar.

2.1.7.1. Bu truva atları bu saldırılarla nelere zarar verebilirler?

- Dosyaları "cryptoviral extortion" yani " kriptoviral alıkoyma " yöntemi ile şifreleyebilirler.
- Dosyaları şifreleyebildikleri gibi zarar verebilirler.
- Verileri silip, üzerine yazabilirler.
- Bilgisayar kamerasını ele geçirip kullanıcının fotoğrafını çekebilirler.
- Kullanıcı bilgisayara uzaktan erişim sağlayabilirler. (RAT- Remote Access Trojan)
- Güvenlik duvarınıza(firewall) zarar verebilir, devre dışı bırakabilirler.
- Spam e-posta göndermek için e-posta toplayabilirler.
- Şifrelerinizi "keylogger" yöntemi ile kaydedip çalabilirler.
- Memory(bellek) üzerinde gizli şekilde çalışabilirler.

2.1.7.2. Truva Atından korunma yolları:

- Local network (yerel ağ) paylaşan programları kullanmayın.
- Tanımadığınız birinden gelen e-postalarınıza açmadan önce tarayın. Gönderen kişinin gönderdiği kaynağını araştırın.
- Bilgisayarınızda anti-virüs programı bulundurun. Güncelleştirme takibi yapın.
- İşletim sistemleri bilgisayarlara gelen güncellemelerde virüsleri de dikkate alarak güncelleme sağlarlar. Bu yüzden işletim sistemi güncelleştirmelerinizi takip edin.

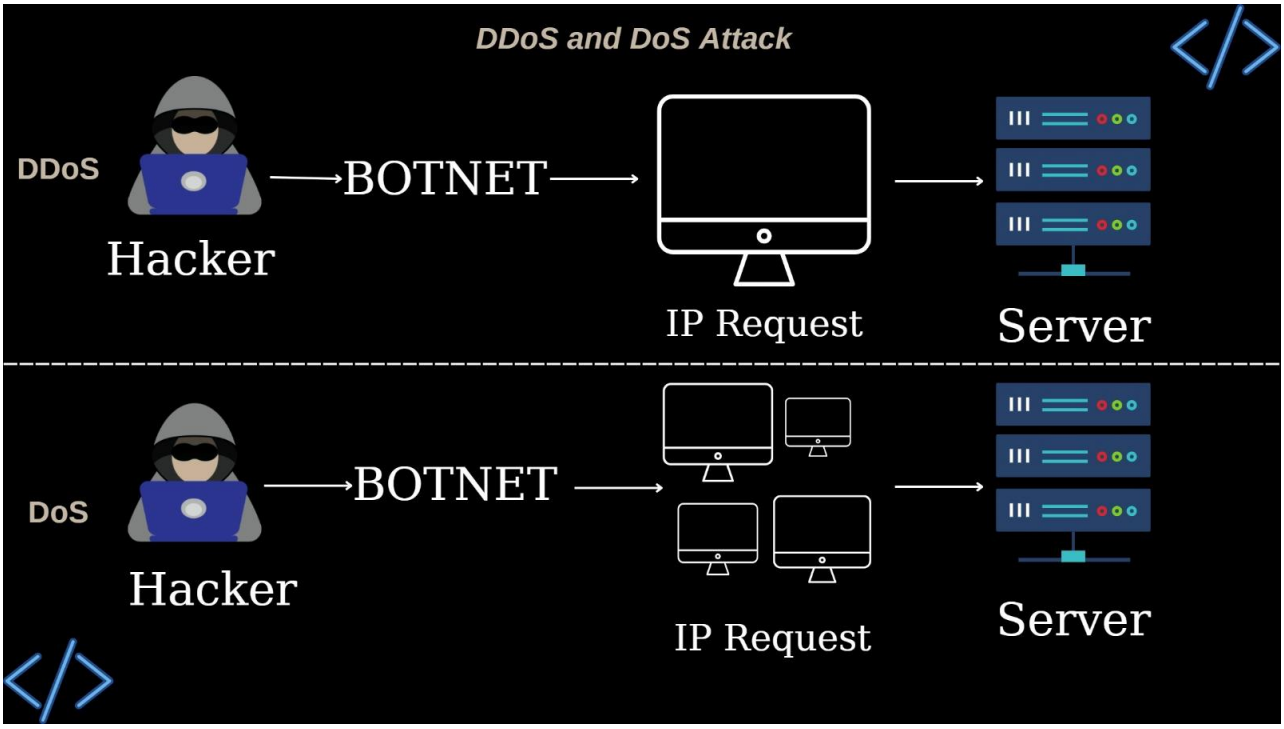
Truva atları, genellikle hileli programlarla bulaşır. O yüzden bilinmedik hiçbir şeyin açılmaması tavsiye edilir. Çünkü bir resmin, linkin içinde solucan ya da truva atı olabilir ve siz açtığınız anda program aktifleşir.

2.2. Phishing (oltalama):

Phishing saldırıları duyumları çok yaygınlaşmasına karşın hala bilmeyenlerin en büyük düşmanı olarak nitelendirilebilir. Genelde oltalama saldırısında sızma yöntemi çok basit ve klasiktir. E-posta ya da link yolu ile sizi inandırmak istediği şeye inandırarak sizden istenileni alır. Bu yüzden e-postalara gelen şeylere dikkat edilmeli ve resmi e-postalar hakkında bilgi sahibi olunmalıdır ki e-posta ayrımı rahatlıkla yapılabilsin. Neredeyse bilinen en eski saldırı yöntemi olduğundan geçmişe göre artık insanlar bu saldırı konusunda daha bilinçlidir.

2.3. DDoS ve DoS:

Siber suçlu, potansiyel hedefe çok sayıda istek göndermek için genellikle virüs yaydığı bilgisayarlardan oluşan bir "*zombi ağı*" kurar. Sunucuya(server) çok fazla istek göndererek trafiği kilitleyerek sistemlerin çalışmasını engeller. İnternete bağlı olan bilgisayarın sunmuş olduğu hizmetleri aksatmayı ya da durdurmayı hedefler. Geçmişten günümüze en çok karşılaşan siber saldırı tiplerindendir. DoS, servis dışı bırakma olarak adlandırılır. Çalışan servislere çok fazla istek gönderir, sunucu bu trafiğe dayanamayarak devre dışı kalır. DDoS, dağınık hizmet sunucuları beklenmedik şekilde tüketir. Saniyeler içerisinde neredeyse binlerce IP göndererek sistem erişimini engeller. DDoS, hackerler tarafından hazırlanan bir saldırı tipidir. Botnet ağları ile yaparlar. Sunucularda ciddi açık verilmesini sağlarlar.



