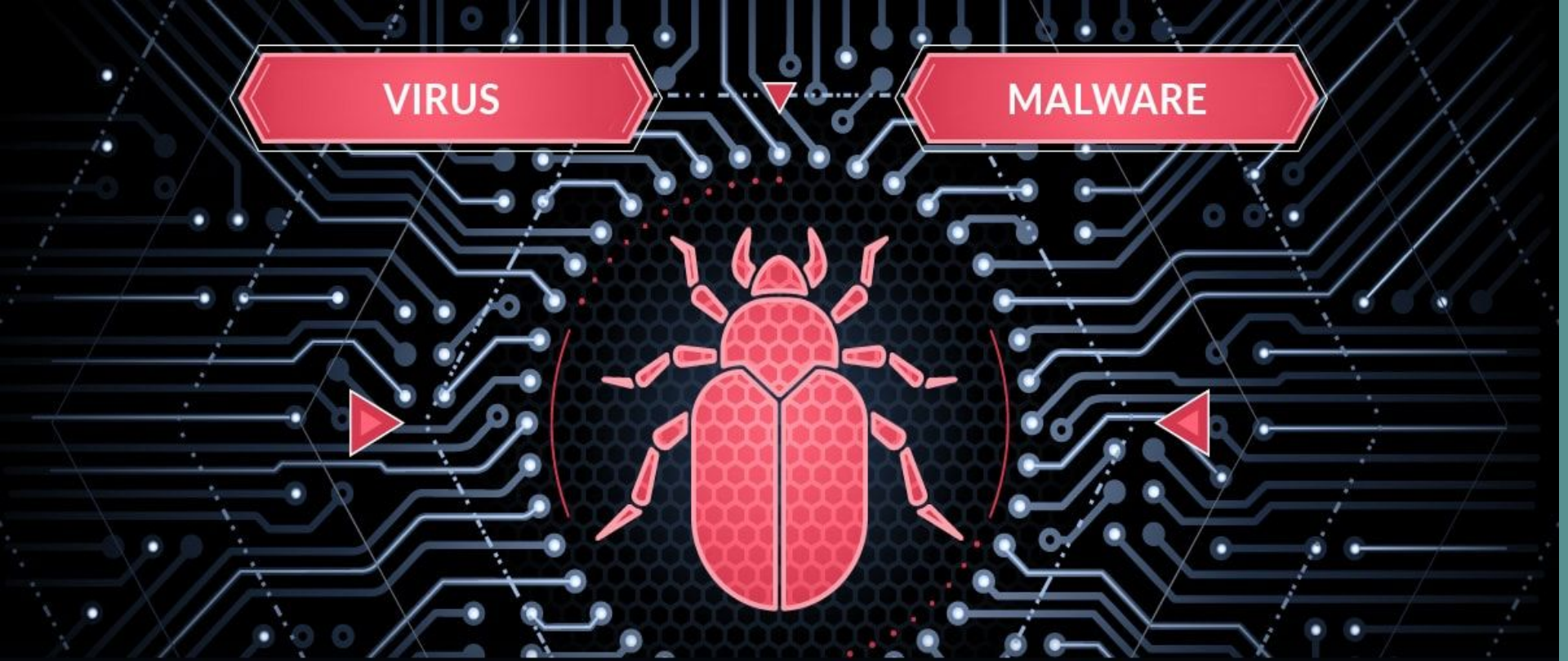


Assignment

Viruses and Malware

By: Rainier Jorge Jorda

What Is A Computer Security Risk

- A computer security risk is basically anything on your computer that may be damaged or stolen from your computer.

-There's is a variety of ways that can cause a computer security risk, this mostly includes malware, which is a general term used to describe malicious software.

-These program do no only include the commonly known computer virus, there are still several types of bad program that can create a security risk such as viruses, worms, ransomware, spyware, and Trojan horses.

-While the topics above cover most security risks, misconfigurations of computer products as well as unsafe computing habits also pose security risk as well.

Video: https://www.youtube.com/watch?v=W1Uadq_a3F4&ab_channel=FADILAHBINTIABDULRAUFBM

What is a Social Engineering

- Social Engineering is one of the most serious threat to a well-configured and well-secured network. There are at 10 types of social engineering: Pretexting, Phishing, Spear Phishing, Spam, Something for something, Baiting, Impersonation, Tailgating, Shoulder surfing, and Dumpster Diving.

-Cybercriminals use social engineering techniques in order to deceive and trick unsuspecting individuals into revealing their confidential information or volatile security to gain information.

