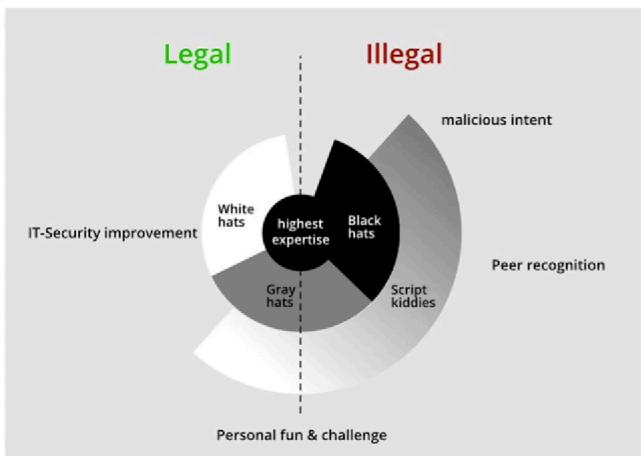




Cyber Security Notes

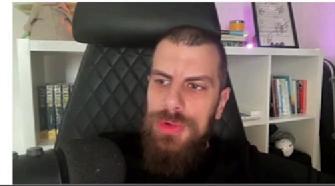


SIYAH SAPKALI HACKER (BLACK HAT HACKERS)



KAYNAK: <https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/>

- Amaçları kötüdür.
- Bilgisayar sistemlerine izinsiz erişmek, bilgileri çalmak veya zarar vermek gibi kötü niyetli eylemleri gerçekleştirirler.
- Saldırganlar, kişisel kazanç veya zarar verme amaçlarıyla hareket edebilirler.



BEYAZ SAPKALI HACKER (WHITE HAT HACKERS)

White hat hacker VS Black hat hacker



- Increases the security framework
- Develops a high-security structure
- Updates and regularly checks the security
- Develops systems like firewall, ad blocker, etc.



- Reduces security by stealing data
- Gains access to accounts and sensitive data
- Steals valuable data from the organization
- Gains access to restricted areas

KAYNAK: <https://www.wallarm.com/what/black-hat-hacker>

- Amaçları iyidir.
- Bilgisayar sistemlerinin güvenliğini test etmek veya zayıflıkları tespit etmek için izin almış güvenlik uzmanlarıdır.
- Sorunları tespit edip düzeltme konusunda organizasyonlara yardımcı olurlar.



Bug Bounty: Sistemlerdeki zafliyetleri bulmak için yapılan hacklemelerdir. Sistemin açıkları bulunmaya çalışılır ve bulununca da bu açıklar sistem sahiplerine iletilir. Sistem sahipleri, hacklere karşılığında ödül verebilir.

GRI SAPKALI HACKER (GREY HAT HACKERS)

White, gray and black hat comparison



WHITE HAT
Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws



GRAY HAT
May have good intentions, but might not disclose flaws for immediate fixes
Prioritize their own perception of right versus wrong over what the law might say



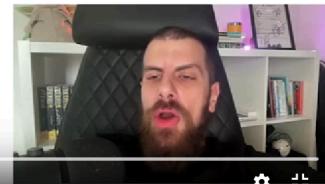
BLACK HAT
Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong
Exploit security flaws for personal or political gain—or for fun

KAYNAK: <https://lahjaty.com/white-hat-vs-black-hat/>



KAYNAK: <https://techcrunch.com/sponsor/king-university/different-types-of-hackers/>

- Amaçları karmaşıktır ve genellikle belirsizdir.
- İzin almadan bilgisayar sistemlerini test edebilirler, ancak bu işlemi kötü niyetli amaçlarla yapmazlar.
- Sistem zayıflıklarını tespit edip sahiplerine bildirirler, ancak izin almadan test yapma eğilimindedirler.



SOSYAL MÜHENDISLER (SOCIAL ENGINEERS)

Social Engineering

The Art of Human Manipulation

Definition

Social engineering is the act of manipulating people into divulging sensitive information or performing acts that compromise security.

Techniques

Phishing, pretexting, baiting, and tailgating

Targets

Employees, customers, and vendors

Goals

Obtain sensitive information, gain unauthorised access, or commit fraud

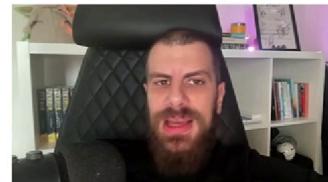
Prevention

Awareness, training, and robust security measures

KAYNAK: <https://www.stanfieldit.com/social-engineering/>



- Teknik bilgisayar becerileri yerine insanları manipüle etmeye odaklanan saldırganlardır.
- Kişisel bilgileri, kimlik bilgilerini veya giriş bilgilerini elde etmek için insanların güvenini kazanmaya çalışırlar.



SCRIPT KIDDIES

- Genellikle teknik bilgiye sahip olmayan veya sınırlı bilgiye sahip olan amatör saldırganlardır.
- Hazır yazılımları veya saldırın araçlarını kullanarak basit saldırılar gerçekleştirirler.
- Genellikle popüler olmayan hedeflere yönelirler.

