Common types of cyberattacks and countermeasures – a brief explanation

www.eccentrix.ca

In today's world, our valuable properties include digital information – e-mail accounts, e-banking, company's documentation, personal data, etc. Everything has become digital. Because of that, cyberattacks have evolved to a point where serious efforts need to be taken to ensure our information remains secure. But, what is a cyber attack? It is an action started by threat actors, cyber criminals, hackers that aim at affecting the integrity, confidentiality, or availability at your data. So, the objective can be to disrupt, steal, or prevent the use of a legitimat system for its users.

Nowdays, attacks have become easy to lunch – everyone interested can find so many ways to initiate this, as the tools and the documentation have also become very accessible online.

Common cyber attacks are divided in types:

- Social engineering
- Applications and network services
- Wireless
- Cryptographic

Let's explore them by taking an understanding of the type and by enumerating ways it can harm a system, data, or a digital asset that is valuable to you or to your organization.

Social Engineering

Social enginnering exists as long as this world. There were always people who tried to get valuable information, once a trust between two individual is established. It can also be done by tricking someone inexperienced. Attacks in this category are the most successful, as the human is very often the weakest link in the chain of events.

Social engineering exists in multiple forms:

Phishing : A social enginnering technique in which threat actor or attacker tries to get user's information by sending him an email where attacker falsely claims to be from trustworthy source.

Spear phishing : A targeted phishing, where attacker is sending a very customized email to the victim.

Whaling : Similar to targeted phishing, but the target is often someone very know, for example a celebrity, an executive of a large company ("whale"), etc.

Vishing : A phishing attack that occurs by a telephone call or VoIP.

Smishing : A phishing attack that occurs over SMS messages.

Pharming : This term was created as combination of terms of phishing and farming. Threat actors use this attack to redirect users to false websites by altering the DNS system of a network or a computer.

Tailgaiting : A physical form of social engineering, where the attacker follows closely someone with authorization to enter a security area.

Impersonation : A threat actor impersonate someone else as a method to achive a goal.

Dumpster diving : Attackers often search for valuable company information in company's employees thrash cans, wher they could find ie printed emails, papers with account paswords, network diagrams, etc.

Shoulder surfing : A way to see information looking behind someone's shoulder.

Watering hole : Similar to spear phishing, but in this type of attack threat actor doesn't use mail, but attacks a site which user visits on regular basis, to compromise the company's security.

Countermeasures

Countermesures against social engineering are very different, compared to other forms of attacks. Since the user is at the center of every action, it is unlikely that this can be prevented solely by using technology, for example software or hardware.
Here, the focus is on building awareness. It is by nature for employees to help, or to be curious. However, there needs to be an ongoing effort to ensure people understand the implication of such attacks, and how easy the can get launched. The common effort that is provided by everyone in the organization will provide that strength.
Although training and awareness is at the heart of the solution, it is not the only one:

- Establish corporate policies, guidelines, and other form of documentation that is relevant to control the way information is accessed and shared;
- Use technical countermeasures, such as software that can detect potential harmful activities;
- Use physical controls, such as locked doors, mantraps, as well as other mechanisms to prevent easy acess to controlled areas of your facility.

Overall, the implement a company culture that emphasis on each and everyone's responsibility is key to help mitigate social engineering attacks.

Applications and network services

Today, we use applications and services resources that are availabile anytime and anywhere. Because of high interaction with them, attacks has grown rapidly in this domain. There are several types of application and network services attacks we should know about:

Spoofing : A technique of providing false identity on the network. There are two common spoofing attacks:

- **IP spoofing** : Attacker modifies his source IP address trying to hide his computer to gain access to unauthorized resources. It is commonly used for the purpose of establishing a connection in between two systems (man-in-the-middle) or to launch a denial of service.
- **MAC spoofing** : Threat actor masquerade his MAC (Media Access Control) address of his network device trying to gain access over company's network.

Countermeasure : It is important to ensure network scanning that helps detect network integrity threats, and provides a way to ensure the packets and frames are valid in transit.