Sistem hızının normale göre yavaşlaması, çok fazla ağ trafiğinin olması, çok fazla UDP, SYN ve GET/POST protokol isteklerinin bulunması DoS ya da DDoS saldırısı belirtilerindendir.

İnternet dünyasında neredeyse en eski ve en etkili saldırı tipleri olarak bilinirler. Saldırganlar tarafından oluşturulduğu için hala kesin çözümü saptanamamıştır.

2.3.1. DoS ve DDoS Türleri:

- Volume Based DDoS (Hacim Odaklı Saldırılar): Bilgisayar dünyasında her sunucunun bant genişliği bulunmaktadır. Bu bant genişlikleri sayesinde sunucunun kapasitesi bellidir. Sunucuya kapasitesinin üzerinde istek gönderilirse sunucu bunu kaldıramaz ve devre dışı kalır, isteklere cevap veremez. Bu saldırıda bunu amaçlamaktadır. Sunucuya bant genişliğinin kaldırabileceğinden fazla istek gönderilir ve sunucu gelen isteklere cevap veremez.
- Protocol Based DDoS (Protokol Odaklı Saldırılar): İnternetin kullanımında aktif kullanılan protokoller vardır, işleyiş bu protokollere göre sağlanır. OSI (Open Systems Inter Connection) protokolü bunlardandır. Protokol odaklı saldırılar, OSI katmanları hedef alınarak yapılan saldırılardandır. OSI'de yer alan 3. (network katmanı) ve 4. katman (transport katmanı) protokollerinde zafiyetler ele alınır. Protokollerin yıllardır kullanılmasından ve güncellenmemiş olmaması bu saldırıları güçlü ve etkili yapmaktadır.

- Application Layer DDoS (Uygulama Katmanlı Saldırılar): OSI protokolünün 7.katmanı olan uygulama katmanından faydalanılır. Bu saldırı türünde uygulama katmanındaki servis açıklarından faydalanarak veri paketlerindeki HTTP metotlarından GET ve POST özellikleri kullanılır. GET ve POST metotları ağ trafiği ile sistem tüketilmeye çalışılır. GET metodu ile sunucudaki kaynaklara erişilir ve POST metodu ile sunucuya veri gönderilir. Sunuculardaki veri yoğunluğu ile sunucuların cevap veremez hale gelmesi sağlanır.
- UDP Flood DDoS Saldırıları: UDP protokolündeki zafiyetler kullanılarak yapılan bir DDOS türüdür. Sunucuya aşırı şekilde UDP paketleri gönderilerek UDP Portlarının kullanılamaz hale getirilerek sunucu cevap veremez hale getirilir.
- PING Flood DDoS Saldırıları: PING Flood DDoS saldırılarında PING paketleri kullanılır ve trafik ağı oluşturulur, sunucunun tüketimini arttırma hedef alınır. Sunucu gönderilen PING paketlerine cevap vermeye çalışırken CPU ve RAM tüketimi sağlanır ve cevap vermemesi sağlanır. Genel olarak protokol zafiyetleri kullanılarak yapılan bu saldırılar başarılı olmaktadır. Bu da şirketlere yüksek oranda maddi kayıp sağlamaktadır. Bunu en aza indirmek için kurum-kuruluşların DDoS saldırılarına karşı farklı tiplerde test altyapıları bulundurmalı ya da bu hizmeti almalıdırlar. Aynı zamanda büyük firmalara da bu testler yaptırılabilir.

İşletmeler açısından ağ altyapılarındaki konfigürasyon hataları, bant genişlikleri ve kullanılan uygulamalara kadar birçok noktada DDoS zafiyeti bulunmaktadır. Bu testleri yapacak olan kişilerin ve kurumunuzu korumakla yükümlü olan kişilerin de teknik olarak TCP/IP gibi protokollerde uzmanlaşmış olması gerekmektedir. (berqnet)

2.3.2. DoS ve DDoS Saldırı Engelleme Yöntemleri:

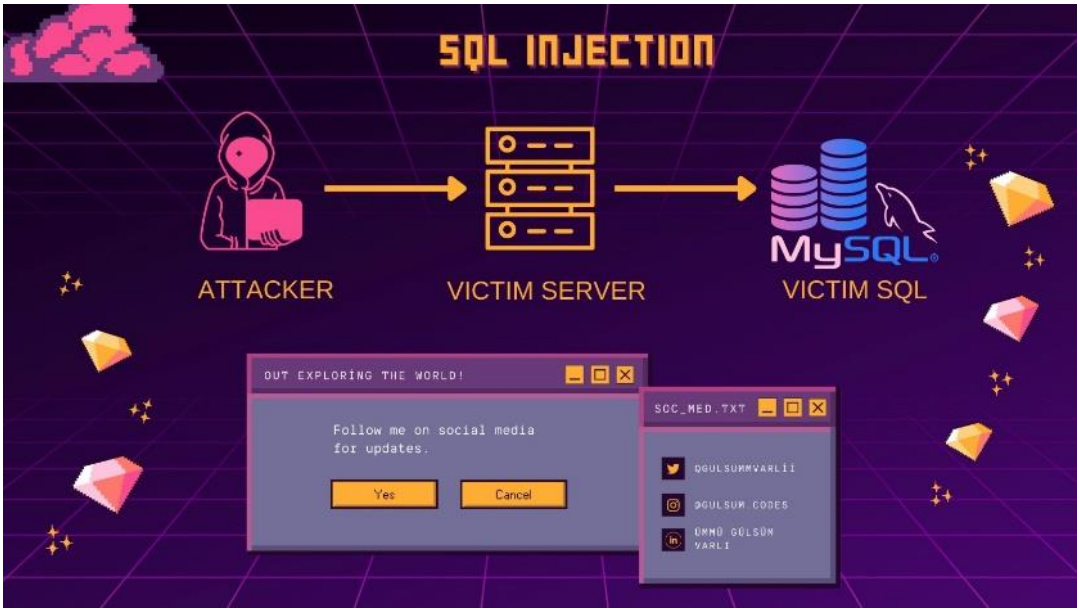
Aslına bakılırsa günümüzde DDoS saldırısı yapmak ve başarılı olmak çok olası durumlardandır. O yüzden şirketler düzenli olarak test sürecine girmelidir.