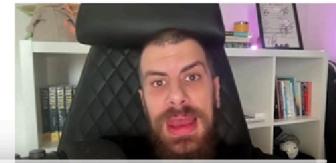
Hackers vs. script kiddies									
	<table border="1"> <thead> <tr> <th>HACKERS</th><th>SCRIPT KIDDIES</th></tr> </thead> <tbody> <tr> <td>Experience</td><td> <ul style="list-style-type: none"> More experienced </td></tr> <tr> <td>Knowledge</td><td> <ul style="list-style-type: none"> Inexperienced Limited knowledge and skills Launch exploits without knowing much about them Apt to quit </td></tr> <tr> <td>Methods</td><td> <ul style="list-style-type: none"> Skilled and knowledgeable Well researched Persist through challenges Use off-the shelf exploits but also can code their own and adapt methods to challenges Use off-the-shelf and beginner programs written by other people </td></tr> </tbody> </table>	HACKERS	SCRIPT KIDDIES	Experience	<ul style="list-style-type: none"> More experienced 	Knowledge	<ul style="list-style-type: none"> Inexperienced Limited knowledge and skills Launch exploits without knowing much about them Apt to quit 	Methods	<ul style="list-style-type: none"> Skilled and knowledgeable Well researched Persist through challenges Use off-the shelf exploits but also can code their own and adapt methods to challenges Use off-the-shelf and beginner programs written by other people
HACKERS	SCRIPT KIDDIES								
Experience	<ul style="list-style-type: none"> More experienced 								
Knowledge	<ul style="list-style-type: none"> Inexperienced Limited knowledge and skills Launch exploits without knowing much about them Apt to quit 								
Methods	<ul style="list-style-type: none"> Skilled and knowledgeable Well researched Persist through challenges Use off-the shelf exploits but also can code their own and adapt methods to challenges Use off-the-shelf and beginner programs written by other people 								

Script Kiddies

Motivation: Use existing malware to break into personal devices and private networks

Potential Targets: Internet users and businesses

KAYNAK: <https://us.norton.com/blog/emerging-threats/types-of-hackers>



SIBER GUVENLIK UZMANLARI



Firewall: Ağ trafiğini izleyen ve izin verilen trafiği geçiren, izin verilmeyen trafiği engelleleyen bir güvenlik cihazıdır.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Sizma Testi Yöntemleri (Black Box – Gray Box – White Box):** Sizma testi sırasında test edilen sistem veya uygulamanın bilgilendirilme düzeyine göre kullanılan yaklaşımalar.
 - **Siyah kutu (Black Box),** hiçbir önceden bilgiye sahip olunmadan test edilirken, **beyaz kutu (White Box)** tam bilgiye sahip olunarak test edilir. **Gri kutu (Gray Box)** ise kısmi bilgiye sahip olunarak yapılan bir yaklaşımı ifade eder.



GENEL SİBER GÜVENLİK KAVRAMLARI



- **Exploit:** Güvenlik açığı veya zayıflığı kullanarak bir sisteme veya uygulamaya sızmayı veya kontrol etmemeyi amaçlayan yazılım veya kod parçası.

GENEL SİBER GÜVENLİK KAVRAMLARI



KAYNAK: <https://stock.adobe.com/>

- **Google Hacking (Google Dork):** Google gibi arama motorları kullanarak hassas veya gizli bilgilere erişmeye çalışan siber saldırılar veya arama sorguları.



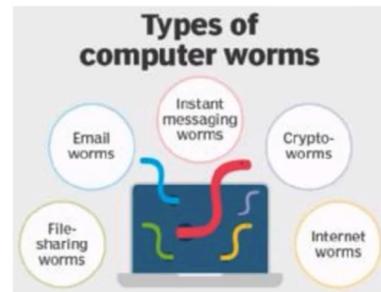
Hack Türleri

2- WORM (SOLUCANLAR)

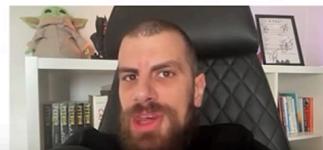
- Worm (Solucan), bilgisayar ağlarında hızla yayılan ve çoğalan, zararlı bir yazılım türüdür.
- Bir Worm, bir bilgisayar ağı veya cihaz içindeki diğer cihazlara kendini kopyalayabilecek bir zararlı yazılımdır.
- Worm'ler, kendilerini çoğaltarak hızla yayılır ve genellikle bilgisayar sistemlerine zarar verirler.

Nasıl Bulaşır?

- Worm'ler, genellikle bilgisayar ağlarında veya internet üzerindeki güvenlik açıklarını kullanarak yayılırlar.
- İnfekte edilmiş bir cihazdan diğer cihazlara otomatik olarak kopyalanabilirler.
- E-posta eklentileri veya indirilebilir dosyalar gibi bulaştırma yöntemleri de kullanılabilir.



KAYNAK: <https://bkhost.vn/blog/worm-sau-may-tinh/>



3- SPYWARE (CASUS YAZILIM)

- Spyware (Casus Yazılım), kullanıcının bilgisayarını veya diğer cihazlarını izlemek, bilgi toplamak ve genellikle izinsiz olarak kişisel bilgileri çalmak amacıyla tasarlanmış zararlı yazılımlardır.
- Spyware, kullanıcının bilgisayar aktivitelerini izleyen ve toplayan bir yazılım türüdür. Bu yazılım, genellikle kullanıcının izni olmadan veya farkında olmadan kurulur.
- Spyware, kullanıcının gezdiği web sitelerini, klavye girişlerini, e-posta adreslerini, parolaları ve diğer kişisel bilgileri kaydedebilir.



KAYNAK: <https://www.fortinet.com/de/resources/cyberglossary/spyware>



5- TROJAN (TRUVA ATI)

EXAMPLES OF TROJAN HORSE VIRUS



KAYNAK:
<https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/>



- Trojan (Truva ATI), görünüşte zararsız veya yararlı bir program veya dosya gibi davranışarak, kullanıcının bilgisayarına kötü amaçlı yazılım bulaştırmak için tasarlanmış bir tür zararlı yazılımdır.
- Görünüşte zararsız bir program veya dosya gibi davranışır, bu nedenle kullanıcılar tarafından kolayca kurulabilir.
- Amaçları, bilgisaya kötü amaçlı yazılım, casus yazılım veya diğer zararlı işlevleri yüklemektir.