Buffer overflow : A faulty design in an applications allows for a memory storage space allocation to be exceeded by the application's demand for storage in system memory. This causes privilege escalation, or a crash of the application.

Countermeasure : When designing an application, its security must be considered from the very beginning. Moreover, it is important to implement an update process once it gets released to use. Continuous improvements made to the software will decrease the risk of a buffer overflow.

The system on which the software runs must be secured as well.

Zero-day attack : Exploits unknown threats for which a fix or a patch is not existent yet.

Countermeasure : It is important to be active in community knowledge, and to be informed with appropriate intelligence on these types of threats. Although the software manufacturer will work on a patch, there are often temporary or workaround solutions that can also be implemented, decreasing the possibility of zero-day attack to take place.

Cross-site scripting (XSS) attack : An attacker tampers with a legitimate Web site, and injects malicious code. The malicious code is then executed over the browser when client visits the page. Unauthorized access activities, such as cookies stealing can occur.

Countermeasure : It is important to ensure the security of the website by implementing stress tests, fuzz testing, input sanitization... all these help in ensuring the safety of the code, and gives less of a potential for the XSS attack.

SQL injection : An attacker inserts malicious code into a relational database, which is then forwarded to the database server. The outcome can be elevated privileges, loss of data integrity, credentials stealing, etc.

Countermeasure : Similar to the XSS, it is important to ensure the security of the Web application. Although here, we might think the primary concern is with the database server. It is true, however it is the application that does not filter well the request, allowing the request to alter the data at the back end.

Session hijacking : An attack that happens when an threat actor hijacks a session between a Web server and a trusted client.

Countermeasure : This attack takes advantage of reusable tokens, or session identifiers. By ensuring one client has its own token, and not being reusable, the attack has less possibility to occur. It also all comes to the security of the application itself, as well as of the operating system.

Man-in-the middle attack : An attacker intercepts communication between two computers, with the objective to alter their conversation and steal valuable data. This is done at the protocol level, such as with ARP.

Countermeasure : Probes on the network can be installed that can monitor suspicious activity, such as intrusion detection and intrusion prevention systems. Conventional antivirus or basic firewall tools will not help in mitigating a man-in-the-middle attack.

Replay attack : The threat actor reuses packets that have been already captured in a conversation, in the attempt to bypass the login, typically.

Countermeasure : By ensuring each packet uses a timestamp, and by also protecting the packet integrity with the use of IPSec, for example, this activity would not be possible.

ARP/DNS poisoning : The ARP (Address Resolution Protocol) associates MAC to IP addresses. ARP poisoning involves tampering with the ARP table, where the MAC to IP relationships are held. The result can be a man-in-the-middle attack, a Denial of Service or a MAC flodding attack. In DNS poisoning, the attacker changes the IP record for a specific domain in the DNS cache and redirects traffic to illegitimate site.

Countermeasure : ARP being a very unsecure protocol (but that we need in order for the network to properly function), there are security tools that track the relationship of the entries in the ARP table, located on the systems themselves. It is a similar approach when it comes to DNS – the integrity of the cache on the server and the client is important.

DoS attack : The main purpose of a DoS (Denial-of service) attacks is to disrupt the services for the victim by making system unreponsive. Examples of DoS attacks include: smurf, fraggle, ping flood, SYN flood, teardrop. It can happen at the computer level as well, with the use of a buffer overflow.