- Güvenlik duvarı ya da anti-virüs kullanın.
- Sistem güncellemelerini zamanında yapın.
- Ağ trafiği izlenilmelidir, olağandışı durumlar için ağ cihazları yapılandırılmalıdır. Yönlendiriciler için rate limiting özelliği, sahte ve bozuk paketlerin engellenmesi, SYN, ICMP ve UDP paketlerinin eşik değerlerinin belirlenmesi gibi yöntemler uygulanabilmektedir.
- Bant genişliği kurumun ihtiyacı olandan fazla olmalıdır.
- Büyük ölçekli kurumlar için İçerik Dağıtım Ağı (CDN) verilerin dünyada birden çok sunucuda saklanması- kullanımı uygulanabilir.

2.4. SQL Injection:

SQL, Structured Query Language demektir. SQL, verileri yönetmek ve tasarlamak için kullanılan bir alt dildir. İçinde veri bulunduran neredeyse her şeyin alt yapısında SQL bulunmaktadır. O yüzden veri bulunduran şirketlerin bu saldırıya uğraması ihtimali çok yüksektir. SQL enjeksiyonu, en çok kullanılan web korsanlığı saldırılarından olup veri tabanı yok edebilecek kod ekleme tekniklerindendir.

SQL ekleme genellikle bir kullanıcıdan kullanıcı adı/kullanıcı kimliği gibi bir giriş istediğinizde oluşur ve ad/kimlik yerine, kullanıcı size veri tabanınızda bilmeden çalıştıracağınız bir SQL deyimi verir.

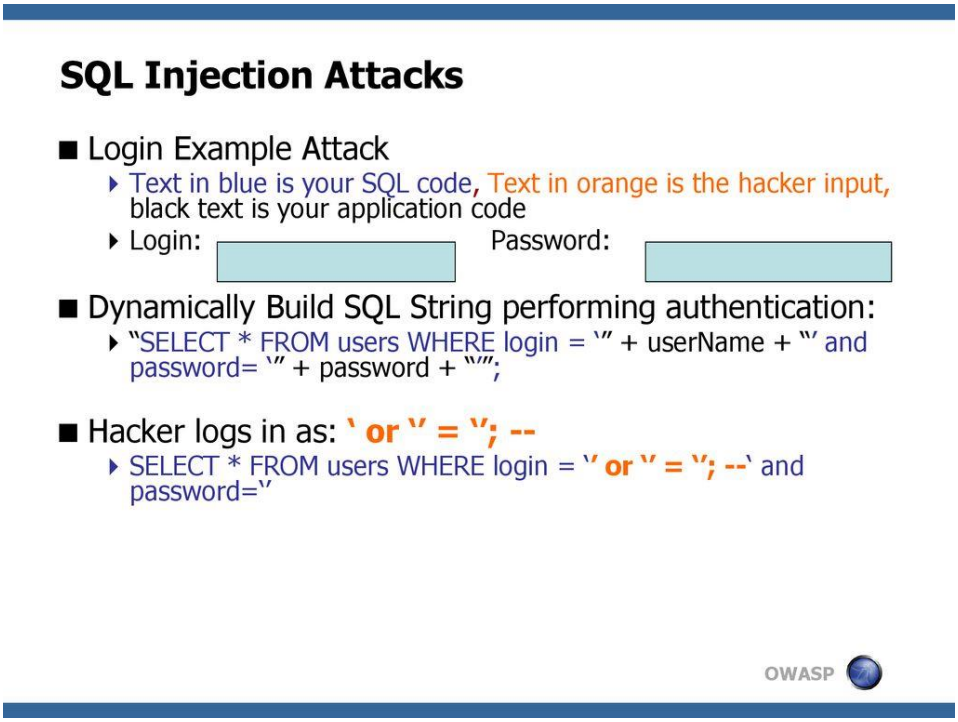


Select dizesine bir değişken (txtUserId) ekleyerek bir deyim oluşturan aşağıdaki örneğe bakın.

- Değişken kullanıcı girişinden getirilir (getRequestString): SELECT
- Örnek
- txtUserId = getRequestString("UserId");
  txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId; (w3school)

SQL; MySQL, MSSQL, Oracle gibi veri tabanlarından veri çekmeye ve işlemeye yardımcı olarak bu veri tablolarında veri hakkında bilgi edinmemizi sağlar. Verileri toplamak ve istediğimiz zaman değiştirebiliyor olmamız bu alt dli popüler kılmaktadır.

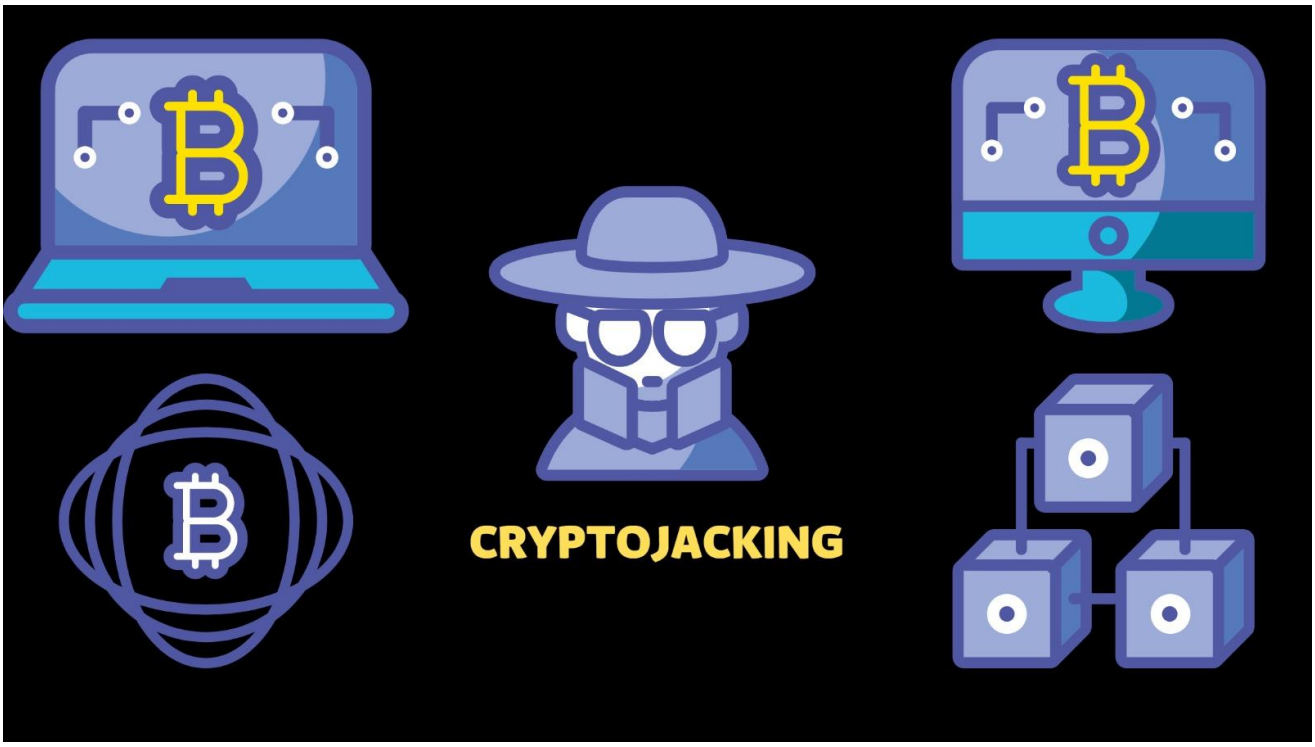
SQL, web uygulamasının yaptığı SQL sorgusuna müdahale ederek veri tabanında bulunan verilere yetkisiz olarak erişim sağlamasıdır. Herhangi bir uygulamaya giriş yapıldığında kullanıcı sadece kendi verilerini görebilir. Fakat SQL enjeksiyonunda saldırgan bununla birlikte diğer kullanıcıların da verilerine ulaşabilir.



