ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

SİBER GÜVENLİK FARKINDALIK EĞİTİMİ - 2026

SİBER OLAYLARA MÜDAHALE EKİBİ
(SOME)

https://some.ogu.edu.tr

"Bir şeyin değerini anlamadan kaybetmek, en büyük öğretmendir." – Konfüçyüs

Siber Güvenlik: Tehditler ve Korunma Yöntemleri

in aytylmz

Siber Güvenlik Uzmanı Aytaç YILMAZ

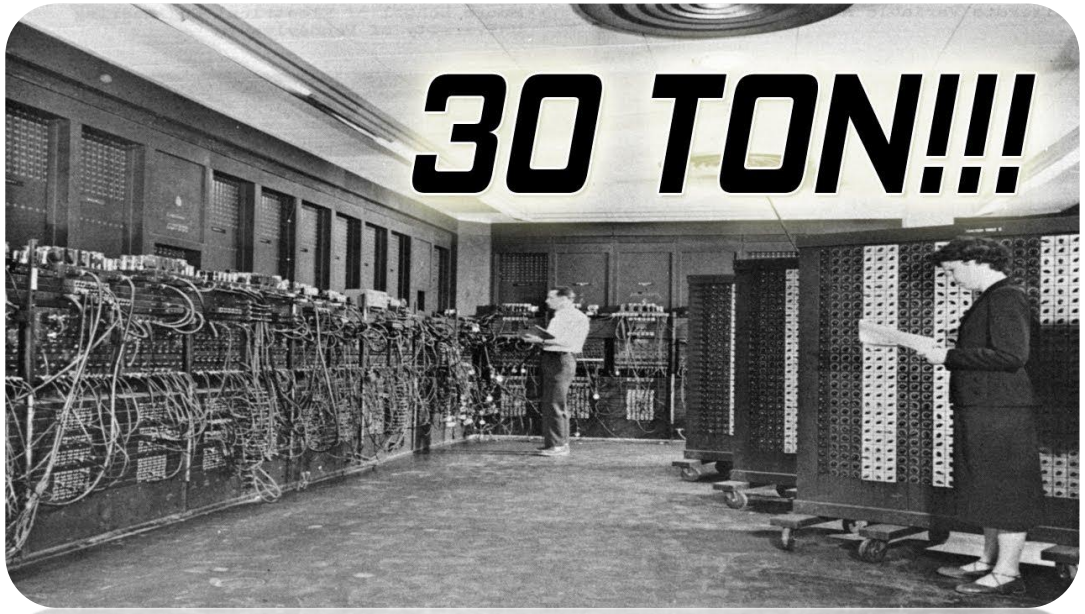
Teknolojinin Gelişim Süreci

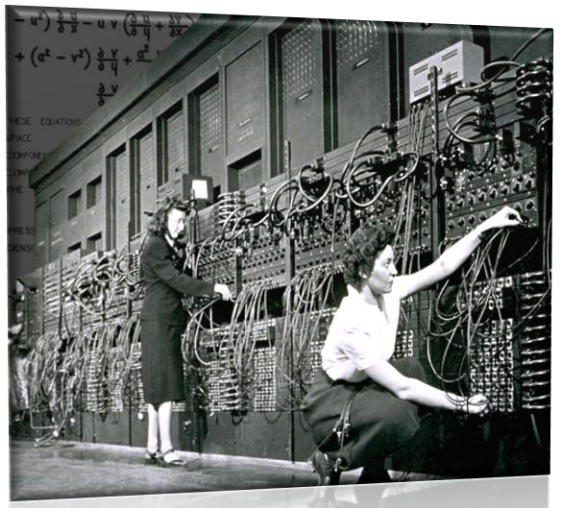
SİBER DÜNYAYA DOĞRU >> İLK BİLGİSAYAR

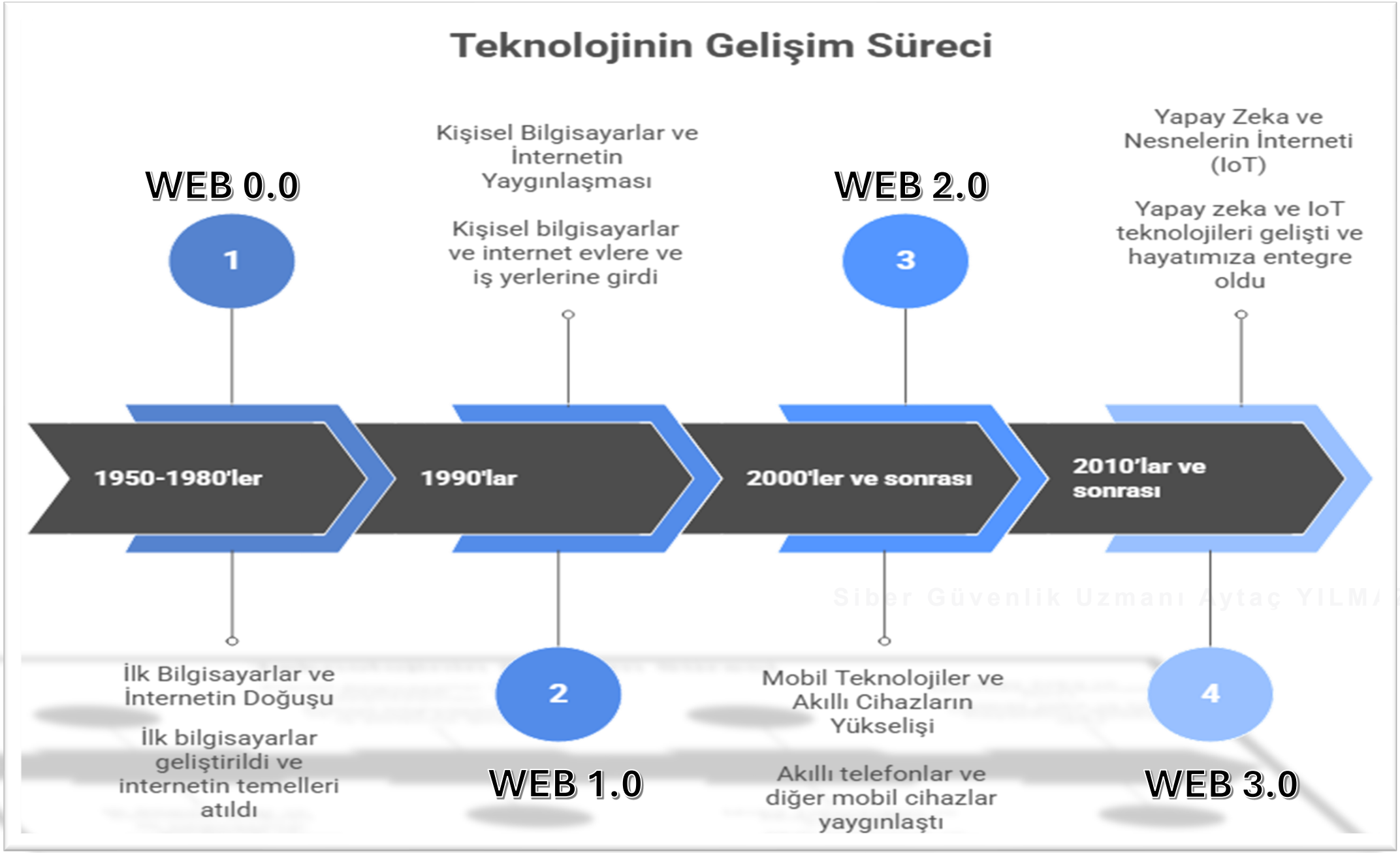
ENIAC

Electronic Numerical Integrator And Computer

- **Tarih:** 1945 yılında faaliyete geçti.
- **İşlem Hızı:** 5000 İşlem/Saat
- **Kullanım amacı:** Askeri hesaplamalar







WEB 0

İnternetin temellerinin atıldığı, henüz "web" kavramının gelişmediği dönemde, bilgi paylaşımı akademik ve askeri ağlarla sınırlıydı.