Nasıl Bulaşır?

- Trojanlar, genellikle bilgisayar kullanıcılarına güvenilir ve çekici görünen e-posta ekleri, indirilebilir dosyalar veya uygulamalar aracılığıyla bulaştırılır.
- Kullanıcılar, bu dosyaları veya uygulamaları indirip açtıklarında Trojan bilgisayarlarına bulaşır.



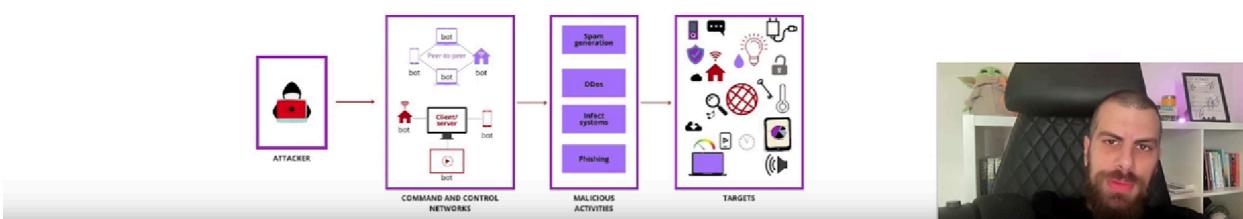
6- BOTNETS

- Bot terimi robotun kısaltmasıdır.
- Amacı, bilgisayarınızı bir bot'a (zombi olarak da bilinir) çevirebilen kötü amaçlı yazılımları dağıtmaktır. Böyle bir durumda bilgisayarınızı, sizin haberiniz olmadan internet üzerinden otomatik görevleri gerçekleştirebilir.

Nasıl Bulaşır?

- Botnetler, bilgisayarlara veya cihazlara bulaşmak için genellikle kötü amaçlı e-posta ekleri, bulaşmış web siteleri, güvensiz uygulamalar veya diğer kötü niyetli yazılımlar aracılığıyla yayılırlar.
- Kullanıcılar, bu bulaşmış dosyaları veya bağlantıları açtıklarında botnet bilgisayarlarına bulaşabilir.

Botnet command and control architecture



7- RANSOMWARE(FİDYE YAZILIMI)

Types of Ransomware

Crypto Ransomware
This type of ransomware encrypts files on a computer so that the user loses access to essential files.

Locker Ransomware
This type of ransomware locks victims out of their device and prevents them from using the device.

Examples:

- BadRabbit
- Cryptolocker
- SamSam
- Thanos
- Ryuk
- WannaCry
- NotPetya and Petya

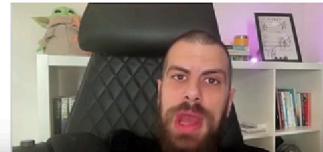
KAYNAK:
<https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-ransomware-attack/>

- Ransomware, kötü amaçlı bir yazılım türüdür ve adını rehine verileri fidye karşılığında serbest bırakma eyleminden alır.

- Ransomware, dosyaları veya bilgisayarın tamamını şifreleyerek kullanıcının erişimini engeller.

Nasıl Bulaşır?

- Ransomware, genellikle sahte e-posta ekleri, kötü amaçlı web siteleri, güvensiz indirme kaynakları veya açıkları kullanarak bilgisayarlara bulaşır.
- Kullanıcılar, kötü amaçlı dosyaları veya bağlantıları açtıklarında ransomware bulaşabilir.

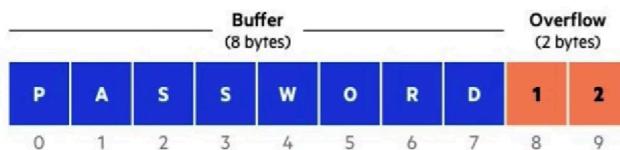
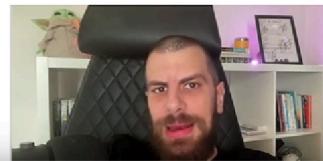


8. BUFFER OVERFLOW:



- Bir programın bellek alanının sınırlarının dışına çıkılarak kötü amaçlı kodların çalıştırılmasına izin veren bir güvenlik açığı.

- Örnek: Morris Worm, buffer overflow açığı kullanarak ilk büyük çaplı internet saldırısını gerçekleştirmiştir.



KAYNAK: <https://www.imperva.com/learn/application-security/buffer-overflow/>

9. CROSS-SITE REQUEST FORGERY (CSRF):

The diagram illustrates a CSRF attack flow:

- Hacker** creates a malicious site that looks like a legitimate site.
- Hacker** shares the link through email or social media.
- A potential victim opens the link thinking they are going to a legitimate website.
- The page is loaded and the malicious payload is executed!

KAYNAK: <https://learn.snyk.io/lesson/csrf-attack/>

• Saldırganların kullanıcıların hesaplarını izinsiz olarak farklı bir web sitesi üzerinden işlem yapmaya zorladığı bir saldırı türü.

• Örnek: Bir saldırgan, kullanıcının banka hesabından para transferi yapmasını isteyen sahte bir web sayfası oluşturabilir.

[Video Player Controls]

TAM EKRANDAN ÇIKMAK İÇİN ESC TUŞUNA BASIN

10. CROSS-SITE SCRIPTING (XSS):

The diagram illustrates an XSS attack flow:

- Perpetrator discovers a website having a vulnerability that enables script injection.
- Perpetrator injects the website with a malicious script that steals each visitor's session cookies.
- For each visit to the website, the malicious script is activated.
- Visitor's session cookie is sent to perpetrator.