Web tabanlı uygulamalarda karşımıza çıkan bu güvenlik açığı veri hırsızlığı için kullanılır. Bir web sitesinde form doldururken arka plana SQL sorgusu gönderilir, database ile iletişim sağlanır. İşte bu kanala hileli şekilde farklı bir SQL sorgusu ile manipüle ederek tüm database ele geçirilebilir. SQL enjeksiyon yöntemi web sitelerinizde bulunan formlarda etkilidir. Bu yüzden sayfalarınızın güvenliğini ihmal etmemelisiniz. En ufak zafiyet şirket için çok büyük veri ihlallerine sebep olabilir.

2.5. Cryptojacking:

Cryptojacking, yani kripto para madenciliği yapmak amacıyla bilgisayarın yetkisi olmayan yerlere girerek işlem yapmasına denir. Fidye yazılımları, güvenilir olmayan web siteleri ya da bilinmeyen e-posta ile saldırganlar saldırı yapabilir. Sahte e-posta sayesinde cryto mining kodları yüklenebilir. Bu şekilde mağdur kişilerin bilgisayarlarına da erişerek tarayıcıdaki reklamlara ya da web-sitesi içeriklerine de bulaştırabilir. Bu da kullanıcıların normal şekilde gezinmesi devam ederken arka planda bilgisayarın işlem gücünü ve diğer kaynaklarını kullanır.



Cryptojacking birden fazla yöntemle yapılabilir ve arka planda çalışarak bilgisayarı tüketerek çalışmasına zarar verebilir. Bu saldırılardan en yaygın olanları kullanıcıları bağlantılara tıklamaya ikna etmek için kimlik avı yöntemi kullanmak, web sitelerine yönlendirme yapan zararlı yazılımlar, komut dosyası ve reklamlar enjekte etmektir. Cryptojacking saldırılarının amacı CPU (Central Processing Unit) sistemine erişmektir. CPU, bilgisayarların veri işleyen ve yazılım komutlarını gerçekleştiren yer olduğu için bu saldırıdan şüphelenenler önce bilgisayarın çalışma performansını değerlendirmelilerdir.

2.5.1. Saldırı Örnekleri:

- 2017 yılında keşfedilen kötü amaçlı Google Chrome uzantılarından olan **FacexWorm** ile kullanıcıların bilgisayarlarına Facebook uygulaması ile erişmesi mümkündür.
- Dünya çapında en büyük platformlardan olan açık kaynaklı kodların depolandığı Github'a şifrelenen zararlı yazılımlar, kaynak erişimini kolaylaştırır.

2.5.2. Cryptojacking Nasıl Tespit Edilir?

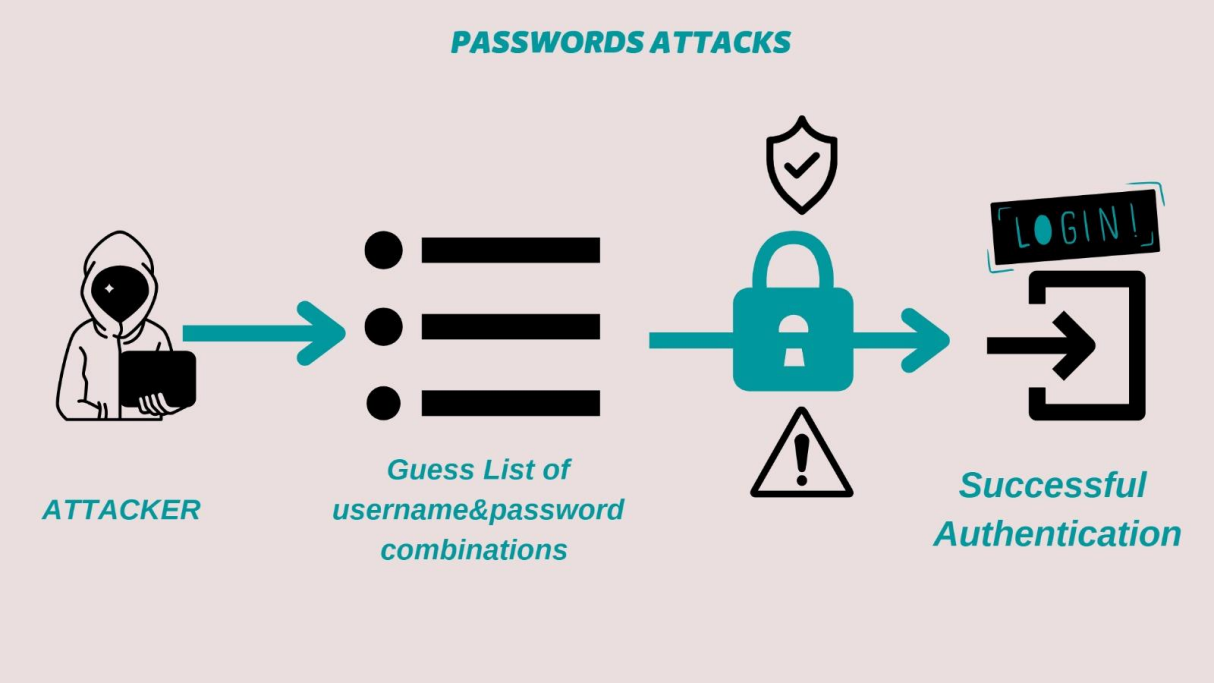
- Bu saldırılar arka planda gerçekleşirken performans düşüklüğüne sebep olacaktır.
- Bilgisayarda yavaşlık yaşayan personeller ilk olarak yardım masasına bakmalıdır. Dolayısıyla bilgisayarı inceleyen kişinin cryptojacking saldırısına hakim olmalıdır.
- Saldırılar ağ izleme yöntemi ile tespit edilebilir. Ağların izlenmesi, analiz edilmesi ve yönetimi yapay zeka kullanılarak tasarlanan çözümler tespit etmeyi sağlar.