-Social engineering prey on people's weaknesses and often rely on human nature and people's willingness to helpful

-Social engineering is often used in conjunction with other network attacks

Video: https://www.youtube.com/watch?v=Vo1urF6S4u0

What is Phishing

-Phishing is a type of social engineering.

-It is often used to steal the users data, including their login credentials and credit card numbers.

-This occurs when the attacker; whom is masquerading as a trusted entity, dupes the user/victim into opening any kinds of email, instant message, or text message. They will then trick them into clicking a malicious link, which will lead to them installation of malware, the freezing of the system or revealing sensitive information about the user/victim.

-These attack usually have very devastating results, especially towards the victim. Moreover, phishing is used to gain a foothold over many corporate or government network as part of a larger attack.

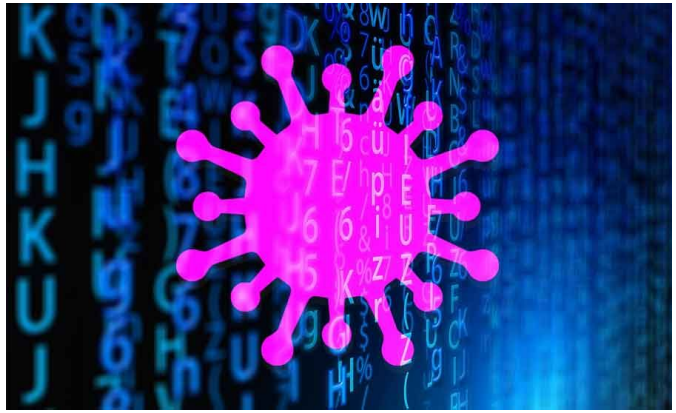
Video: https://www.youtube.com/watch?v=Y7zNlEMDmI4&ab_channel=IDGTECHtalk

What is a Virus

-A computer virus is a malicious piece of code which is designed to spread from device to device.

-It is basically a subset of malware that are self-copying threats, designed to damage a device or steal their data. It is basically very similar to a biological virus, the ones that make you sick.

-A computer virus is very similar to a regular virus, designed to replicate itself relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stops it from working altogether.



Video: https://www.youtube.com/watch?v=qNodotqsUqg

An Example Of A Virus

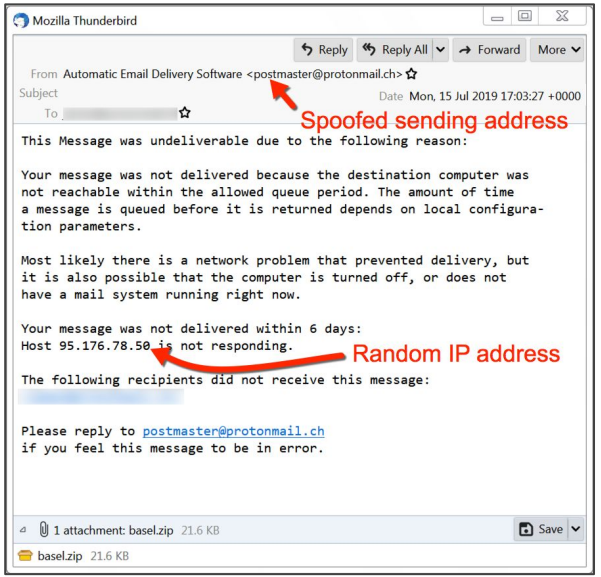
-An example of a computer virus is one of the most dangerous virus in the world which is the Mydoom virus. This certain virus had caused around $38 billion in damage in 2004. Adjusting for inflation, it would've caused $52.2 billion in damages if it was done now. Another name of this virus is Novag.

-It was spread through mass emailing, at one point during its execution, it was responsible for 25% of all emails sent throughout the world.

-The way Mydoom worked is by scraping email addresses from infected machines and sent copies of itself to other machines. It also created a botnet with infected machines in order to DDOS(Denial of Service) targeted servers.

-The Mydoom virus is still here even today, and it still generates at least 1% of all phishing emails.

Video: https://www.youtube.com/watch?v=7kPNVKqSGz0&ab_channel=Disrupt



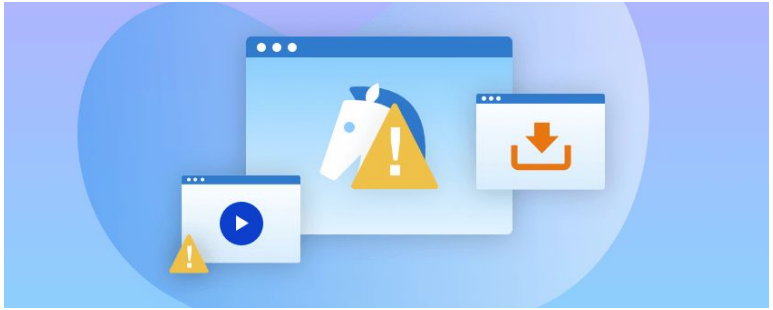
What is A Trojan Horse

-A trojan horse is a type of malware that downloads itself on the computer as a legitimate program.