WEB 1.0

Web 1.0, İnternet'in ilk kullanıcı dostu halini temsil eder. Bu dönemde, web siteleri statik, yani değişmeyen sayfalardan oluşuyordu. Kullanıcılar sadece bilgi alabiliyor, içerikle etkileşime giremiyorlardı.

WEB 2.0

Web 2.0, internetin dinamik, etkileşimli ve kullanıcı merkezli bir hale geldiği dönemi ifade eder. Bu dönemde sosyal medya platformları, kullanıcıların içerik üretmesine olanak tanıdı.

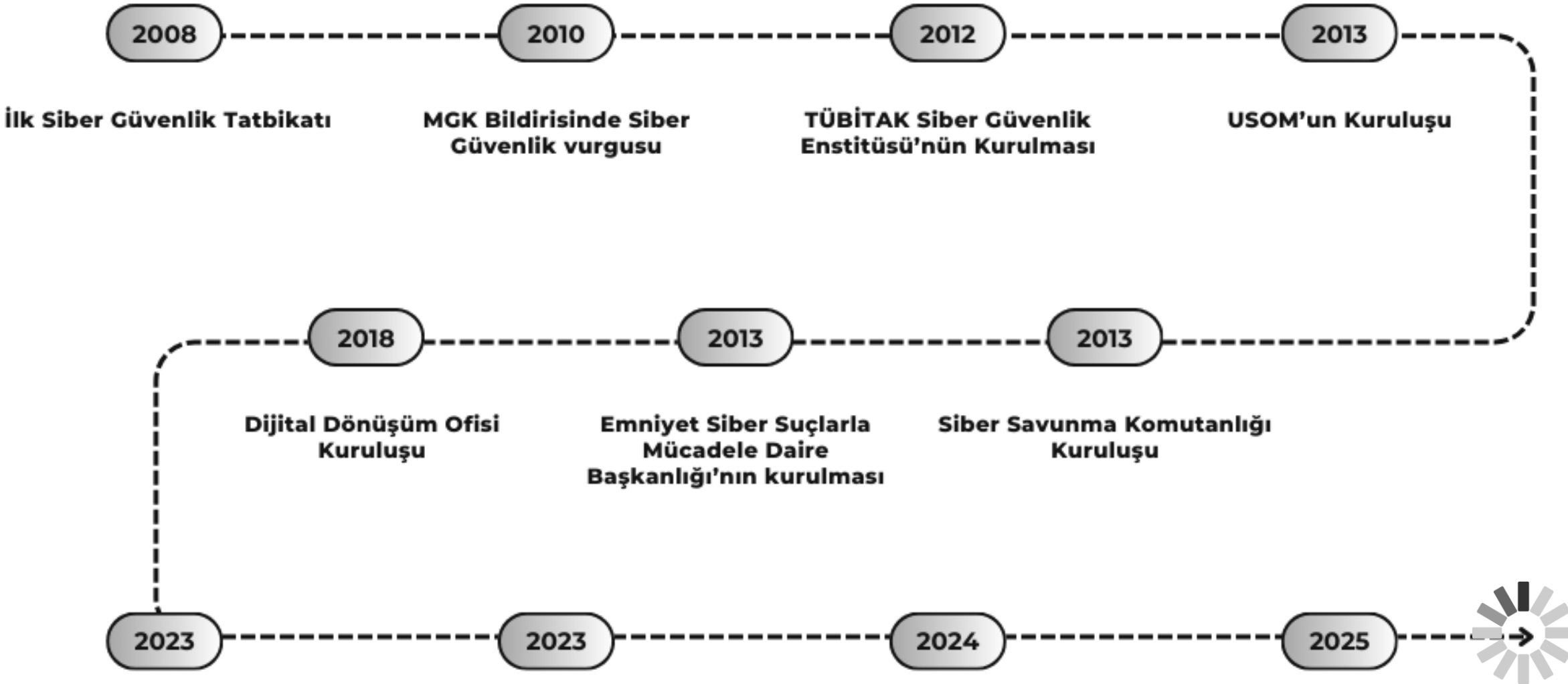
WEB 3.0

Web 3.0, internetin daha akıllı ve kişisel hale geldiği dönemi ifade eder. Yapay zeka, blok zinciri ve merkeziyetsiz uygulamalar gibi teknolojiler, verinin bağlamını anlayarak kişiselleştirilmiş deneyimler sunar.

WEB 4.0

internete bağlanan her cihazın birbirine entegre olduğu ve her kullanıcının deneyiminin tamamen kişiselleştirildiği bir ağ yapısını ifade eder.


TÜRKİYE'de
Siber Güvenlik


2008
İlk Siber Güvenlik Tatbikatı
2010
MGK Bildirisinde Siber Güvenlik vurgusu
2012
TÜBİTAK Siber Güvenlik Enstitüsü'nün Kurulması
2013
USOM'un Kuruluşu
2013
Siber Savunma Komutanlığı Kuruluşu
2013
Emniyet Siber Suçlarla Mücadele Daire Başkanlığı'nın kurulması
2018
Dijital Dönüşüm Ofisi Kuruluşu
2023
MİT Siber İstihbarat Başkanlığı Kuruldu
2023
Siber Güvenlik Meslek Yüksekokulları'nın Açılması
2024
Siber Güvenlik Mühendisliği Programının Açılması
2025
Siber Güvenlik Başkanlığı

SİBER GÜVENLİK

Nedir ?

Siber Güvenlik

Tanımı:

Siber güvenlik, bilgisayar sistemleri, ağlar, yazılımlar ve verilerin yetkisiz erişim, saldırı, hasar veya hırsızlık gibi siber tehditlerden korunmasını sağlamak amacıyla alınan önlemleri ifade eder.

Önemi:

Günümüzde dijitalleşmenin artması, bireyler ve organizasyonlar için siber güvenliği kritik hale getirmiştir. Siber saldırılar, finansal kayıplara, itibar kaybına ve veri ihlallerine yol açabilir. Bu nedenle, etkili siber güvenlik stratejileri geliştirmek ve uygulamak hayati önem taşır.