2.5.3. Crytojacking Saldırılarından Nasıl Korunulur?

- Ağ trafiğini ve sistem trafiği kontrol edilmelidir.
- Web tarayıcılarına ait özel, güvenli uzantılar kullanabilirsiniz. (Anti Miner, minerBlock)
- Reklam yoluyla bulaşabilirler o yüzden Ad Blocker gibi reklam engelleyicileri kullanılabilir. Ayrıca güvenilir web sitelerinde gezinilmeli, bilinmeyen reklamlara tıklanmamalıdır.
- Bu saldırı genellikle JavaScript kodu üzerinden tasarlanır. Saldırıdan şüphelendiğiniz zaman web tarayıcısındaki JS kodunu devre dışı bırakıp diğer performans değerlerini tekrar değerlendirebilirler.

2.6. Password Attacks (şifre saldırısı):

Kullanıcı hesaplarının kimlik bilgilerinden yararlanmak için yapılan saldırı türüdür. En yaygın saldırı türlerinden olan şifre saldırısı, 2020'de veri ihlallerinin %81'inden fazlasını oluşturuyor. Şifre saldırıları, parolaların tahmin edilmesini ya da parolalarının kırılmasını hızlandıran araçlarla açıklardan faydalanmayı amaçlar.



2.6.1. Şifre Saldırısı Türleri:

2.6.1.1. Kimlik Avı Saldırısı:

En yaygın şifre saldırısı türlerindendir. Bilgisayar korsanının kurbana kötü amaçlı bir bağlantı göndererek güvenilir site kılığına girdiği tekniktir. Meşru bir şekilde kimlik doğrulaması yapıldıktan sonra kurban bağlantıya tıklayarak saldırgana kimlik bilgilerini gönderilmesini sağlar. Kimlik avı saldırılarında kullanıcıya bağlantıyı tıklattırmak için çeşitli yöntemler denenir.

- DNS- önbellek zehirlenmesi: Saldırganlar, kullanıcı isteklerine benzer farklı bir siteye yönlendirilir. Yani kullanıcıyı ikna etmek için DNS sunucundaki açıklardan faydalanır.
- URL- ele geçirme/yazım hatası yapma: Saldırganlar, kullanıcının gitmek istediği siteden küçük farklılıklar gösteren gerçek görünümlü bir URL oluşturur. Kullanıcı yazım hatası yaptığında kötü amaçlı sayfaya yönlendirirler.
- Tabnabbing: Meşru web sayfalarına benzeyen kötü amaçlı siteleri yeniden yazarlar.
- UI düzeltme/iFrame kaplaması: Saldırganlar meşru bir tıklama bağlantısına kötü amaçlı yazılım eklerler.
- Kimlik avını klonlama: Orijinal e-postadaki bağlantıların kötü amaçlı sitelerin URL'leri ile değiştirildiği saldırıdır.

2.6.1.2. Brute-Force Şifre Saldırıları:

Kullanıcının kimlik bilgilerini tahmin etmek için deneme- yanılma yolu kullanılır. Saldırgan, çok fazla permütasyonla çalışmak için komut dosyaları kullanır. Bu yöntem her ne kadar eski bir yöntem olsa da otomatik ve basit oldukları için hela standarttır, kullanılır.

2.6.1.3. Sözlük Şifre Saldırıları:

Belirli bir ağ tarafından parola olarak kullanılma ihtimali en yüksek olan liste oluşturulur. Önceden tanımlanmış bu liste kullanıcının davranış kalıplarından ve önceki veri ihlallerinden oluşmuştur. Bu listeler kullanıcı adlarına göre otomatik kimlik doğrulaması yapılan araca geçirilir.

2.6.1.4. Şifre Püskürtme Saldırısı:

Bilgisayar korsanı, başka bir parolaya geçmeden aynı parolayı kullanarak kimlik doğrulaması yapmaya çalışır. Web sitesi kullanıcıları basit şifreler belirlediğinden ve birkaç hesapta aynı şifreyi kullandığından şifre püskürtme en etkili yöntemlerdendir.

2.6.1.5. Keylogging:

Saldırgan, kullanıcının bilgisayarını izleme araçları yükler. Keylogger, kullanıcıların giriş formlarına yazdığı tüm bilgileri kaydeder ardından üçüncü tarafa gönderir. Bu da yetkisiz erişim sağlar.