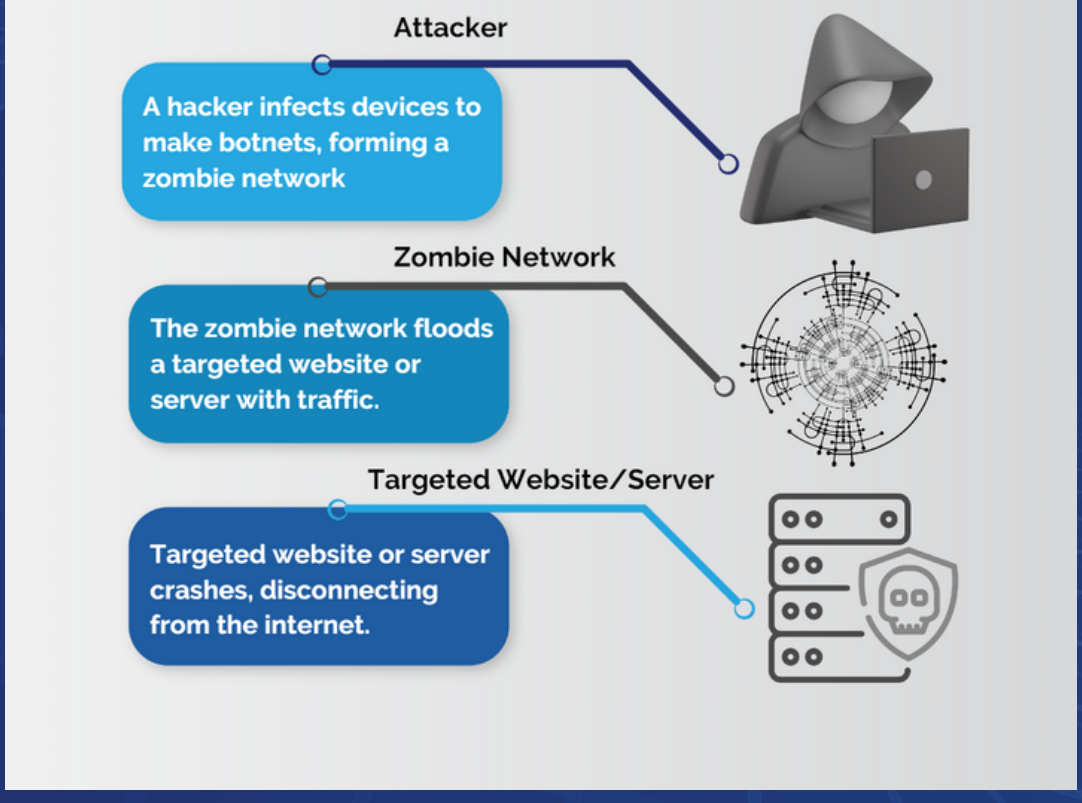
Countermeasure : Network and computer security devices can be of use, for example strong firewalls, intrusion detections systems, but also a strategy to minimise the exposure of a system to the outside world, limiting the possibility of finding a vulnerability for this type of attack.

DDoS attack – An attacker creates his „army“ of zombie computers by deploying a malware to them, and then uses these systems to attack the victim. A DDoS attack is more massive, where the objective is to incapacitate victim's server or website by flodding it with bogus requests, preventing legitimate requests to get processed.

Countermeasure : We can rely on Internet Service Providers that can block some IPs to get to us through a blacklist process, or acquire specialized hardware that will use its intelligence to block unwanted network traffic. Although, it is often a combination of multiple countermeasures that will be overall the best prevention technique.

DDOS ATTACKS EXPLAINED

DDoS attack occur when a hacker uses a zombie network to flood a website/server with traffic or requests until it crashes.



Wireless attacks

Wireless networks are prone to the same types of attacks that exist on wired networks – man-in-the-middle, denial-of-service, replay attacks. But, wireless networks have additional security issues that can prevent their use. In general, since the signal is spread over air, the contention of information that travels over the air is more difficult to achieve.

Jamming : This is an attack that targets the availability of the service. Someone will tune its devices to function at the same frequence as yours, which in turn will make your clients more difficult to access your antenna, and have a reliable link. This is essentially interference at its highest level.

Countermeasure: Ensure a physical inspection of the area where your corporate access points are located. You can also use tools to find unknown devices.

Rogue access point : An unauthorized device that is used to present itself as a legit access point, where clients can connect. This can be used for a man-in-the-middle attack. It would also bypass the corporate security policies, and expose the device to become less secure.

Countermeasure : Similar as in jamming, it is important to physically identify devices that are not managed by the company. It is also possible to use a device to map physical locations of such rogue devices, and send them a signal to stop.

Evil twin attack : Due to a higher strength in signal, a client can chose a rogue access point to connect - it becomes its privileged device to connect to, due to the stability of the signal. This device is likely to broadcast the same network name, making it more difficult for the end user to see the attack.