-The delivery method usually sees the attacker use social engineering in order to hide the malicious code within the legitimate software in order to try and gain the users' system access with their software.

-A simple way to answer "What is a Trojan horse" is that it's a malware that typically gets hidden attached to a file in a email or a free-to download file. Once downloaded, the malicious code will then execute the task assigned to it, such as gaining backdoor access to corporate system, spy on users' online activity, or steal sensitive data.

- An indication of a Trojan horse being on your computer system is when unusual activities, such as computer settings are changed.



Video: https://www.youtube.com/watch?v=pzOM8sc2RPU&ab_channel=EyeonTech

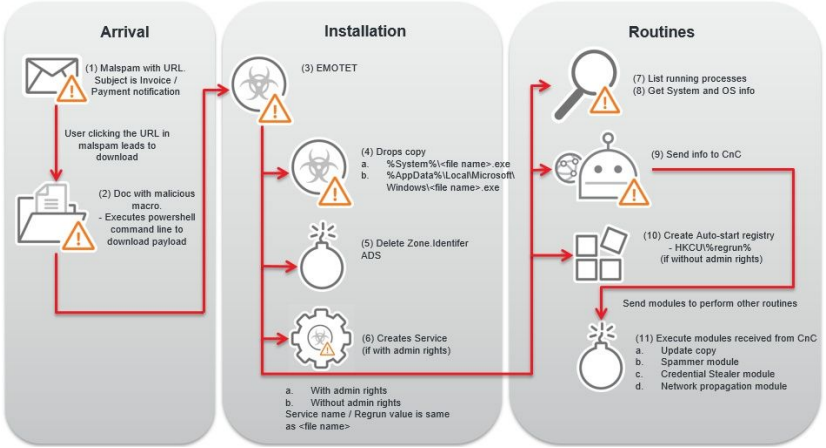
An Example of a Trojan Horse

-An example of a Trojan Horse is Emotet. It is a computer malware that was originally developed in a form of banking Trojan.

-The goal of Emotet was to access foreign devices and spy on sensitive private data. Emotet had been known to be able to hide and deceive from basic antivirus programs.

-Emotet spreads like a computer worm and attempts to infiltrate other computers in the network. Emotet spreads mainly through spam emails. The respective emails contains malicious link or an infected document. If you download or open the link, further malware will be automatically downloaded on your computer. These emails are meant to look authentic and many had fallen for these tricks.

-Emotet had target many private companies, organizations, and authorities in 2018, an example was a German hospital, Fürstenfeldbruck having to shut off and log out of 450 computer in order to at least control the virus. In September 2019, the Berlin Court of appeal was affected by this virus. In December 2019, the University of Giessen had been affected. These are just one of many examples that the Emotet virus had been able to infect and spread through.



Video: https://www.youtube.com/watch?v=CkwKTBifXJg&ab_channel=MetaCompliance

What is Rootkit

-A rootkit is a clandestine computer program that is designed to provide continue privileged access to a computer while actively hiding its presences.

-The term rootkit is a connection of two words “root” and “kit”. Originally, rootkit was a collection of tools which enable administrator-level access to the computer or network. The root refers to the admin accounts such as Unix and Linux system. While the kit refers to the software components that implement the tools.

-Today rootkits however, are now generally associated with malware. Trojans, worms, viruses, now use it to conceal their existence and actions from user and other system processes.

Video: https://www.youtube.com/watch?v=0LvF0KtBWxY&ab_channel=Techquickie

An example of a Rootkit

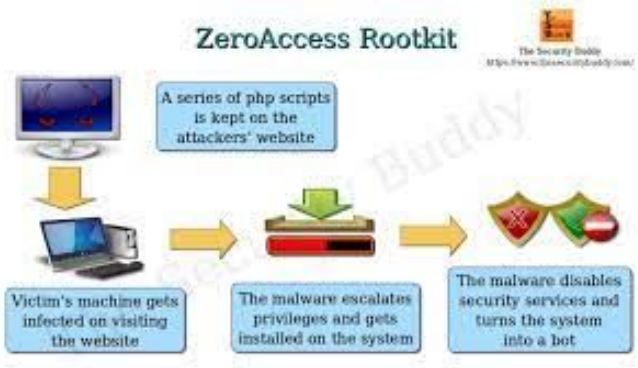
-An example of a rootkit is the ZeroAccess Rootkit.

