The New Face of Organized Crime and its Security

Ritu Sharma
EXTC Department
ACE (Malad)

Kunal Shriwas
EXTC Department
ACE (Malad)

Shilpa Jaiswal
EXTC Department
ACE (Malad)

Jyoti Gurav
EXTC
ACE (Malad)

Abstract : **The core functionality of cyber security involves self-protective information and systems from major cyber threats. These cyber threats take many forms (e.g., application attacks, malware, ransomware, phishing, exploit kits). Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks using these tactics – at lower and lower costs. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most disorderly form, cyber threats often take aim at secret, political, military or infrastructural assets of a nation, or its people.. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cyber security and physical security.**

Keyword – Protection , attacks, malware, attacks, vulnerable

I. INTRODUCTION

As we all are aware of the fact that the world is pacing fast towards digitalization. With the digital world the security has also came in to the matter here. Cyber security has turned out to be most important field in present scenario. Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organizations and individuals from the illegal exploitation of systems, networks and technologies.

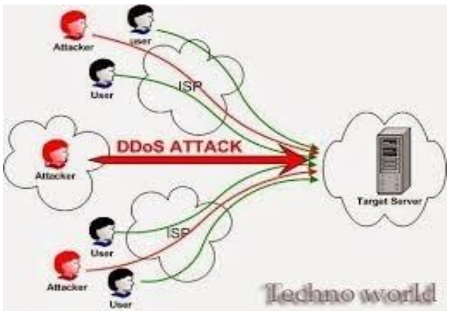

Fig1 .DDos Attack

II. TYPES OF ATTACKS

FIG12 . TYPES OF ATTACKS

2.1 Malware

What is it? Malware is an all-encompassing term for a diversity of cyber threats including Trojans, viruses and worms. Malware is simply defined as code with malicious intent that characteristically steals data or destroys something on the computer.

How does it work? Malware is most often introduced to a system through email attachments, software downloads or operating system vulnerabilities.

How can I prevent it? The best way to prevent malware is to avoid clicking on links or downloading attachments from unidentified senders. This is sometimes done by deploying robust and updated firewalls, which prevent the transfer of large data files over the network in a hope to weed out attachments that may contain malware.

It's also important to make sure your computer's operating system (e.g. Windows, Mac OS X, and Linux) uses the most up-to-date security updates. Software programmers update programs frequently to address any holes or weak points. It's important to install these updates as well to decrease your own system's weakness.

2.2 Phishing

What is it? Often posing as a request for data from a trusted third party, phishing attacks are sent via email and ask users to click on a link and enter their personal data. Phishing emails have gotten much more sophisticated in recent years, making it difficult for some people to discern a genuine request for information from a false one. Phishing emails often fall into the same category as spam, but are more harmful than just a simple ad.

How does it work? Phishing emails include a link that directs the user to a dummy site that will steal a user's information. In some cases, all a user has to do is click on the link.

How can I prevent it? Verify any requests from institutions that arrive via email over the phone. If the email itself has a phone number, don't call that number, but rather one you find independently online or within documentation you've received from that company.

Most companies are adamant that they will not ask for personal information via email. At the same time, most companies strongly recommend that users not make sensitive information available. While it might seem like a pain to make a phone call to find out if something is legitimate, the hassle of having your Social Security number or EIN stolen is worse.

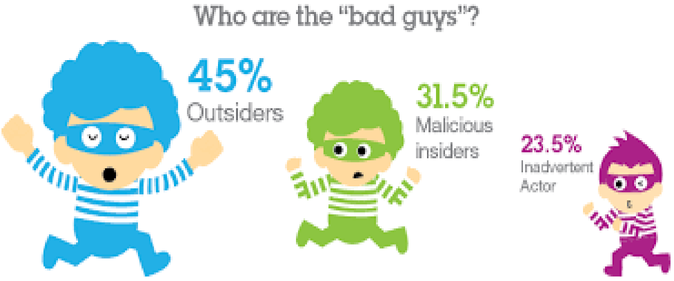

Fig 3.Password Attacks

What is it? A password attack is exactly what it sounds like: a third party trying to gain access to your systems by cracking a user's password.

How does it work? This type of attack does not usually require any type of malicious code or software to run on the system. There is software that attackers use to try and crack your password, but this software is typically run on their own system. Programs use many methods to access accounts, including brute force attacks made to guess passwords, as well as comparing various word combinations against a dictionary file.