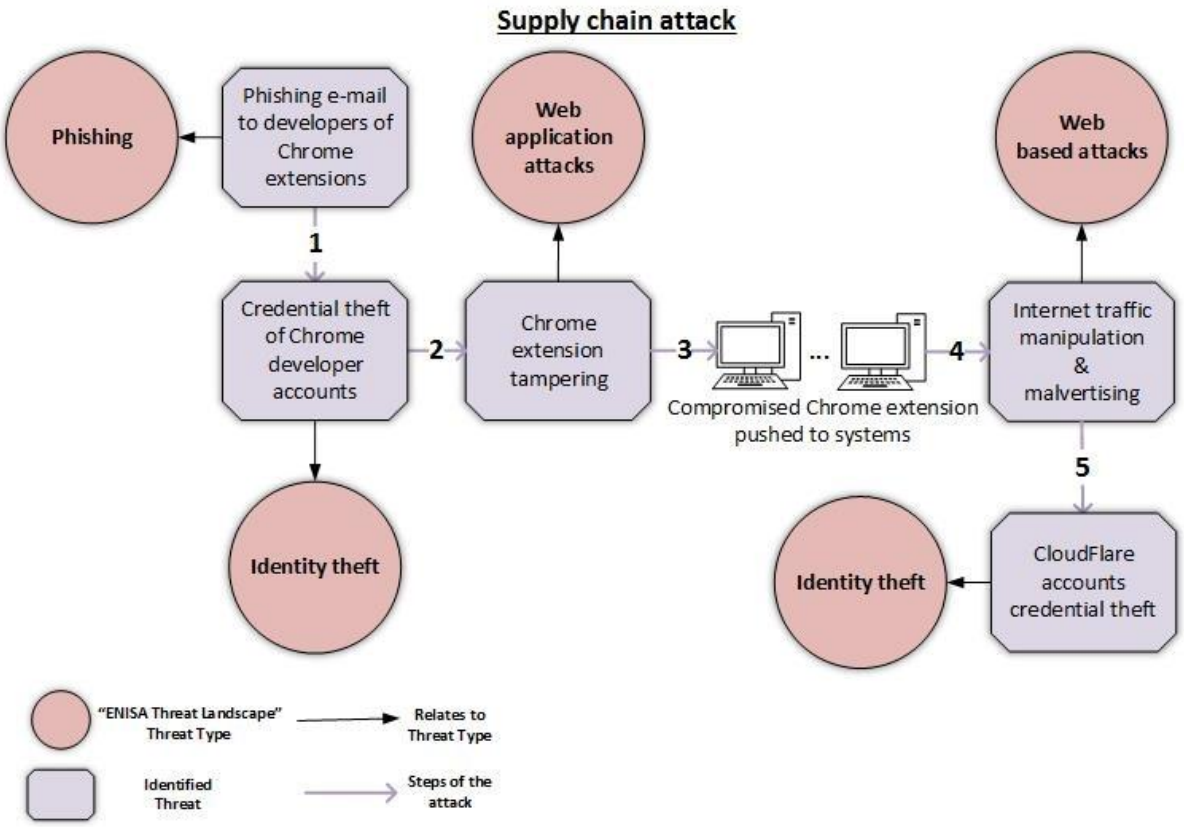
2.7. Supply Chain Attack – Tedarik Zinciri Saldırısı:

Tedarik zinciri, zincir içinde yer alan temel iş süreçlerinin entegrasyonunu sağlayan iş modellerinin ve süreçlerinin tamamına denir. Müşteriye doğru zamanda, doğru yerde sorunsuz şekilde para, bilgi, malzeme ulaşımını sağlar.

Tedarik zinciri saldırısı ise kurum - kuruluşların sağladığı donanım, yazılım açıklarından faydalanarak işleyişe hasar veren saldırılara denir.

2.7.1. Tedarik zinciri saldırısı türleri:

- Yazılım Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları: Büyük firmaların maksimum iş akışı verimi sağlamak amacıyla kullandıkları yazılımlara yapılan saldırılardır.
- Donanım Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları: Basit ve ucuz saldırı yöntemi olan donanım yoluyla gerçekleştirilen tedarik zinciri saldırı yöntemi, USB sürücüsü ya da ethernet kablosu gibi farklı imkanlar sunan çipler yöntemi sayesinde görüntü ya da ses kaydedici cihazlar yerleştirilmesiyle gerçekleşiyor.
- Firmware Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları: En çok tercih edilen saldırı türüdür. Diğer türlere göre daha çok bilgi beceri gerektiriyor. Güvenlik duvarını aşıp sistemlere zarar veriliyor.

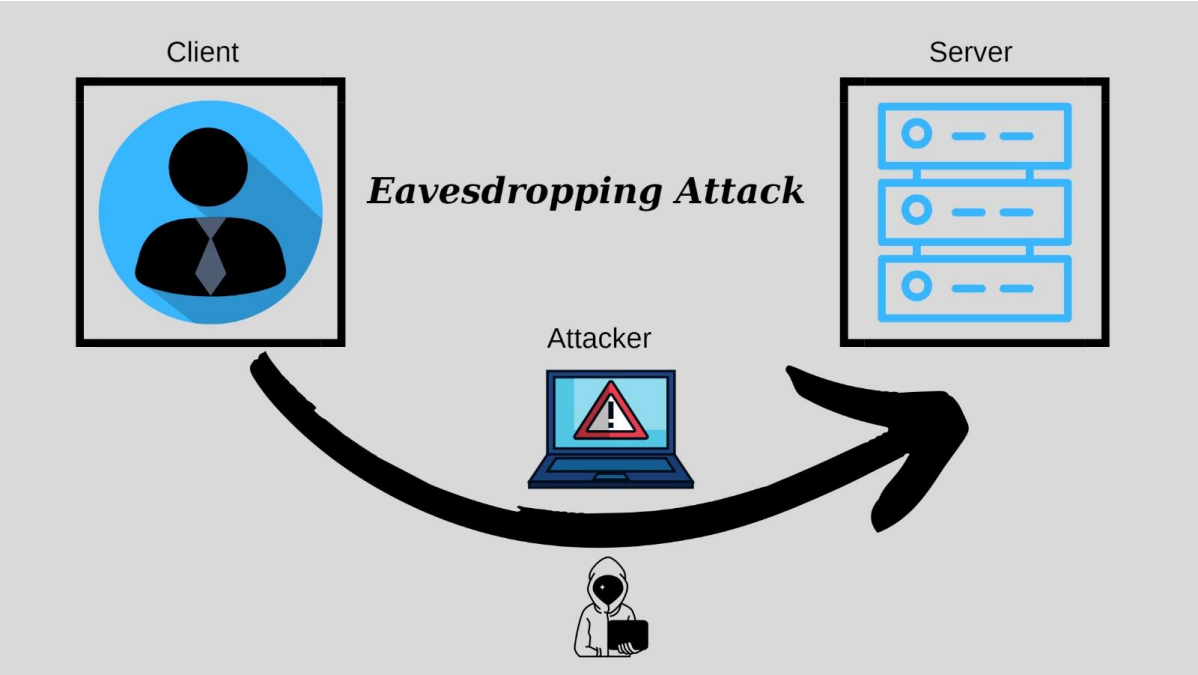


http://bit-sentinel.com

2.8. Eavesdropping Attack – Telekulak / Gizli Dinleme Saldırısı:

"Gizlice dinlemek" anlamına gelen eavesdropping, günümüz dünyasında Cihazlar arasında iletilen verilerin üçüncü kişi tarafından dinlenilmesi, ele geçirilmesi ya da izinsiz kullanılmasını ifade eder.