Saldırıların Sonuçları:

- Maddi Kayıplar
- Veri Kaybı
- İtibar Kaybı
- Hizmet dışı kalma durumu
- Yasal Sorunlar

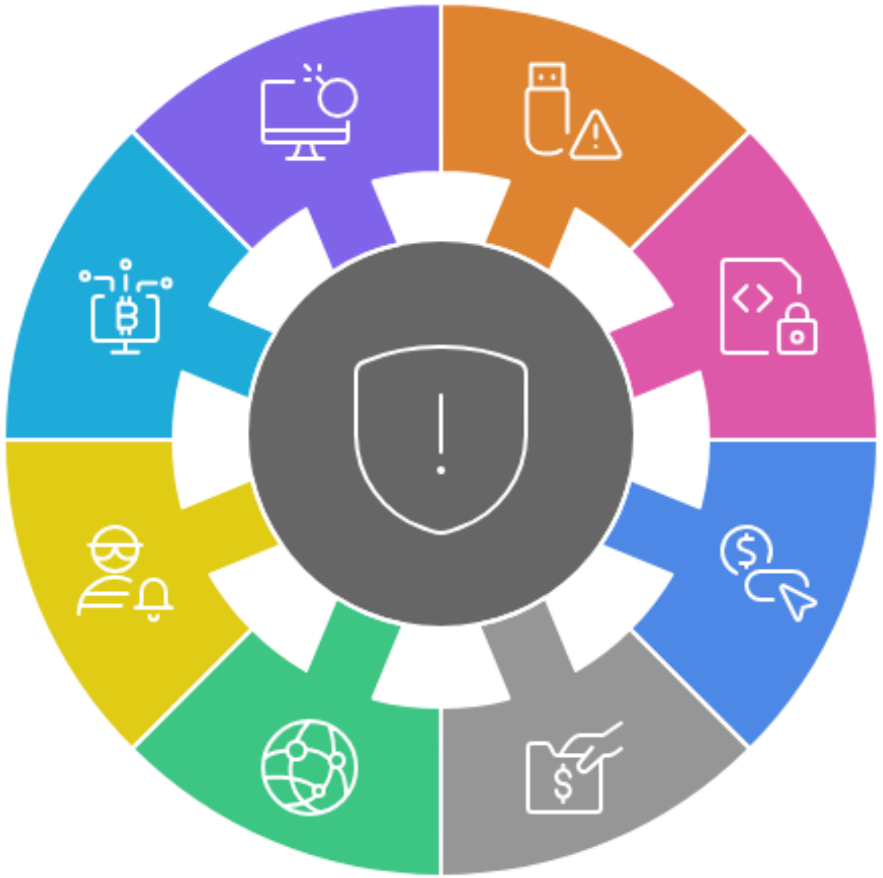
SIK KARŞILAŞILAN TEHDİTLER

Zero-Day Attacks

Bilinmeyen güvenlik açıklarından yararlanır.

Malware

Zararlı yazılımlar sistemlere zarar verir ve veri çalar.



Cryptojacking

Bilgisayar kaynaklarını izinsiz kripto para madenciliği için kullanır.

Ransomware

Verileri şifreler ve fidye talep eder.

Insider Threats

İçeriden gelen çalışanlar tarafından gerçekleştirilen saldırılar.

Phishing

Sahte e-postalar veya web siteleri aracılığıyla hassas bilgiler toplar.

Botnet

Kontrolsüz bilgisayarlar ağı oluşturur ve spam gönderir.

APT

Uzun süreli ve gizli saldırılar gerçekleştirir.

Malware

Virüs: Bilgisayara bulaşarak kendini kopyalayan kötü amaçlı yazılım.

Trojan: masum gibi görünen fakat arka planda zarar veren yazılımlar.

Spyware: Kullanıcının izni olmadan bilgi toplayan yazılımlar.

Adware: Kullanıcıyı rahatsız eden reklamlar gösteren yazılımlar.

Ransomware

Ransomware: kullanıcının dosyalarını şifreleyerek erişimini engelleyen ve şifreyi çözmek için fidye talep eden bir yazılım türüdür.

Ransomware saldırılarından en meşhuru “WannaCry Ransomware“ saldırısıdır, Microsoft Windows işletim sistemindeki bir güvenlik açığını (EternalBlue) kullanarak yayılmıştır.


Wana DecryptOr 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/3/1970 17:00:00
Time Left
00:00:00:00
Your files will be lost on
1/7/1970 17:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
WannaCry
WannaCry
WannaCry
Sonuçlarının özeti ismine yansımış olan kötücül yazılım

Malware Saldırılarından Korunmak İçin

- Tüm önemli hesaplarda 2 adımlı doğrulamayı (MFA) aç.
- Bilgisayar güncellemelerini kapatma.
- Crackli / lisanssız program indirme.
- Bilmediğin e-posta eklerini açma.
- “Makroyu etkinleştir” uyarısına basma.

- Önemli dosyalarını yedekle.
- Tanımadığın USB belleği bilgisayarına takma.
- Lisanslı bir antivirüs yazılımı kullan

Phishing

Phishing (Kimlik Avı) saldırısı, bilgisayar korsanlarının kullanıcıların kişisel bilgilerini (parola, kredi kartı vb. bilgileri) elde etmek için sahte SMS, e-postalar veya web siteleri kullanarak gerçekleştirdiği bir saldırı türüdür.

Kimden: "PTT" <noreply@offer-b6dfd.firebaseapp.com>
Kime: "nakyel" <[redacted]>
Gönderilenler: 24 Ocak Cumartesi 2026 13:52:39
Konu: Gönderiniz Beklemede - Gümrük Vergisi Ödemesi Gerekiyor

Bilinmeyen adres

Ptt
Gümrük Vergisi Ödeme Bildirimi

Sayın Müşterimiz,

Gönderiniz, şu anda **PTT gönderi merkezinde** bulunmaktadır. Gümrük mevzuatı kapsamında, gönderiniz için ithalat vergisi ve ilgili masraflar tahakkuk etmiştir.

Gönderi Takip Numarası

Ödenecek Tutar

https://linklock.titanhq.com/analyse?url=https%3A
com%2Furl%3Fq%3Dhttps%253A%252F%252Fsamo
pace.myclickfunnels.
com%252Foorbe%26user_uuid%3D7e9d935d-1e26-
b0111%26stage%3D1%26hmac%3D735e4993a46749
8507e804d6fa33d3f37ea5f31675e7248&data=eJxFjD1
GwaGSFWmLB06V8Z3TIlMdm3cin9fowyVTqc76b1
zhXnqE0u-pXafL-8fyMz--bhu5tXnaQsLoj0aQ4Bym
qxtmjazHOhP7D9Wpse-x9zwS8OudazxuIE_TqW-Jfm
aJ1ZbOGGEMMeUez_oa05Ggs9uth_dMurmwb-vxK
t5Qs1qHGHkEjqKTHVCmKEbFKMdWpCSuJIQSquS
MY7cCKXFKCybubCD40Q6AFCDJBoHIkA5wzlwxzU
RvPg%%
Bağlantı izlemek için tıklayın veya dokunun.

Ödemeyi Tamamla

Ödeme işlemi tamamlanmadan gön
edememektedir. İşlemlerin devam e
ödemenizi gerçekleştiriniz.

Ödeme işleminin ardından gönderiniz en kısa sürede tekrar işleme alınacaktır.