How can I prevent it? Strong passwords are really the only way to safeguard against password attacks. This means using a combination of upper and lower case letters, symbols and numbers and having at least eight characters or more. As a point of reference, an attacker using a brute force password cracking program, can typically unlock a password with all lower case letters in a matter of minutes. It's also recommended not to use words found in the dictionary, no matter how long they are; it just makes the password attacker's job easier.

It's also good practice to change your passwords at regular intervals. If a hacker is able to obtain an older password, then it won't work because it's been replaced!

2.3 Denial-of-Service (DoS) Attacks

What is it? A DoS attack focuses on disrupting the service to a network. Attackers send high volumes of data or traffic through the network (i.e. making lots of connection requests), until the network becomes overloaded and can no longer function.

How does it work? There are a few different ways attackers can achieve DoS attacks, but the most common is the distributed-denial-of-service (DDoS) attack. This involves the attacker using multiple computers to send the traffic or data that will overload the system. In many instances, a person may not even realize that his or her computer has been hijack and is contributing to the DDoS attack.

Disrupting service can have serious consequences relating to security and online access. Many instances of large scale DoS attacks have been implemented as a sign of protest toward governments or individuals and have led to severe punishment, including jail time.

How can I prevent it? Unless your company is huge, it's rare that you would be targeted by an outside group or attacker for a DoS attack. Your site or network could still fall victim to one, however, if another organization on your network is targeted.

The best way to avoid an additional breach is to keep your system as secure as possible with regular software updates, online security monitoring and monitoring your data flow to identify any unusual or threatening spikes in traffic before they become a problem. DoS attacks can also be perpetrate by simply cutting a cable or dislodging a plug that connects your website's server to the internet, so due diligence in physically monitoring your connections is recommended as well.2.

2.3 Man in the Middle (MITM)

What is it? By impersonating the endpoints in an online information exchange (i.e. the connection from your smartphone to a website), the MITM can obtain information from the end user and the entity he or she is communicating with.

For example, if you are banking online, the man in the middle would converse with you by impersonating your bank, and communicate with the bank by impersonate you. The man in the middle would then receive all of the information transferred between both parties, which could include sensitive data, such as bank accounts and personal information.

How does it work? Normally, a MITM gains access through a non-encrypted wireless access point (i.e. one that doesn't use WAP, WPA, WPA2 or other security measures). They would then have access to all of the information being transferred between both parties.

How can I prevent it? The best way to prevent them is to only use encrypted wireless access points that use WPA security or greater. If you need to connect to a website, make sure it uses an HTTPS connection or, for better security, consider investing in a virtual private network (VPN). HTTPS uses certificates that verify the identity of the servers you're connecting to using a third-party company such as VeriSign, while VPNs allow you to connect to websites through virtual private networks.

2.4 Drive-By Downloads

What is it? Through malware on a legitimate website, a program is downloaded to a user's system just by visiting the site. It doesn't require any type of action by the user to download.

How does it work? normally, a small snippet of code is downloaded to the user's system and that code then reaches out to another computer to get the rest and download the program. It often exploits vulnerabilities in the user's operating system or in different programs, such as Java and Adobe.

How can I prevent it? The best way is to be sure all of your operating systems and software programs are up to date. This lowers your risk of vulnerability. Additionally, try to minimize the number of browser add-ons you use as these can be easily compromised. For example, if your computers don't need Flash or the Java plug-in, consider uninstalling them.

2.7 Malvertising

What is it? A way to compromise your computer with malicious code that is downloaded to your system when you click on an affected ad.

How does it work? Cyber attackers upload infected display ads to different sites using an ad network. These ads are then distributed to sites that match certain keywords and search criteria. Once a user clicks on one of these ads, some type of malware will be downloaded. Any website or web publisher can be subjected to malvertising, and many don't even know they've been compromised.

How can I prevent it? The best way to prevent falling victim to malvertising is to use common sense. Any ad that promises riches, free computers or cruises to the Bahamas is probably too good to be true, and therefore could be hiding malware. As always, up-to-date software and operating systems are your best first line of defense.

2.8 Rogue Software

What is it? Malware that masquerades as legitimate and necessary security software that will keep your system safe.

How does it work? Rogue security software designers make pop-up windows and alerts that look legitimate. These alerts advise the user to download security software, agree to terms or update their current system in an effort to stay protected. By clicking "yes" to any of these scenarios, the rogue software is downloaded to the user's computer.

How can I prevent it? The best protection is a good offense—in this case, an updated firewall. Make sure you have a working one in your office that protects you and your employees from these types of attacks. It is also a good idea to install a trusted anti-virus or anti-spyware software program that can detect threats like rogue software.