KAYNAK: <https://www.mobindustry.net/blog/11-web-application-security-best-practices-you-need-to-know/>

• Saldırganların web sitelerine zararlı kodlar ekleyerek kullanıcıların tarayıcılarında çalışmasını sağladığı bir saldırı türü.

• Örnek: Bir saldırgan, kullanıcılara zararlı bir JavaScript kodu içeren sahte bir e-posta gönderebilir.

• [Image of a hand pointing at an envelope icon]

• [Video Player Controls]

11. BROKEN ACCESS CONTROL:

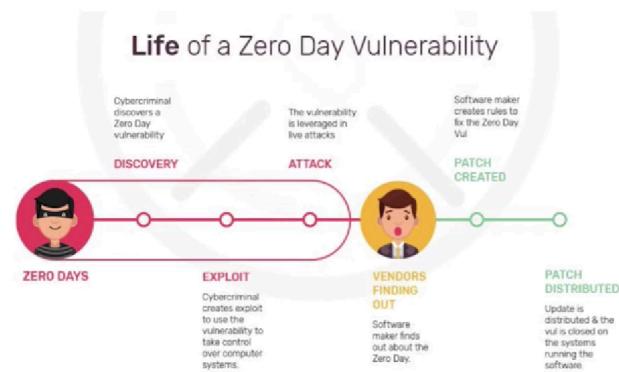


- Kullanıcıların izin verilmeyen kaynaklara veya işlevlere erişim sağlamaına izin veren bir güvenlik açığı.

- Örnek: Bir kullanıcının hesap ayarlarını değiştirmesi gereken bir işlevin, yetkisiz erişime açık olması.

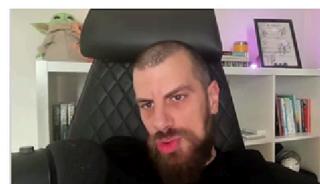


12. ZERO-DAY EXPLOITS (0 DAYS):

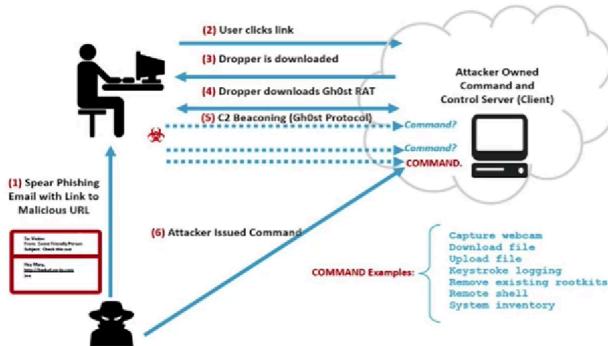


- Yazılım veya sistem güvenlik açıklarının keşfedildiği ve henüz üretici tarafından düzeltilemediği durumlar.

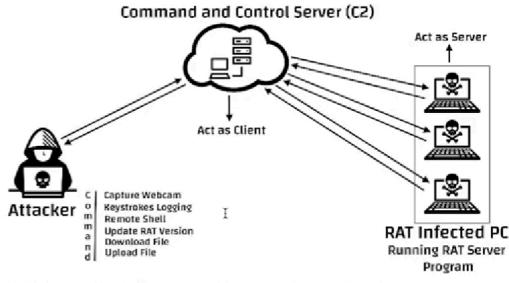
- Örnek: Saldırganlar, henüz açığı kapatılmamış bir yazılık veya işletim sistemi güvenlik açığından faydalanabilirler.



14. RAT (REMOTE ACCESS TROJAN):



KAYNAK: <https://medium.com/codex/the-birth-and-rise-of-remote-access-trojans-rats-2819d7ab2b06>



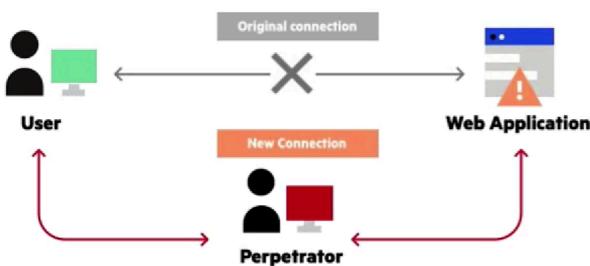
KAYNAK: <https://hackerterminal.com/what-is-remote-access-trojan/>

- Saldırganların bir bilgisayar sistemine uzaktan erişim sağlamak amacıyla kullanılan truva atları.

- Örnek: Poison Ivy RAT, uzaktan bilgisayar kontrolü sağlayan bir RAT örneğidir.



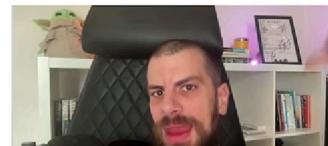
15. MAN-IN-THE-MIDDLE (MITM) SALDIRILARI:



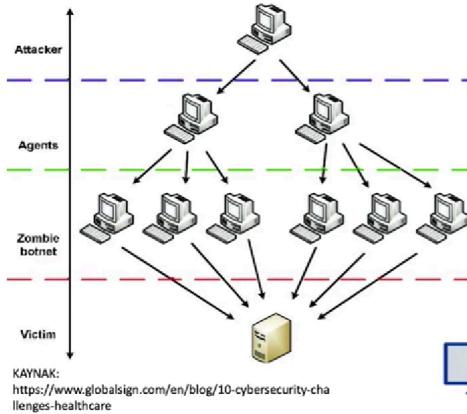
KAYNAK: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

- Saldırganların iki iletişen tarafın arasına girerek iletileri izlemesine veya manipüle etmesine olanak tanıyan saldırı türü.

- Örnek: Bir kişi, halka açık bir Wi-Fi ağlarından verileri izleyebilir veya değiştirebilir.