Saygılarımızla,
PTT Müşteri Hizmetleri

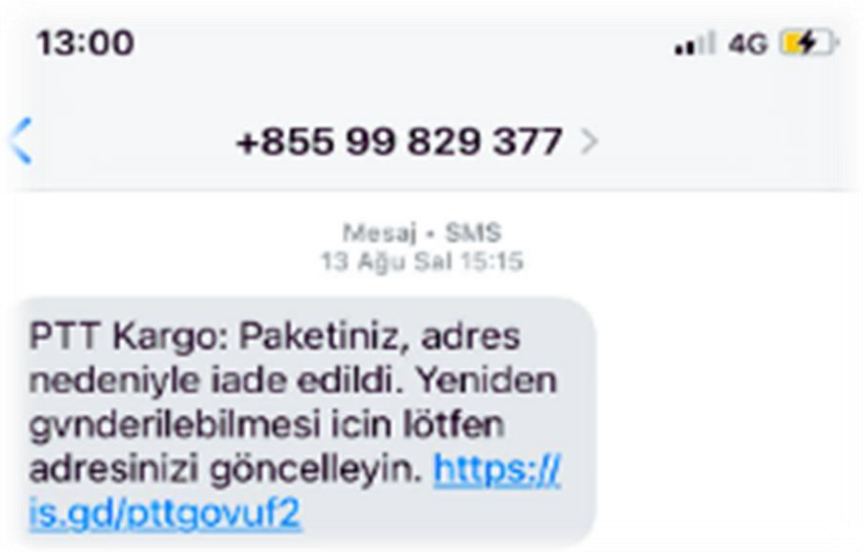
© 2026 PTT | Tüm hakları saklıdır

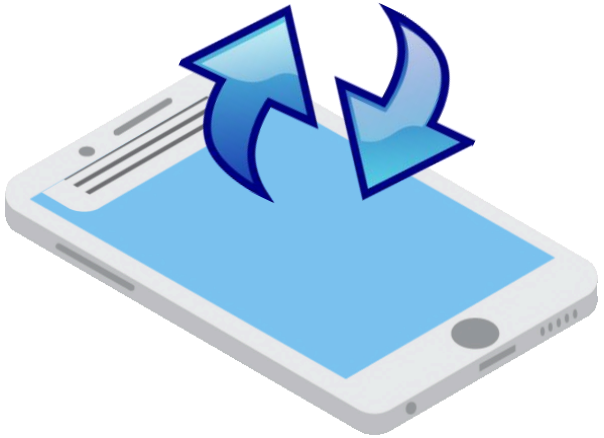
https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fcalendly.
com%2Furl%3Fq%3Dhttps%253A%252F%252Fsamoppoposteamworks
pace.myclickfunnels.
com%252Foorbe%26user_uuid%3D7e9d935d-1e26-44a8-8621-ecd550f
b0111%26stage%3D1%26hmac%3D735e4993a467494c2b34c8f305fddd6
8507e804d6fa33d3f37ea5f31675e7248&data=eJxFjD1vgzAQQH8NbCB_
t5Qs1qHGHkEjqKTHVCmKEbFKMdWpCSuJIQSquSd3PHip_3YzX2NLIE
MY7cCKXFKCybubCD40Q6AFCDJBoHIkA5wzlwxzUa6ThVWqJmYvgD5Z
RvPg%%
Bağlantı izlemek için tıklayın veya dokunun.

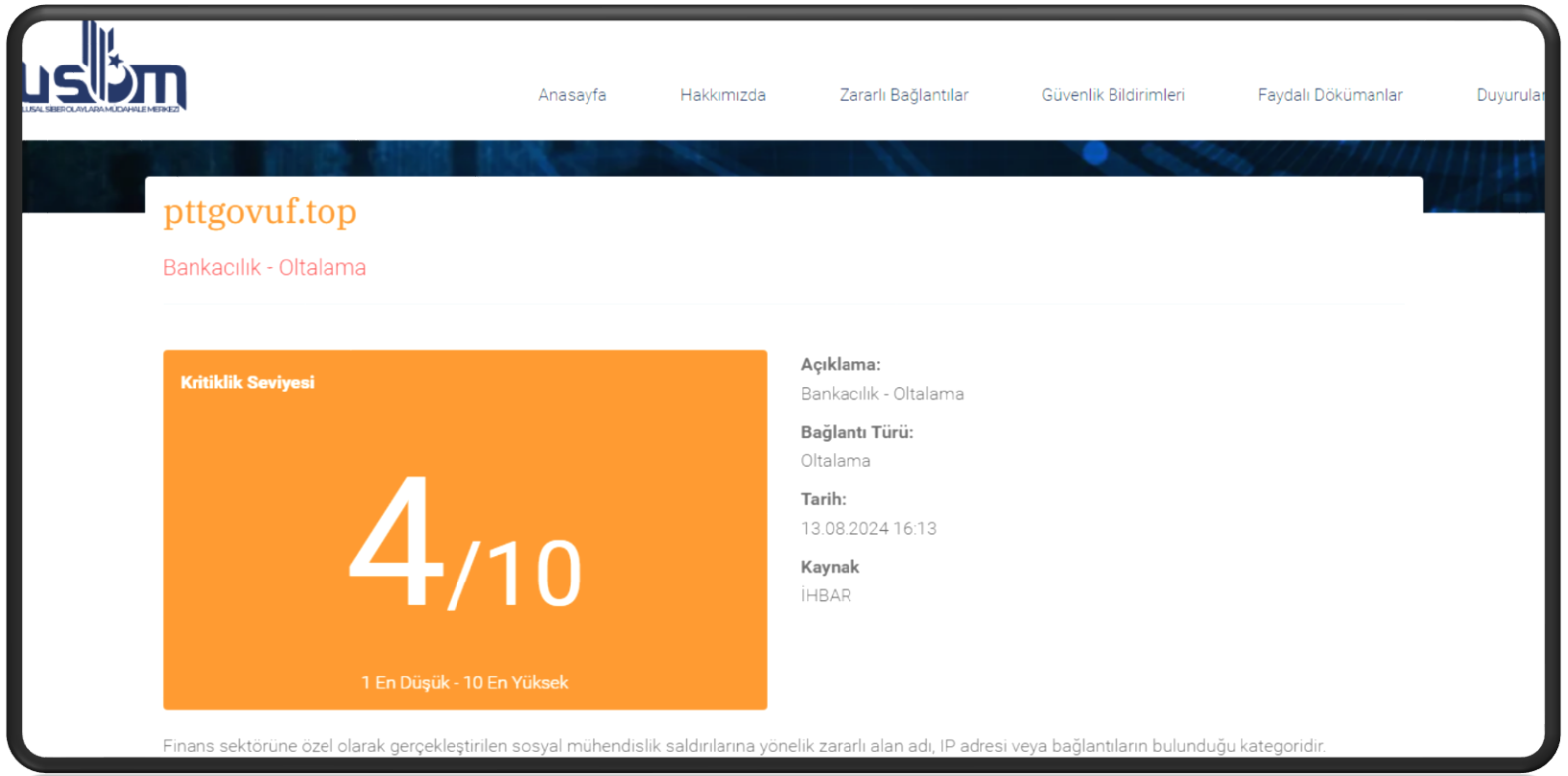
https://calendly.com/url?q=https://samoppoposteamwork
space.myclickfunnels.com/oorbe

Ödemeyi Tamamla

SAHTE PTTAVM SİSTEMİ (KİŞİSEL BİLGİ ÇALMA AMAÇLI)







Phishing Saldırılarından Korunmak İçin

- **Tanımadığın kişilerden gelen linklere tıklama.**
- **Gönderen e-posta adresini dikkatle kontrol et.**
- **Bilmediğin e-posta eklerini açma.**

Kimden: "PTT" <noreply@offer-66dfd.firebaseapp.com>
Kime: "nakyel" <[redacted]>
Gönderilenler: 24 Ocak Cumartesi 2026 13:52:39
Konu: Gönderiniz Beklemede - Gümrük Vergisi Ödemesi Gerekiyor

Bilinmeyen adres

Zero-Day Saldırıları

Yazılımda veya sistemde keşfedilen bir güvenlik açığının, bu açık için henüz bir yama veya çözüm geliştirilmeden kötü niyetli kişiler tarafından kullanılması sonucu gerçekleştirilen saldırılardır.