Bu saldırı türü artık güvenli olmayan ağlar üzerinde gerçekleştirilmektedir. Yani cihazların güvenli olmayan ağ bağlantıları aracılığıyla aktarılan verilerin yakalanmasıdır.



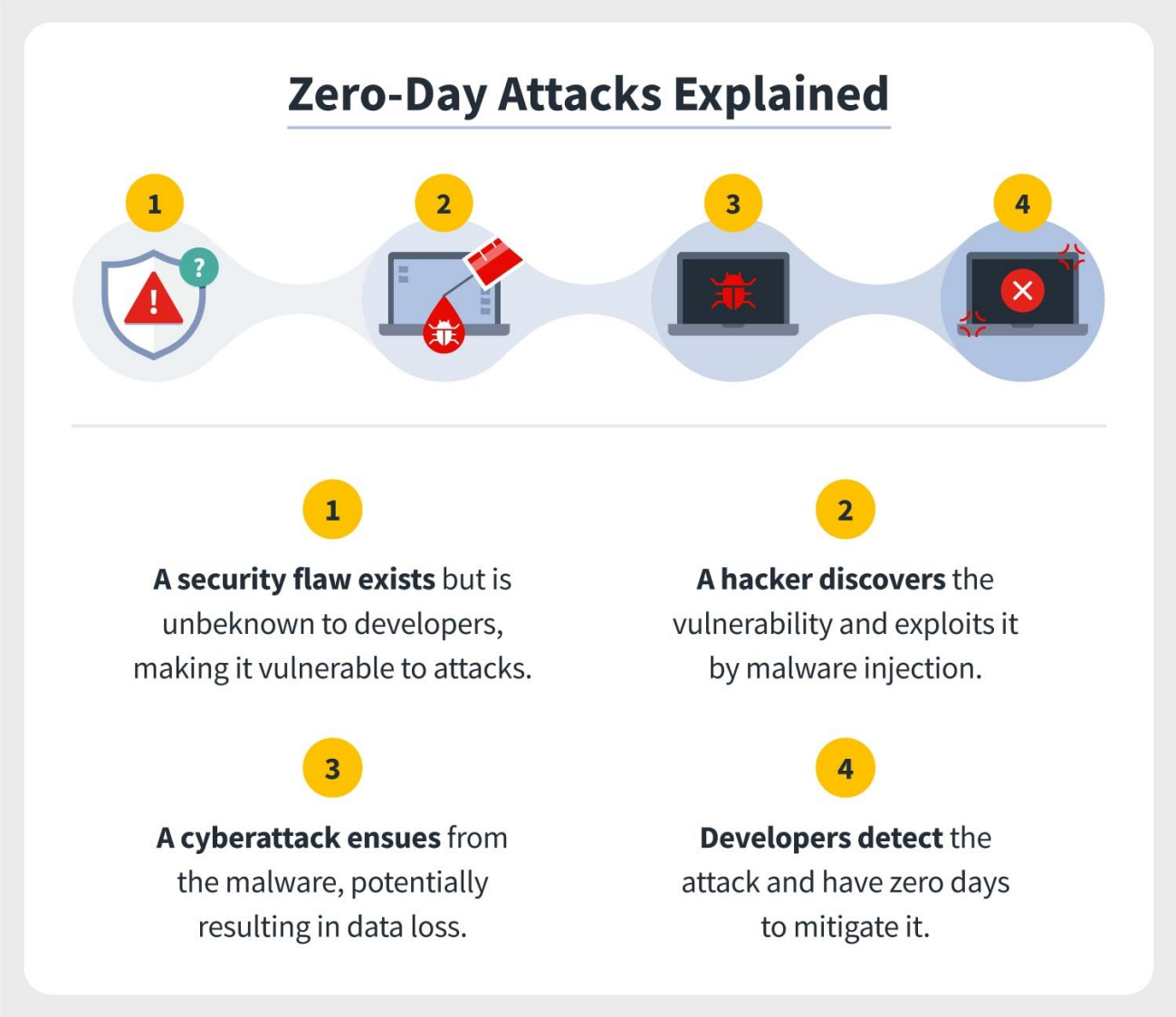
2.8.1. Gizli Dinleme Saldırısı Yöntemleri:

- Pasif Eavesdropping: Bu yöntem daha çok pasif olarak bilgi toplamaya yönelik saldırı yöntemidir. Saldırgan, sizin her yaptığınız işlemi pasif olarak izleyebilir, bilgi toplayabilir ama verilerinizi değiştirmez. Bu saldırı yöntemi genelde ortak wifi bağlantılarında sorun oluşturur.
- Aktif Eavesdropping: Ağ üzerinden sisteminize sızıp verilerinizi değiştirebilirler. Saldırgan kendi isteklerine göre her şeyi yapabilir.

Tanıdığınız birinden geldiğini düşündüğünüz e-posta üçüncü niyetli şahıs tarafından gönderilmiş olup sizi aldatıyor olabilir. Bilgisayar korsanları güvenli IP adreslerini kopyalayıp taklit ederek size ulaşmaya çalışmak için güvenilir e-postaları değiştirebilir.

2.9. Zero Day Exploit - Sıfır Gün Açığı Saldırısı:

Saldırılacak yerdeki ağdaki ya da donanımdaki açığı oranın geliştiricisinden, yöneticisinden, yetkilisinden önce keşfederek saldırmaktır. Sıfır gün açığı olmasının sebebi ise açık fark edildikten sonra sıfır gün içinde saldırılmasıdır. Geliştiriciler açığı fark ettiğinde yama yapmaya ya da düzeltmeye çalışacaklardır fakat bu zaman alacaktır. O yüzden de genelde sıfır gün açığı saldırıları başarılı olmaktadır.



- **Sıfır gün güvenlik açığı,** bilgisayar korsanlarının tedarikçiden önce açığı fark etmesidir.
- **Sıfır gün exploiti,** saldırganların sistemlere önceden bilinmeyen açığa yapılan saldırı yöntemidir.
- **Sıfır gün saldırısı,** bilgisayar korsanlarının açığı fark ettiği andan itibaren sıfır gün içinde saldırı gerçekleştirmesidir.