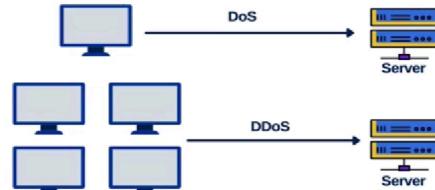


16. DENIAL-OF-SERVICE (DOS) SALDIRILARI:



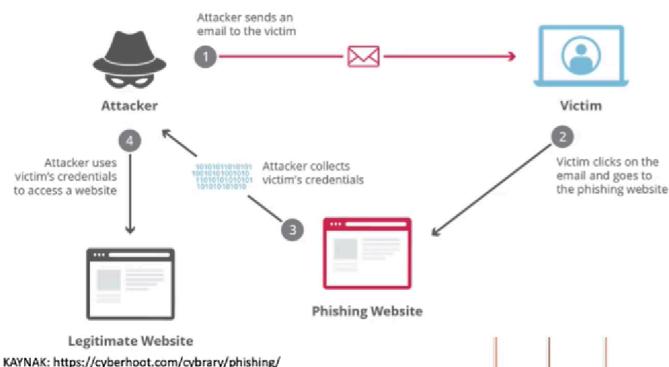
- Hedeflenen sistem veya ağa yoğun talep gönderilerek hizmetin kesilmesine neden olan saldırılardır.

• Örnek: SYN Flood saldırısı, bir sunucunun hizmet veremeyecek kadar çok bağlantı isteği aldığı bir tür DOS saldırısıdır.



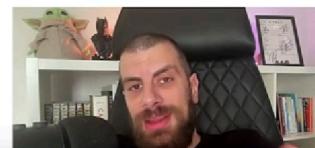
Sosyal Mühendislik Çeşitleri

I. PHISHING (YEMLEME)



- Saldırganlar, sahte e-postalar, web siteleri veya mesajlar kullanarak kullanıcıları kişisel bilgileri ifşa etmeye veya kötü amaçlı yazılımları indirmeye ikna etmeye çalışır.

• Örnek: Kullanıcılara sahte bir banka e-postası göndererek, hesap bilgilerini paylaşmalarını isteyen bir phishing saldırısı.



II. SPEAR PHISHING

Phishing vs. spear phishing vs. whaling

Phishing

A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.



Spear phishing

A type of phishing that targets individuals



Whaling

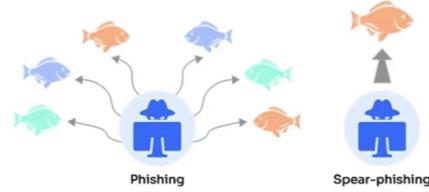
A form of spear phishing that targets high-ranking victims within a company.



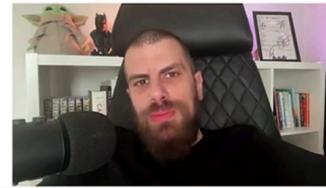
- Phishing'in özelleştirilmiş bir türüdür; saldırganlar belirli kişileri hedef olarak daha inandırıcı mesajlar gönderir.

- Örnek: CEO'yu taklit eden bir e-posta göndererek finans müdüreni para transferi yapmaya ikna etmeye çalışan bir spear phishing saldırısı.

KAYNAK: <https://www.wallarm.com/what/what-is-a-spear-phishing-attack-how-to-prevent-one>



KAYNAK: <https://www.valimail.com/guide-to-phishing/spear-phishing-vs-phishing/>



III. SHOULDER SURFING (OMUZ SÖRFÜ)



- Saldırganlar, birisinin bilgisayar ekranını veya klavyesini izleyerek hassas bilgilere erişim sağlamaya çalışır.

- Örnek: Halka açık bir Wi-Fi ağına bağlıken, yan masada oturan kişinin şifresini izlemek.



IV. DUMPSTER DIVING (ÇÖP KARIŞTIRMA)

Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



KAYNAK: <https://www.techtarget.com/searchsecurity/definition/dumpster-diving>

- Saldırganlar, kurumların veya bireylerin çöplerini karıştırarak hassas bilgilere ulaşmaya çalışır.

- Örnek: İşyerinin atıklarını karıştırarak, bilgisayarların atılan belgeleri üzerinden önemli bilgilere erişmeye çalışan bir saldırgan.



V. ROLE PLAYING (ROL YAPMA)



- Saldırganlar, güven kazanmak veya inandırıcılıklarını artırmak için sahte bir rol üstlenirler.

- Örnek: Teknik destek uzmanı gibi davranarak, kullanıcılarından uzaktan bilgisayarlara erişim izni talep eden bir role playing saldırısı.



VI. PRETEXTING (BAHANE UYDURMA)

Pretexting Attack Techniques



1. A fraudster **impersonates a trusted authority** and crafts a scenario to reach out to their victims.



2. The victim **believes the scenario** and shares any information the 'trusted' authority requests.



3. The fraudster **gains valuable information** from their victim and often uses it maliciously.

KAYNAK: <https://www.wallarm.com/what/pretexting-types-and-prevention-methods>

KAYNAK: <https://us.norton.com/blog/online-scams/what-is-pretexting>

- Saldırganlar, inandırıcı bir bahane uydurarak kişilerden bilgi veya yardım talep ederler.

- Örnek: Sahte bir müşteri temsilcisi gibi davranışarak, bir kişinin banka hesabını çalmaya çalışan bir pretexting saldırısı.