Countermeasure : A visual inspection of the area is required, or the use of a site survey to detect these types of attacks. Such attacks can be launched from a conventional system that transforms itself as an access point, thus that also has to be taken in consideration when investigating.

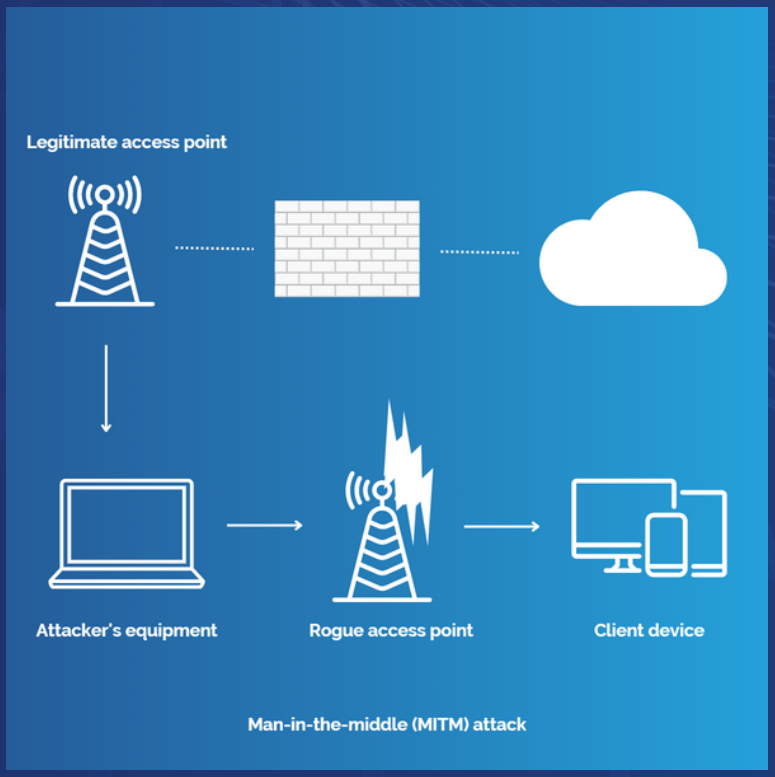
Dissociation or deauthentication : This is mainly targeting the availability of a stable connection. The client gets continuously disconnected and reconnectted to an access point, as a malicious user was able to reproduce the MAC address of the legitimate client, and that is using it to send fake disconnect requests.

Often, to ease the connection by the user, a technology named WPS (wireless protected setup) was introduced. However, major flaws have been discovered into this over time, thus relying on it would not be a solution.

Countermeasure : The implementation of an intrusion detection system that listens to specific requests in the air, produced by the malicious user can help in detecting the origin of a dissociation or deauthentication attack.

ARP replay attack : An ARP replay attack aims at establishing a man-in-the-middle, allowing the malicious user to listen to the communication between parties. It is also the base for many other wireless attacks, such as the discovery of a WEP key in correlation with initialization vectors (IVs).

Countermeasure : It is critical to implement surveillance systems, and to upgrade to higher and more secure authentication and encryption algorithms.



Cryptographic Attacks

With cryptographic attacks attackers tries to break contents like ciphertext or encrypted keys. One of the biggest problems of every corporate IT department are passwords. Users usually have easy-to-remember passwords and even if an IT department set complex passwords policies, user writing down their passwords and put an company's assets to a risk.

Dictionary attack : It is when an attacker use a „password dictionary" to gain acces to the system, which is most succesful on easy, simple passwords.

Countermeasure : Implement stronger password policies to ensure the password is not as simple, and is not likely to be found in a dictionary that can be acquired very easily online.

Brute force attack : It uses cryptoanalysis of algorithms to discover user's password. For short passwords it's much quicker than dictionary attack, but if the password is very complex it's need a lot of time and computing power. The brute force attack always succeeds. However, it all a matter of time – most complex passwords require years to break.

Countermeasure : It is important to work on a strategy to ensure the password can be remembered easily by the user, but because special characters, or password length have been optimised, it would take such a long time for the bruteforce to succeed.