Cryptojacking

Saldırganların, kurbanların bilgisayarının, telefonunun veya diğer cihazlarının kaynaklarını izinsiz bir şekilde kullanarak kripto para madenciliği yapmasıdır. Kullanıcının cihazına zararlı bir yazılım yükleyerek veya İnternette gezinirken kripto madenciliği komutları barındıran bir web sitesine girdiğinizde, bilgisayarın işlem gücünü kripto para madenciliği için kullanmayı temel alan bir saldırı türüdür.

ZeroDay ve Cryptojacking Saldırılarından Korunmak İçin

ZeroDay (''Önleyemeyebilirim ama yayılmasını ve etkisini sınırlarım.")

- İşletim sistemini ve yazılımları güncel tut,
- Lisanslı antivirüs yazılımı kullan,
- Phishing ve Malware saldırılarından korunma yöntemlerini uygula

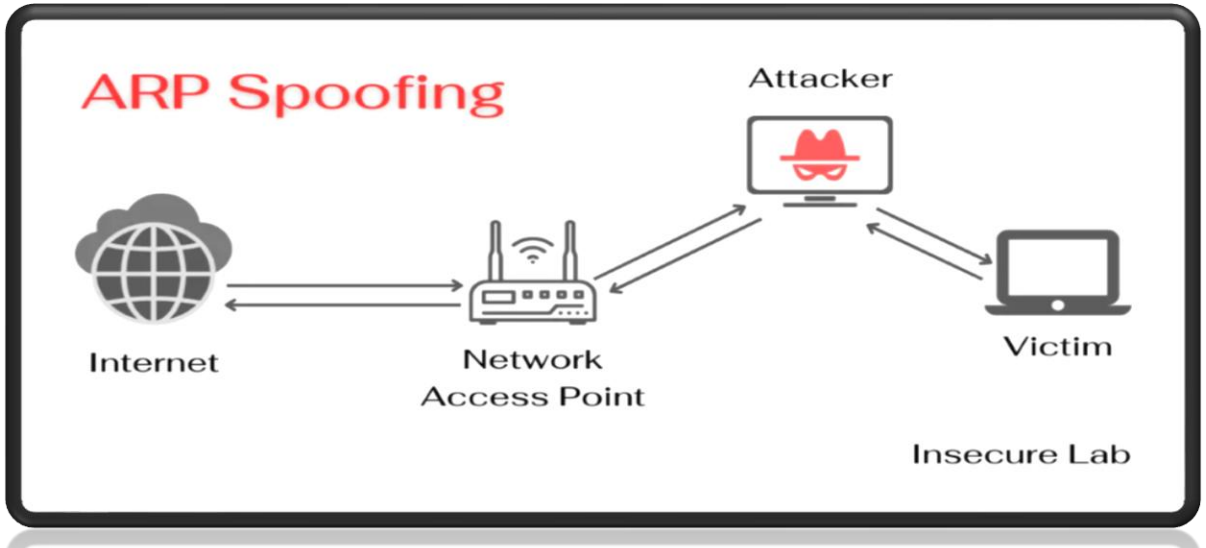
Cryptojacking

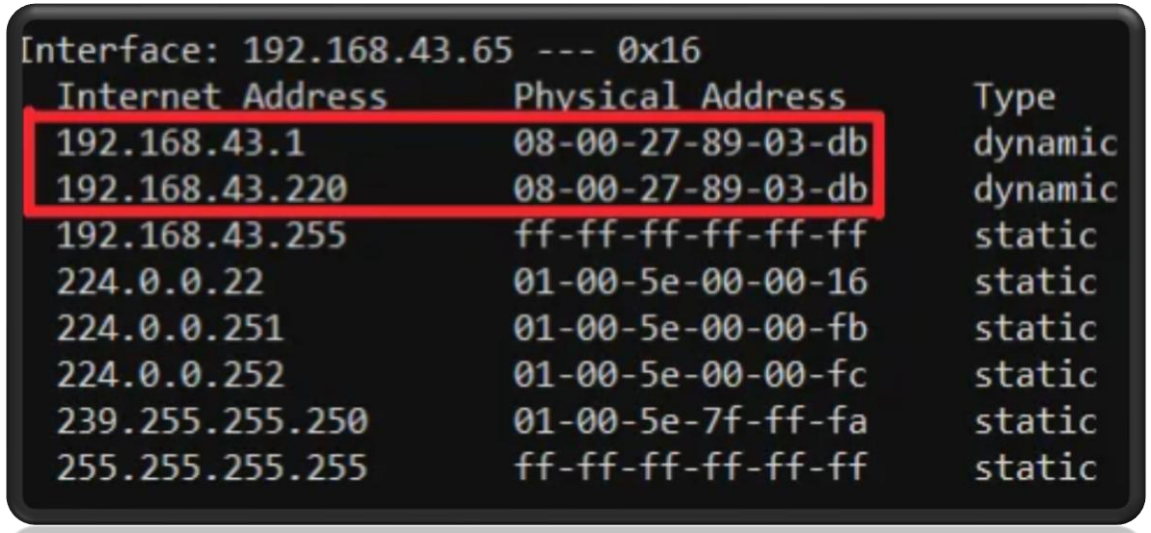
- Güncel tarayıcı ve işletim sistemi kullan.
- Lisanslı antivirüs yazılımı kullan,
- Phishing ve Malware saldırılarından korunma yöntemlerini uygula

Man-in-the-Middle (MitM) Saldırıları:

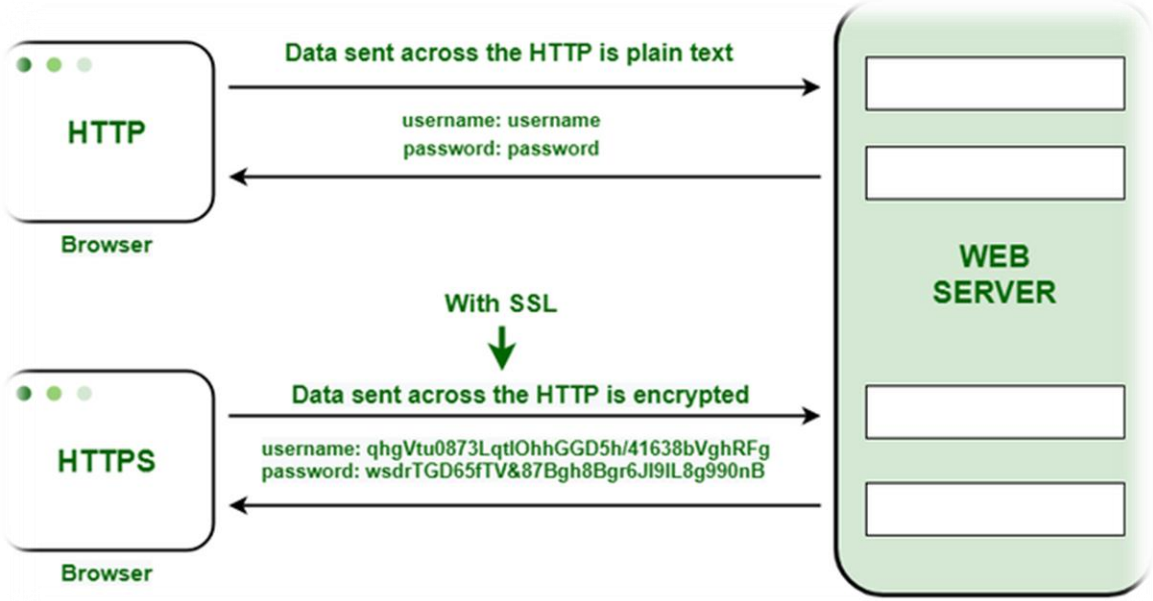
MitM saldırıları, saldırganın iletişimdeki iki taraf arasında gizlice veri alışverişini dinlemesidir. Bu sayede saldırgan, bilgileri çalabilir veya manipüle edebilir.

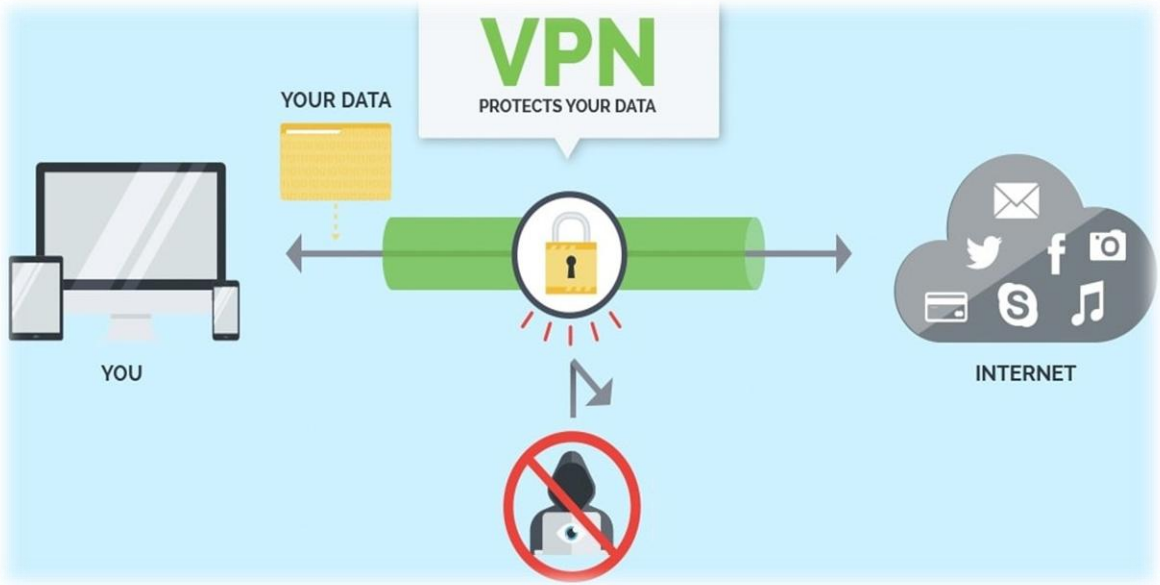
Örnek: Halka açık Wi-Fi ağı üzerinden gerçekleştirilen bir saldırıda, bir kullanıcı güvenli olmayan bu ağda oturum açtığında, saldırgan kullanıcı ile sunucu arasındaki veriyi dinleyebilir.





MITM saldırılarına karşı korunmanın en etkili yolu elbette güvenmediğiniz hiçbir ağda oturum açmamak ve eğer bağlanmak zorunda kalırsanız da veri şifreleme tekniklerini kullanmaktır.





(Güvenilir olmayan ağlara bağlanmamak en etkili korunma yöntemidir!)

APT (Advanced Persistent Threat - Gelişmiş Kalıcı Tehditler)

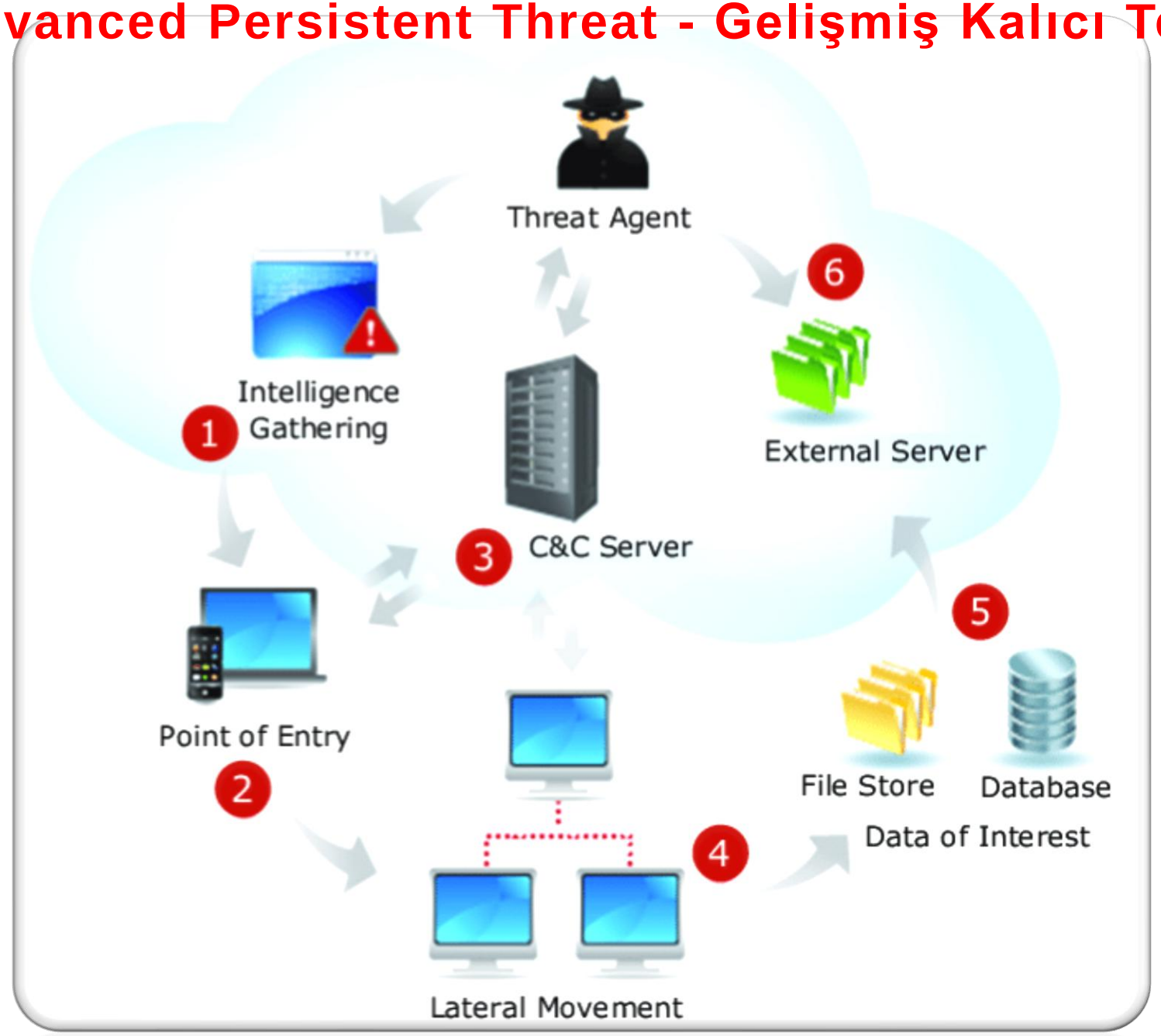
APT, genellikle iyi organize olmuş, uzun süreli, hedef odaklı ve gizli şekilde yürütülen siber saldırılardır. Amaç hızlıca zarar vermek değil; sisteme sızmak, fark edilmeden kalmak ve değerli verileri zaman içinde ele geçirmektir.