VII. BAITING (YEMLEME)



KAYNAK: <https://www.avestagroup.net/Details/104>

VIII. TAILGATING (KUYRUKTA SÜRÜNME)



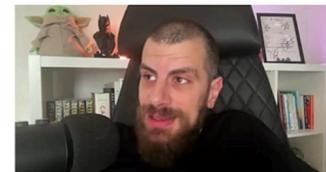
KAYNAK: <https://huperlab.com/products/3d-ai-video-analytics/3d-tailgating-detection/>

- Saldırganlar, birisinin yetkili bir alana girmesine izin vermesini bekleyerek güvenlik önlemlerini atlarlar.

- Örnek: Bir işyerinin girişinde başkasının arkasından girerek içeri sızma girişimi.



KAYNAK:
<https://arindamccctvaccesscontrol.blogspot.com/search/label/Globally%20Tailgating?m=0>



IX. QUID PRO QUO (KARŞILIK BEKLEME)



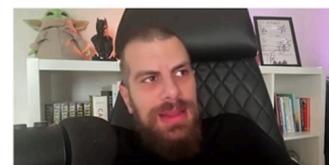
KAYNAK: <https://legal.thomsonreuters.com/blog/quid-pro-quo-social-engineering-infographic-and-explanation/>



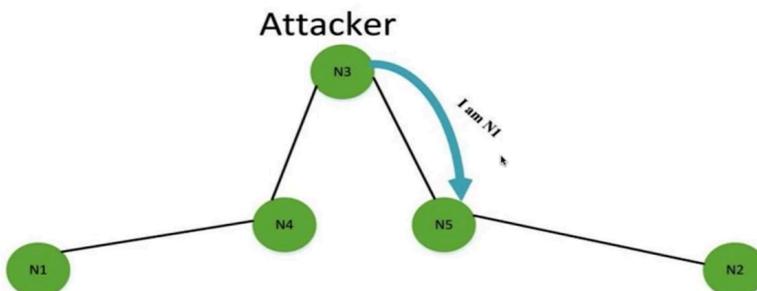
QUID PRO QUO

- Saldırganlar, kullanıcıları bir hizmet sunmaya veya yardım etmeye söz vererek bilgi elde etmeye çalışır.

- Örnek: Sahte bir teknik destek uzmanı olarak arayan saldırgan, bilgisayarın şifresini öğrenmek için yardım isteyebilir.

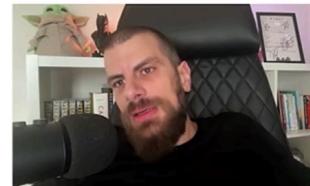


X. IMPERSONATION (KİMLİK TAKLİDİ)



KAYNAK:
https://www.researchgate.net/figure/A-simple-impersonation-attack-behavior_fig5_282856952

- Saldırganlar, başkasının kimliğini taklit ederek güven kazanmaya çalışır.
- Örnek: Birinin telefon numarasını taklit ederek, sahte bir kimlikle banka işlemi yapmaya çalışan bir impersonation saldırısı.



XI. PHARMING (ÇİFTÇİLİK)

Phishing

VS

Pharming

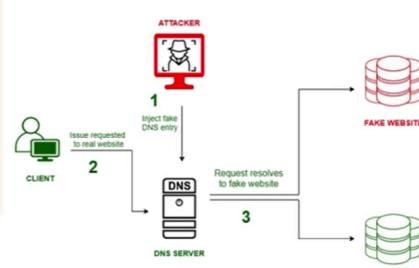
Easier to identify
Targets a single person
Malicious e-mail sent to inbox
Requires the user to manually click the link to activate code



Trickier to identify
Multiple simultaneous targets
Malicious code installed on computer
Redirects automatically without user needing to click

- Saldırganlar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini toplamaya çalışır.

- Örnek: Kullanıcıları sahte bir banka web sitesine yönlendiren ve giriş bilgilerini çalmaya çalışan bir pharming saldırısı.

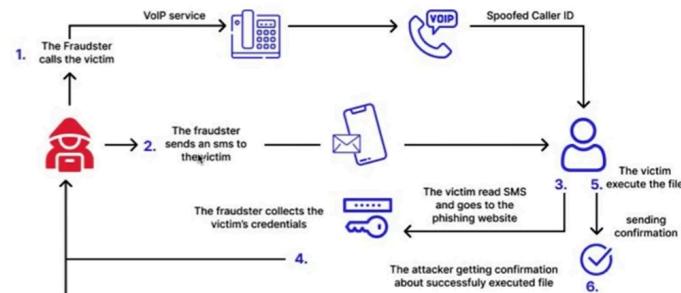


KAYNAK:
<https://www.linux-wlan.org/what-is-the-difference-between-phishing-and-pharming>

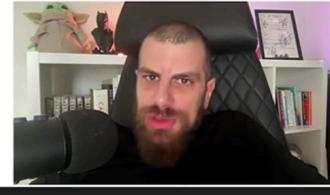
KAYNAK:
<https://www.geeksforgeeks.org/pharming-attack-prevention-and-examples/>



XII. VISHING (SESLİ FISHING)

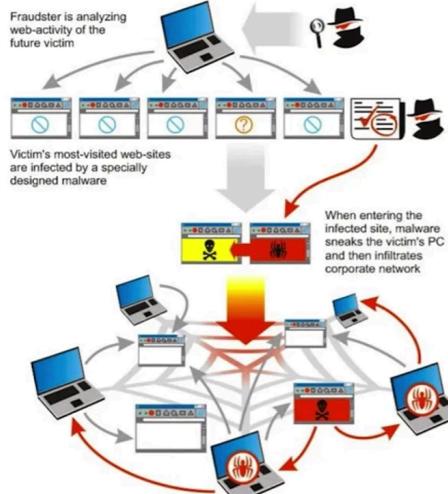


- Saldırganlar, telefonla arayarak kurbanları kişisel bilgileri veya finansal bilgileri vermek konusunda kandırmaya çalışır.
- Örnek: Sahte bir banka temsilcisi olarak arayan saldırgan, müşterilerden hesap bilgilerini vermesini isteyebilir.