Hybrid attack : It is essentially a dictionary attack, but letters are interchanged with numbers to try cracking the simple substitutions someone can make when using a password (S for 5, 0 for o, etc.).

Countermeasure : Ensure that the password policy protects from simple passwords, as well as their variants.

Birthday attack : It exploits the birtday paradox - the probability to find two inputs with the same hash value.

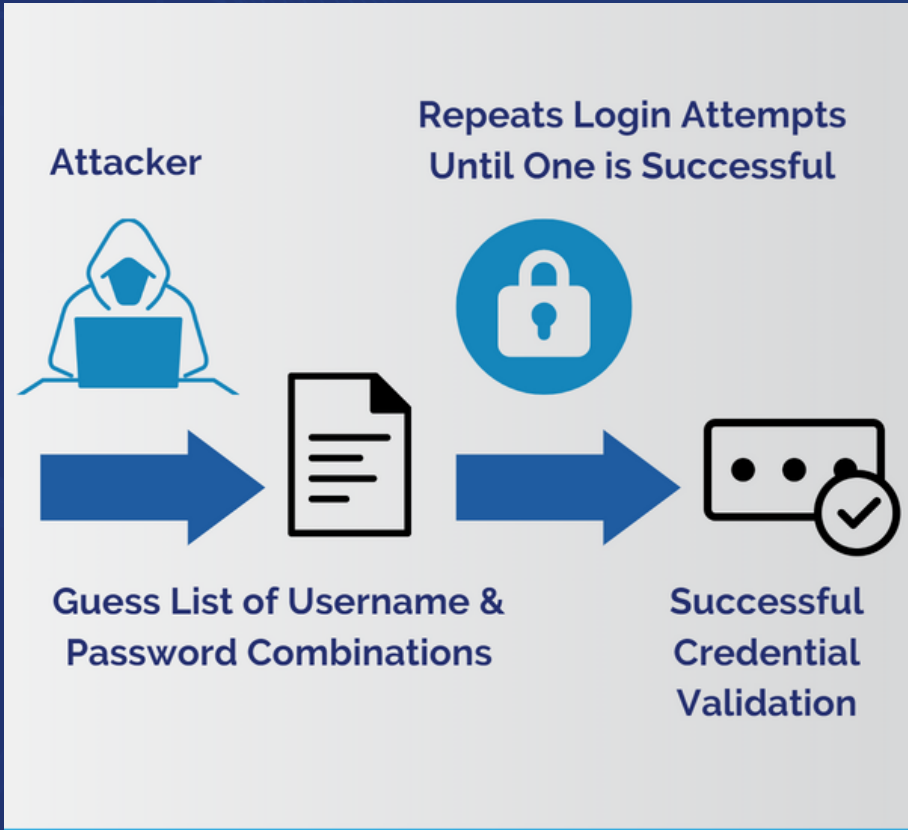
Countermeasure : Older hashing or cryptographic algorithms may be more at risk. Thus, improving and upgrading them can help in preventing such attack.

Rainbow table attack : A very large database of precomputed hash values for every characcter combination exists with two columns – the plaintext password, as well as its hash value. An attacker inputs the hash value (stolen), and expects the equivalent in its plaintext form will be shown.

Countermeasure : Salting works best against rainbow tables, as two plaintext values will not equal to the same hash.

Downgrade attacks : It forces the computer to abandon a safer protocol for an older, not-so-safe protocol (to maintain compatibility with older software) which allows to atttacker to exploit vulnerabilities in older protocol (for example, SSL versus TLS).

Contermeasure : The use of strong cipher suites, enabling MFA (multiple factor authentication), etc.



KEY STEPS OF A BRUTE FORCE ATTACK

Recommended cybersecurity trainings related to this writing:

CompTIA Security+ (CT8731)

CompTIA CySA+ (Cybersecurity Analyst) (CT8742)

Cybersecurity Bootcamp (CS8524)

Certified Ethical Hacker (CEHv12) (EC6154)

ECCENTRIX

CONTACT US


1-888-718-9732


www.eccentrix.ca


info@eccentrix.ca