Advanced (Gelişmiş): Karmaşık teknikler kullanır.

Persistent (Kalıcı): Aylarca, hatta yıllarca sistemde kalabilir.

Threat (Tehdit): Ciddi ve stratejik bir risktir.

APT (Advanced Persistent Threat - Gelişmiş Kalıcı Tehditler)

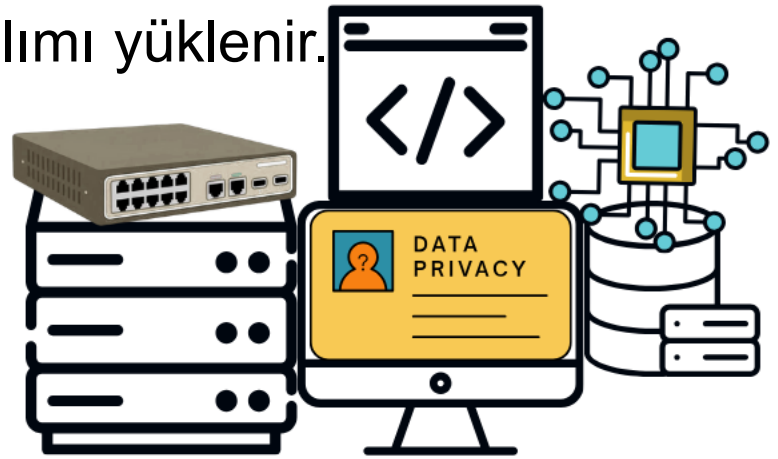


ÖRNEK VAKALAR

Sızma (Phishing)

1

- Kurum çalışanına bir **spear phishing** e-postası gönderilir.
- E-posta eki indirilir.
- Bilgisayara uzaktan kötücül ekran izleme **(Malware)** yazılımı yüklenir.
- Bilgisayarın kontrolü elde edilir.

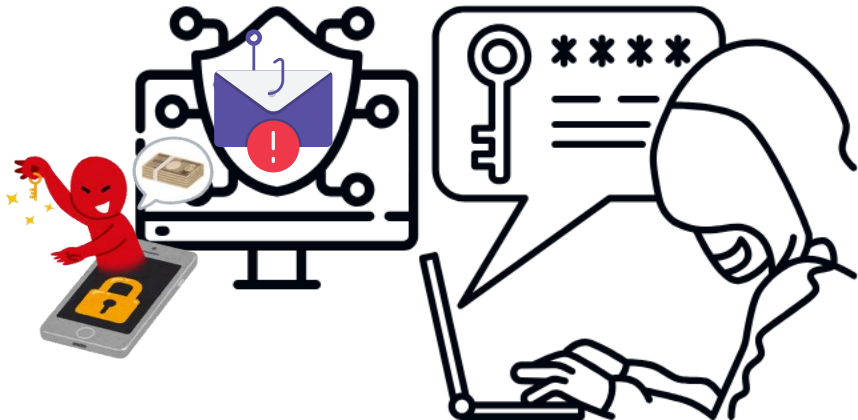


İç Ağ Keşfi ve Bilgi Toplama

- Kritik sunucular belirlenir.
- Ağ haritası çıkartılır.
- Çalışanların ekranları izlenir.
- Şifreler ele geçirilir.

Sonuç

- Veritabanına erişim
- Veri sızıntısı / Maddi kazanç



2

Sızma (Insider Threats)

- Çalışan USB ‘yi sistemine taktı.
- **ZeroDay** sayesinde kötücül yazılım **(virüs)** sisteme enfekte oldu.

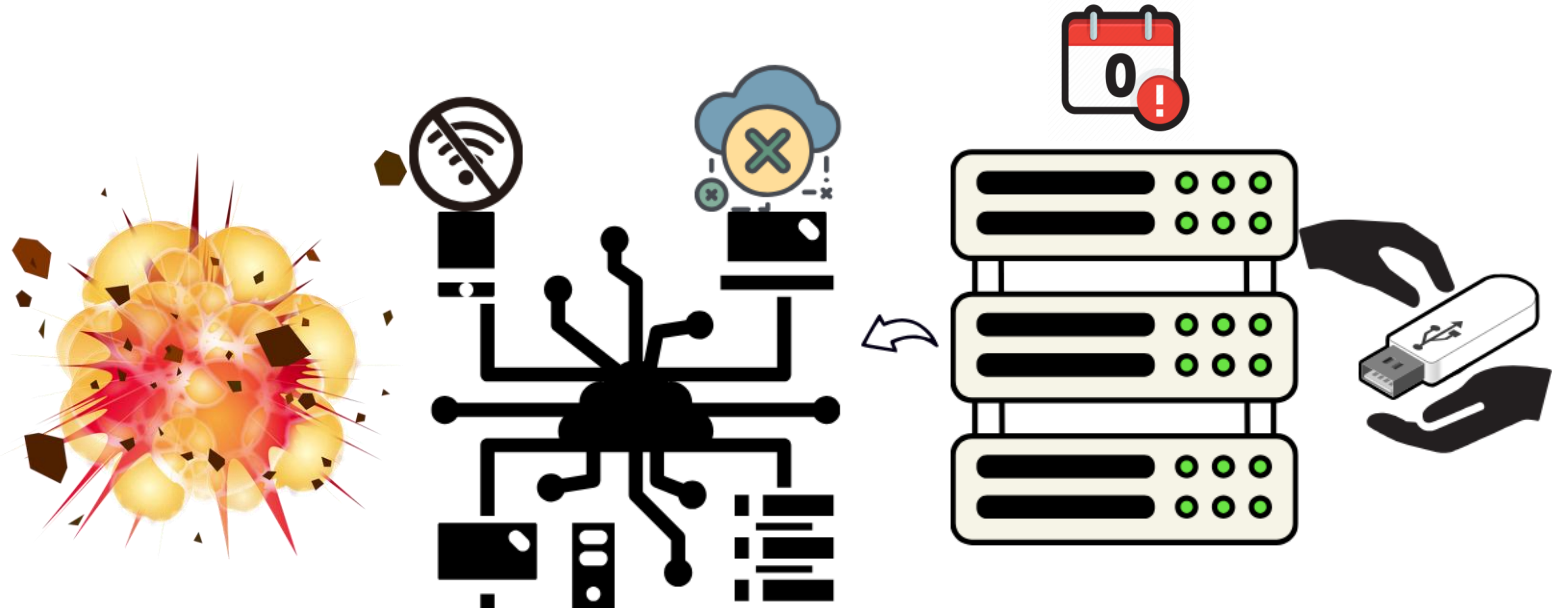
İç Ağ Keşfi ve Bilgi Toplama

- Kritik sistemler belirlendi.
- Ağ haritası çıkartıldı.
- Hedef sistem belirlendi

“İnternetsiz bir sistem mutlak güvenlik sağlamaz!”