-This rootkit is a malware that infects a computer silently, turns the system into a bot and exploits the computer for malicious purposes.

-It can corrupt many things such as TV, printers, mobiles, tablets, etc and consider to be a high-security risk.

-The way this rootkit infects computers is by creating a server/website that the attacker put malicious code on. It then uses social engineering to send a link to a victim and deceive them into clicking that link. Once upon website, it would instantly download the malware and exploit many security vulnerabilities. It will then gain administrator access to the ramp up the installation of scripts to execute.

-This rootkit has been found in 2011, and since then, it infected and still infect millions of system today.



Video: https://www.youtube.com/watch?v=2po_dqZzmTE&ab_channel=siliciumsec

What is Ransomware

-Ransomware is a malware that employs encryption in order to hold a victims information hostage. A user or organization's most important data might be encrypted so that they cannot access their files, database, or applications. A ransom is then sent to the victim if they want to obtain access to their files.

-Ransomware is designed to spread across a network and target database file servers, which will thus paralyze the organization.

-Ransomware uses many social engineering techniques in order for the attacker to gain access to the victim's computer. After gaining access the attacker will execute malicious binary in order to search valuable files about the victim. They will then encrypt these files, before sending a ransom to the victim. Usually these victims only have 24-48 hours to send the ransom or their files will be lost forever.

Video: https://www.youtube.com/watch?v=Vkjekr6jacg&ab_channel=Kaspersky

An Example of Ransomware

-A famous example of ransomware is one ransomware attack called Sodinokibi or REvil.

-REvil, first appeared in 2019. It took advantage of its advance evasion capacity and large number of measures that it takes in order to avoid detection. It had a large amount of targets with the main focus being Europe, the USA, and India.

-It multiple infection include exploiting known security vulnerabilities and also the use of email phishing campaigns.

-In April 2021, the group that created REvil claimed that the hacked a computer network called Quanta, a Taiwan-based company that manufactures MacBooks. They demanded $50 million for the encryption key however Quaata didn't give in. They were true to the claim and released some information to the public however just recently in November 2021, two of the cyber criminals were hunted down and arrested.

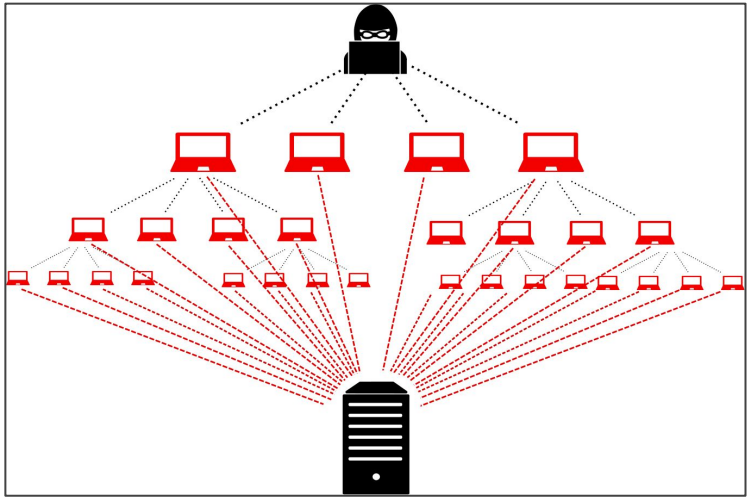
Video: https://www.youtube.com/watch?v=14NwrgdIEXY&ab_channel=SiamAlam

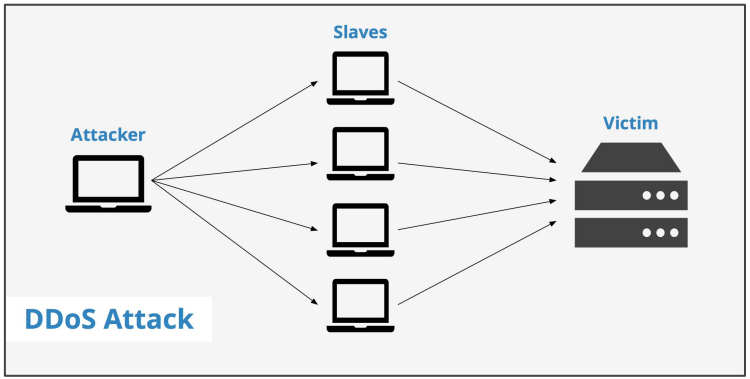
What is a DDOS attack

-A DDOS or distributed denial of service are a subclass of denial of service or DOS attacks. A DDOS attack usually is connected to multiple online devices, mostly known as a botnet which are typically used to overwhelm a target website with fake traffic.