As with most types of crime, care is one of the keys to prevention. As cyber criminals become more sophisticated and more transactions migrate online, the number of threats to people and businesses will continue to grow. Prepare yourself and your business by taking the time to secure your systems and make cyber security a priority.

Force users to use https in firefox and Chrome both have this feature. Lots of sites have log-ons on http where credentials are in plaintext on your network, or even the internet routing path in general that expose log-ons. Firefox now default to smacking users that try to use auto-fill on http sites. Educate users about this. And if, heaven forbid, your site has a log-on over http, you need to turn in your security stirrups while your horse still rides. There's too much change. Insurance companies love receipts and having things in order, as do police departments—which the insurance companies must have a report from. Yes, there's something to the tactic of taking a video of all your stuff, as well as the serial numbers, on a periodic basis and uploading it to two places. Get rid of them. Allow users to get scary error messages when something tries to route them to somewhere expired so that they don't swallow the next thing that inevitably arrives: the fake certificate "open-wide" page. Face it, you need a key management system and rigorous enforcement once the trial has been completed. Key managers are worth their weight in stolen assets. In my personal opinion, Microsoft should be banned for ignoring a hosts file, the file that contains hosts and IP addresses. It's done because this can disrupt Active Directory under some circumstances, so they ignore the file.

The problem is there are many well-thought cogent lists of fake and misspelled sites in hosts files that can prevent users from shooting themselves in the spelling foot. This is such an unholy act that Microsoft should be spanked.

MacOS and Linux both respect this file dutifully, which is why it needs to be periodically examined by scripts to see if it's been corrupted by unscrupulous users or, more importantly, malware. Always write your organization's hosts file once in a while just to remove potential corruptions. Running scans of your network for new and unknown MAC addresses means you've perhaps discovered new purchases or worse, newly implanted machinery on your network. After reading of the new DISHWASHER CVE (look it up—Meile USA), you have no idea until you've done the work of slogging through your ACLs and MAC address tables to look for the new backdoors into your network.If you're on a security team, schedule regular meetings with other departments within IT. Let people voice their concerns. Remind people of organizational security needs. Allow yourselves time to physically visit important assets. Several eyes on assets might reveal something new or strange to investigate.There are lots of great syslog amalgamation services that read Microsoft and standard syslog files. Filter and read them. Act upon what you see. The logs are there for a reason. Yes, Facebook can be more interesting, but read the damn logs. Security at other organizations ranges from tight to non-existent—and everythingin between. When a new hire comes on board, presume they know nothing at all about your organizational security mandates. Best practices for many organizations include training on Sarbanes-Oxley, HIPPA and other industry tenets. But security in every business segment is different. At minimum, make it a video with a quiz. Then you've established a baseline.

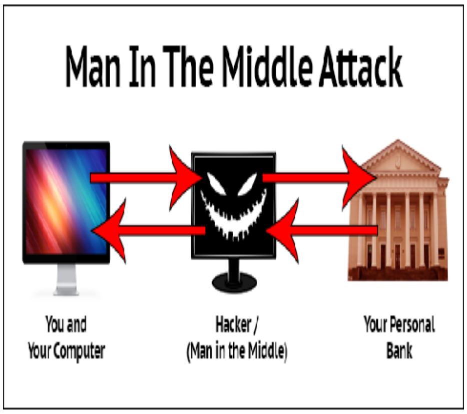

Fig 3 MAN IN THE MIDDLE ATTACK

CONCLUSION

cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, eco nomics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. In practice, although technical measures are an important element, cybersecurity is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Furthermore, what is known about cybersecurity is often compartmented along disciplinary lines, reducing the insights available from cross-fertilization.

This primer seeks to illuminate some of these connections. Most of all, it attempts to leave the reader with two central ideas. The cybersecurity problem will never be solved once and for all. Solutions to the problem, limited in scope and longevity though they may be, are at least as much nontechnical as technical in nature.

REFERENCES

Journal Papers:

[1] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation, 18(2),* 1998, 112-116. (8)

[2] *A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES G.NIKHITA REDDY , G.J.UGANDER REDDY*

[3] *Cybercrime: A threat to Network Security Ammar Yassir and Smitha Nayak, 84 IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012*

[4] https://www.nap.edu/read/18446/chapter/5

[5] *W.J. Book, Modelling design and control of flexible manipulator arms: A tutorial review, Proc. 29th IEEE Conf. on Decision and Control, San Francisco, CA, 1990, 500-506*