Sonuç

- Hedefte fiziksel hasar



Sızma (ZeroDay)

3

- Ağ taraması ile SMB portu (445) açık olan sistem tespit edildi.
- Güncel olmayan sisteme uzaktan kod çalıştırılarak ‘’**Ransomware**’’ fidye yazılımı yüklendi.

İç Ağ Keşfi

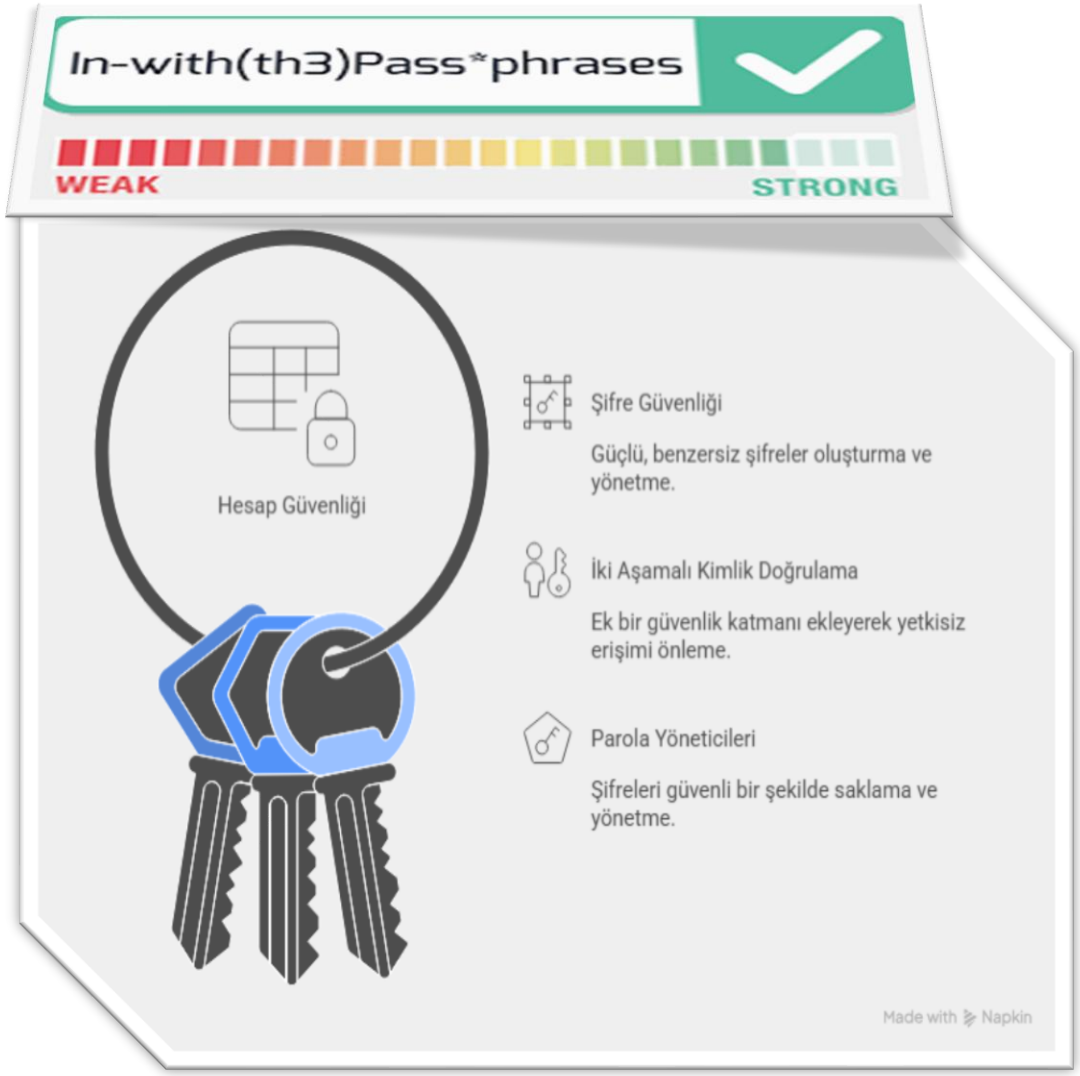
- Kötücül yazılım ağdaki **güncel olmayan** diğer sistemleri tespit etti.
- Tespit edilen zafiyetli portlarda uzaktan kod çalıştırarak kendini kopyalamaya devam etti.

Sonuç

- Dosyalar şifrelendi / Fidye talep edildi.
- Ulaştırma, Sağlık, Finans vs. birçok sektör durma noktasına geldi.

BU TEHDİTLERDEN BİREYSEL KORUNMA YÖNTEMLERİ

- İKİ FAKTÖRLÜ KİMLİK DOĞRULAMA KULLANIN
- GÜÇLÜ PAROLA KULLANIN
- İŞLETİM SİSTEMLERİNİZİ VE UYGULAMALARINIZI GÜNCEL TUTUN
- GÜNCEL LİSANSLI ANTİVİRÜS YAZILIMI KULLANIN
- BİLİNMEYEN E-POSTALARA DİKKAT EDİN VE EKLERİNİ AÇMAYIN
- SAHTE İNTERNET SİTELERİNDEN KAÇININ
- SOSYAL MÜHENDİSLİK SALDIRILARINA KARŞI DİKKATLİ OLUN
- SOSYAL MEDYA HESAPLARINIZI KORUYUN



Güçlü Parolaların Özellikleri

Karmaşıklık (A1!a+2@%3)

Uzunluk (En az 12-16 karakter)

Tekrarlanmaması (E-Devlet ≠ Netyetki ≠ Mail ≠ PC)

Tahmin Edilemezlik (Admin1990)

İki Faktörlü Kimlik Doğrulama (2FA)

İki faktörlü kimlik doğrulama, bir hesaba giriş yaparken yalnızca parolanızı kullanmak yerine, ikinci bir kimlik doğrulama katmanı ekleyen bir güvenlik yöntemidir. Bu, genellikle telefonunuza gönderilen bir kod veya bir uygulama üzerinden oluşturulan bir kod ile gerçekleştirilir.

2FA'nın en büyük avantajı; parolalar çalınsa bile, ikinci faktör olmadan hesaba erişim mümkün olmaz.

“ Siber güvenlik bir ürün değil, bir süreçtir “

“En zayıf halka her zaman insandır.”

“Şüphe etmek, güvende kalmaktır.”

SORU - CEVAP

“Her e-posta masum değildir.”

“Güven, doğrulama gerektirir.”

TEŞEKKÜRLER...

https://some.ogu.edu.tr