-Unlike other cyberattacks, DDOS is not used breach security but instead to make it unavailable for legitimate user and also as a smoke screen for other malicious activities while also being able to take down security appliance allowing for a breach in the security perimeter.

-DDOS attacks can come in short burst or repeated attacks, however the impact on a website or business can last for days, weeks or even months as the organization tries to fix it. This makes DDOS one of the most destructive force to online organizations as it can lead to loss of revenue, erode customer trust, force businesses to spend fortunes for compensations and cause long-term reputation damage.





Video:https://www.youtube.com/watch?v=ilhGh9CEIwM&ab_channel=PowerCertAnimatedVideos

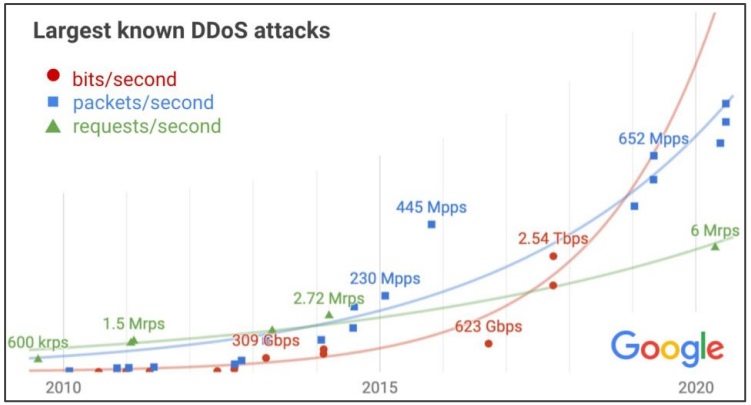
An Example of DDOS attack

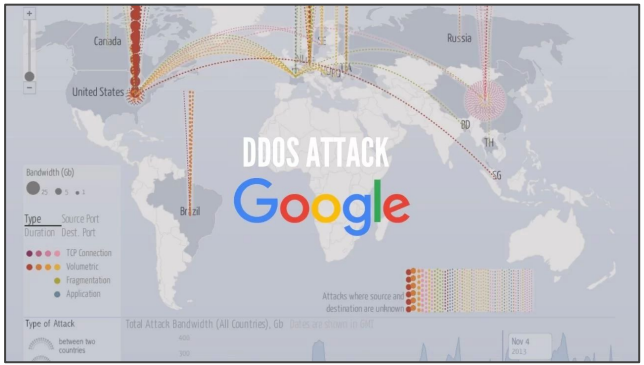
-An example of a massive DDOS attack was one done towards Google called The Google Attack.

-On October, 16 2020, Google Threat Analysis Group (TAG) update the concerning how the threat and the threat actors are changing their tatic due to the 2020 US elections. At the very end of the report, they include something very jaw dropping.

-It record, “in 2020, our Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453, and 9394), which remains the largest bandwidth attack of which we are aware.”

-Coming from three Chinese ISP, the attack on thousands of Google's IP lasted for at least 6 months and peaked at a mouth-dropping 2.5Tbps. Damian Menscher, a Security Reliability Engineer at Google stated, “The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us. This demonstrates the volumes a well-resourced attacker can achieve: This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet a year earlier.”





Video: Sadly, there is no videos as all of this was only recorded through articles.

Work Cited

https://www.imperva.com/learn/application-security/phishing-attack-scam/

https://www.webroot.com/ca/en/resources/tips-articles/computer-security-threats-computer-viruses#:~:text=A%20computer%20virus%20is%20a,kind%20that%20makes%20you%20sick.

https://insider.ssi-net.com/insights/whats-the-most-dangerous-computer-virus-in-the-world

https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

https://www.kaspersky.com/resource-center/threats/emotet

https://www.veracode.com/security/rootkit

https://softwarelab.org/what-is-a-rootkit/

https://nakedsecurity.sophos.com/zeroaccess2/

https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware.html

https://antivirus.com/2021/12/24/famous-ransomware-attacks/

https://www.imperva.com/learn/ddos/denial-of-service/#:~:text=Distributed%20denial%20of%20service%20(DDoS)%20attacks%20are%20a%20subclass%20of,target%20website%20with%20fake%20traffic.

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/