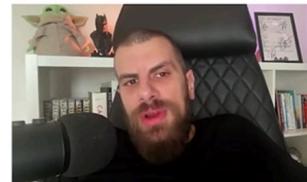
XIII. WATER HOLING

The “Watering hole” attack



- Saldırganlar, kurbanlarının sık kullandığı web sitelerini hedef alarak kötü amaçlı yazılım veya phishing kampanyaları düzenler.

- Örnek: Bir sektörün ilgi çekici bir web sitesini hangleten ve ziyaretçilerini kötü amaçlı yazılım ile enfekte etmeye çalışan bir water holing saldırısı.



Hacker Metodolojisi

HACKER METODOLOJİSİ



(aşamaların detaylarını da not al)

PAROLA SALDIRILARI NEDİR?

- Parola saldıruları, kötü niyetli kişilerin veya yazılımın bir hesaba veya sistemdeki parolayı tahmin etmeye veya kirarak yetkisiz erişim elde etmeye çalıştığı siber saldırı türleridir.

Aşağıda bazı parola saldırısı türleri ve örnekleri verilmiştir:

1. Brute Force Saldırısı:

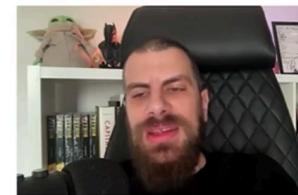
Örnek: "aaaaa", "aaaab", "aaaac", ...



<https://ipreview.net/d/1733uasccfs41.jpg?width=1080&crop=square&auto=webp&s=71b8d997fa7a7e91560ea82b56572a9e>

2. Dictionary Saldırısı:

Örnek: "password", "admin", "123456".



3. Phishing Saldırısı:

Örnek: Kullanıcıların banka hesap bilgilerini girmelerini isteyen sahte bir banka web sitesi.

4. Rainbow Table Saldırısı:

Örnek: Önceden hesaplanmış MD5 veya SHA-1 karma değerlerini içeren bir veritabanı.

Sertifikalar

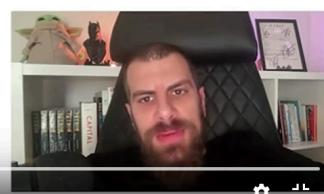
TAM EKRANDAN ÇIKMAK İÇİN **ESC** TUŞUNA BASIN

OFFENSIVE SECURITY (OSWE, OSCE, OSCP, OSWP)

- Offensive Security, siber güvenlik alanında eğitim ve sertifikasyon programları sunan bir şirkettir. Offensive Security'nin sunduğu bazı önemli sertifikalar şunlardır:
- OSCP (Offensive Security Certified Professional):** OSCP, Offensive Security'in en popüler ve tanınmış sertifikasıdır.
- OSCE (Offensive Security Certified Expert):** OSCE, bilgisayar güvenliği uzmanlarının bilgisayar sistemlerine sızma testleri yapma yeteneklerini daha derinlemesine göstermelerine olanak tanır.
- OSWE (Offensive Security Web Expert):** OSWE sertifikası, web uygulamalarının güvenliğini test etme ve web uygulama sızma testleri yapma yeteneklerini ölçer.
- OSWP (Offensive Security Wireless Professional):** OSWP sertifikası, kablosuz ağ güvenliği ile ilgilenen kişilere yöneliktedir.



KAYNAK:
<https://www.offsec.com/wp-content/uploads/2022/10/Artboard-1@2x.png>



Bireysel sertifikalar

- Juniorken genellikle sertifika bekłentisi olmaz.



BTK AKADEMI

CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL)

- CISSP, bilgi sistemleri güvenliği profesyonelleri için dünya genelinde tanınmış bir sertifikadır.
- Bilgi güvenliği yönetimi, risk yönetimi, güvenlik mimarisi ve diğer konularda uzmanlaşmış profesyonellere yönelikdir.



Certified Information
Systems Security Professional

KAYNAK: <https://www.cm-alliance.com/cissp-training-faqs>



BTK AKADEMI

CEH (CERTIFIED ETHICAL HACKER)



KAYNAK: <https://www.credly.com/org/ec-council/badge/certified-ethical-hacker-ceh>

- CEH sertifikası, etik hackerlar için tasarlanmıştır.
- Bu sertifika, ağları güvenlik açıklarını tespit etmek ve kapatmak için yetenekli hale getirmek isteyen profesyoneller için geçerlidir.



COMPTIA SECURITY+



KAYNAK:
<https://www.innovativelearning.eu/products/comptia-cybersecurity/comptia-security.html>

- CompTIA Security+, temel siber güvenlik kavramlarını ve uygulamalarını kapsayan bir sertifikadır.
- Bu sertifika, siber güvenlik kariyerine yeni başlayanlar veya temel bilgiye sahip olanlar için uygundur.



CCNA CYBEROPS (CISCO CERTIFIED NETWORK ASSOCIATE - CYBEROPS)



- CCNA CyberOps, ağ güvenliği ve siber güvenlik alanlarında uzmanlaşmak isteyen ağ profesyonelleri için Cisco tarafından sunulan bir sertifikadır.



KAYNAK: <https://www.fccmeredith.org/ccna-cyber-ops-certification>



CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)


CCSP®

Certified Cloud
Security Professional

An  Certification

KAYNAK: <https://cycubix.com/2022/04/04/isc2-ccsp-martina-costello/>

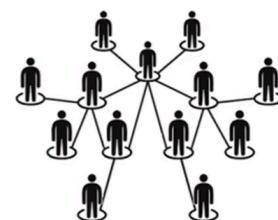
- CCSP, bulut bilişim güvenliği uzmanları için tasarlanmış bir sertifikadır.
- Bulut ortamında güvenliği sağlamak için gereken bilgi ve becerileri ölçer.



SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Bilgi Güvenliği Uzmanı (Information Security Specialist):

- Güvenlik duvarlarını yapılandırır, güvenlik yazılımını güncellerler.



Ağ Güvenliği Mühendisi (Network Security Engineer):

- Ağ içi iletişimini güvenli bir şekilde gerçekleştirden emin olurlar.
- DoS saldırılarına karşı savunma önlemleri geliştirirler.

Sızma Testi Uzmanı (Penetration Tester):

- Örneğin, organizasyonun web uygulamasında açıklar bularak güvenlik zayıflıklarını ortaya çıkarırlar.

Güvenlik Analisti (Security Analyst):

- Örneğin, bir kullanıcının hesabının ele geçirilmesini tespit edip bu olayı incelerler.



Kimlik ve Erişim Yönetimi Uzmanı (Identity and Access Management Specialist):

- Örneğin, bir işletme için tek oturum açma (Single Sign-On) sistemini uygularlar.

SIBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Veri Güvenliği Analisti (Data Security Analyst):

- Bir sağlık kurumu için hastaların tıbbi kayıtlarının güvenliğini sağlarlar.



Güvenlik Mimar (Security Architect):

- Bulut tabanlı bir hizmetin güvenliğini sağlamak için mimari planlar hazırlarlar.

Olay Yanıtı Uzmanı (Incident Response Specialist):

- Bir fidye yazılım saldırısına karşı hızlı bir kurtarma planı oluştururlar.

Uygulama Güvenliği Uzmanı (Application Security Specialist):

- Bir e-ticaret sitesinin web uygulamasının güvenliğini denetlerler.



Eğitim ve Farkındalık Uzmanı (Training and Awareness Specialist):

- Sahte e-posta kampanyaları düzenleyerek çalışanların dikkatini çekerler.

SIBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Yazılım Geliştirme Güvenliği Danışmanı (Secure Development Consultant):

- Yazılım geliştiricilere güvenlik açıklarını düzeltme konusunda rehberlik ederler.



Güvenlik Denetçisi (Security Auditor):

- Bir finans kuruluşunun güvenlik prosedürlerini denetlerler.

Mobil Uygulama Güvenliği Uzmanı (Mobile Application Security Specialist):

- Bir bankanın mobil bankacılık uygulamasının güvenliğini test ederler.

Güvenlik Ekip Lideri (Security Team Leader):

- Bir büyük organizasyonun güvenlik ekibinin liderliğini yaparlar.



Veri Gizliliği Danışmanı (Data Privacy Consultant):

- GDPR gibi düzenlemelere uyum sağlamak için bir şirkete danışmanlık yaparlar.

SIBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Endüstriyel Kontrol Sistemleri Güvenliği Uzmanı (Industrial Control Systems Security Specialist):

- Bir enerji santralinin ICS güvenliğini sağlarlar.



Blockchain Güvenliği Uzmanı (Blockchain Security Specialist):

- Bir kripto borsasının güvenliğini sağlarlar.

Yapay Zeka ve Makine Öğrenimi Güvenliği Uzmanı (AI and Machine Learning Security Specialist):

- Bir sağlık kuruluşu için hastaların sağlık verilerini korurken yapay zeka kullanırlar.



Uygulama Penetrasyon Testi Uzmanı (Application Penetration Testing Specialist):

- Bir e-ticaret uygulamasının güvenliğini test ederler.

Dijital Tehdit Analisti (Digital Threat Analyst):

- Bir siber casusluk saldırısını inceleyerek kimin arkasında olduğunu belirlerler.

SIBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR



Veri Analitiği ve Güvenlik Uzmanı (Data Analytics and Security Specialist):

- Veri madenciliği teknikleriyle güvenlik olaylarını önceden tahmin ederler.



Siber Hukuk Uzmanı (Cybersecurity Lawyer):

- Bir şirketin bir veri ihlali sonucu maruz kaldığı yasal sorunları ele alırlar.



Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
Zafiyet Analizi	<ul style="list-style-type: none"> - Güvenli Yapılandırma Denetimi Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi 	Kurumsal SOME personelinin bir siber olay gerçekleşmeden önce sistemlerindeki önemli zafiyetleri tespit etmesi ve karşı önlem uygulamasını koordine etmesi için gerekli yetenekleri kazanması
Kayıt Yönetimi	<ul style="list-style-type: none"> - Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi 	Kurumsal SOME personelinin sistemdeki kayıtları takip edebilmesi, sistemler ve tehditler ile ilgili farkındalık kazanabilmesi
Siber Olay Müdahale	<ul style="list-style-type: none"> - Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim sistemleri Adli Analizi Eğitimi - Bilgisayar Adli Analizi - Derinlemesine Windows Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku Eğitimi 	Bir siber olay gerçekleşmesi durumunda gerekli olacak olay yönetimi ve koordinasyonu yeteneklerinin kazanılması, dijital delillerin geçerliliğinin bozulmaması için alınacak tedbirlerin öğrenilmesi. Adli analiz esasen kolluk makamının görevi olmakla birlikte, kurumların “sistem izleme” ve “kayıt yönetimi” kapsamında giriş seviyesinde adli analiz bilgisine sahip olması gerekmesi.
Bilgi Güvenliği Yönetimi	<ul style="list-style-type: none"> - ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi 	Bilgi güvenliği/siber güvenlik sürecinin kavrulması ve Bilgi Güvenliği Yönetim Sistemi ile ilgili farkındalık oluşması.