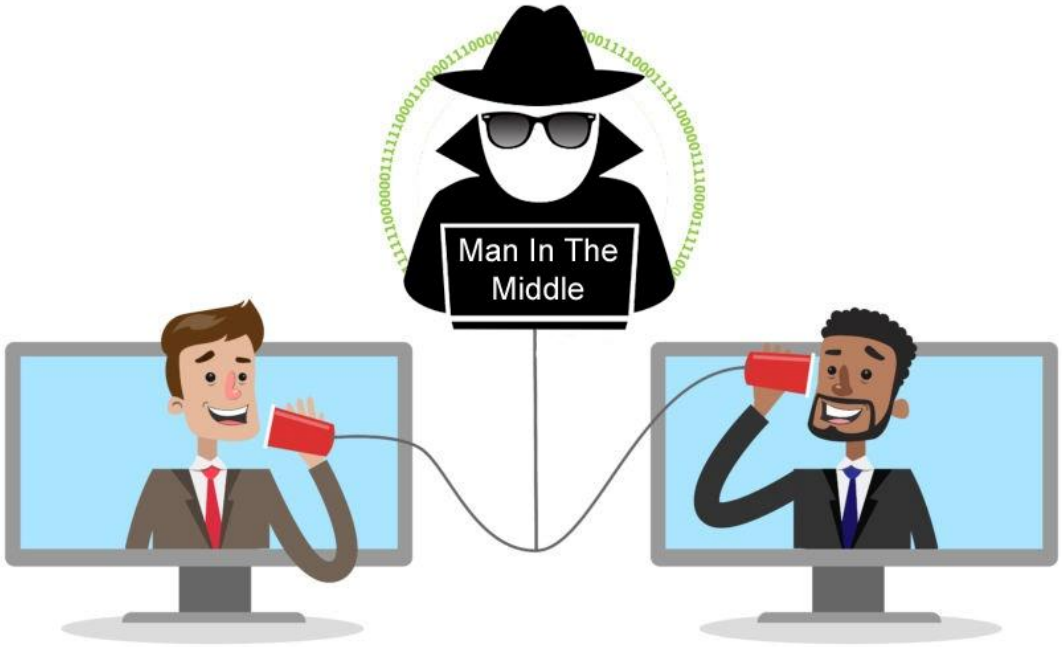
Bazı saldırganlar ya da bilgisayar korsanları, yazılım geliştiricileri fark etmeden tedarik zincirinde açık keşfederler. Ardından bu açığın zafiyetinden faydalanmak için kod yazarlar ve saldırıya geçerler. Bu yazılan koda "exploit kodu" denir. Artık saldırganların güvenlik açığı bulunan sisteme erişmeleri gerekmektedir. Bunun için de genelde sosyal mühendislik hilelerinden olan e-posta aracılığı ile erişmeye çalışırlar.

Elde edilen veriler dark-web üzerinden satışa çıkabilir, veriler kullanılarak şantaj yapılabilir. Exploit keşfedilip yama uygulandıktan sonra bu tehdit ortadan kalkmış olur.

Sıfır gün saldırılarını, siber suçlular, hacktivistler, siber savaşçılar ya da kurumsal casusluk yapanlar yapabilir.

2.10. Man-in-the-Middle Attack:

Zayıf tabanlı web protokollerinden yararlanan saldırganların, veri hırsızlığı için kendilerinin aracı bir kanaldaki varlıklara eriştiği ve verilerle ilgili bilgileri kendi lehine deforme ettiği saldırı tipidir.



2.10.1.Ortadaki Adam (MITM) Saldırılarının Türleri:

- IP Kimlik Sahtekarlığı: Saldırganın kurbanı meşru gibi görünen siteye yönlendirmesini sağlayarak bilgilerini ele geçirmesidir. Saldırgan, sahte IP ile güvenli web-sitesini değiştirmiştir.
- ARP Önbellek Zehirlenmesi: Adres Çözümleme Protokolü (ARP), belirli bir internet katmanı adresi ile ilişkilendirmiş olup diğer bağlantı katmanı adresi ile iletişime geçmeyi sağlayan protokoldür. ARP, bağlantı katmanı adresini yerel ağdaki internet protokolü (IP) adresine çevirdiği için önemlidir. Kurbanın bilgisayarı suçludan gelen yanlış bilgilerle kandırılır, dolandırıcı bilgisayarı ağ geçidi gibi algılanır. Ardından kurbanın bilgisayarı ağa bağlandıktan sonra tüm ağ trafiğini gerçek bir ağ geçidi yerine kötü niyetli üçüncü kişiye gönderir. Bilgisayarda depolanmış kişisel bilgilerin veri hırsızlığı yapılmış olur.

- E-posta Ele Geçirme: Siber suçlular hassas veriler ya da paraya erişimi olan bankaların e-postalarını ele geçirir ve banka müşteriler ile arasındaki iletişim sağlanır, izlenir. Daha da kötüsü saldırgan, kurban bankanın e-posta adresini taklit ederek bankanın müşterilerinden para isteyerek para aklayabilir.
- DNS Kimlik Sahtekarlığı: Etki alanı adı sistemi (DNS) sahteciliği ya da zehirlenmesi, meşru trafiği kullanıcının büyük olasılıkla bileceği ve güveneceği web sitesine yönlendirir bunu DNS kayıtlarını manipüle ederek yapar. Amaç kurbandan olabildiğince veri çalmaktır.
- Wifi Gizlice Dinleme: Saldırganlar, kurbanların yakınlardaki kablosuz ağa bağlanmasını sağlar. Kurban güvenli ağa bağlandığını sanır fakat kötü amaçlı işler için tasarlanmış zararlı ağdır. Kullanıcının çevrimiçi etkinliğini izleyebilir, kredi kartı bilgilerini, oturum açma kimlik bilgilerini kazıyabilir.

2.10.2.Ortadaki Adam (MITM) Saldırısı Nasıl Çalışır?

1. Kurban güvenli sandığı diğer faktöre mesaj gönderir.
2. Saldırgan, diğer faktörün haberi olmadan iletiyi ele geçirir.
3. Saldırgan, ileti içeriğini değiştirir, iki tarafında haberi olmadan iletiyi ortadan kaldırır.

Olağandışı bağlantı kesilmeleri, garip URL'ler ya da herkese açık güvenli olmayan kablosuz ağlardan MITM saldırıları elde edilebilir.

2.10.3.Ortadaki Adam Saldırıları Nasıl Önlenir?

- Uçtan uça şifreleme kullanın.
- Güvenli web-sitelerine bağlanın.
- DNS trafiğini şifreleyin.
- Yamaları yükleyin anti-virüs kullanın ve güncelleştirmeleri takip edin.
- Sıfır güven felsefesini unutmayın.
- Güçlü parolalar kullanın.
- Sanal ağ (VPN) kullanın.