**Network Attacks – Types and Measures to stop them**

DeepaNatarajan

Department of Management Information Systems, Bellevue University

CIS 515: IT Infrastructure

Professor James Krohn

**Network Attacks – Types and Measures to stop them**

Network is ever evolving and has made the world faster and more resourceful. Every organization have a design to implement hardware/software technologies, applications in house or in cloud data center and in many geographical locations. It has flagged globalization and economic growth in many parts of the world with no need for the people to drift in search of prospects and resources. Eventually it benefits business and the customers in more efficient and effective ways. Networks has given equal access for both moral and malevolent purposes. Organizations have to understand the types of attacks in order to implement a network design for the business to happen in a secured way; here comes the security thinking in network infrastructure.

**Types of Attacks**

Data breaches and network attacks are in the raise. For business to function effectively, understanding and building a strong security network defense system is vital. There are five major types of attacks on networks (Panko & Panko,2018). They are,

* Malware – Viruses, worms, Trojan horse
* Payload
* Hacking
* Denial of Service-Bot, Botnet, Botmaster
* Advanced Persistence Threats

**Differences between the attacks**

`**Malware:** It is an evil software under which there are many types like-Viruses, worms and Trojan horses attack the users. Subtle differences exist between these software and they are

* Viruses are small codes which comes as an attachment and can attack the user by downloading the attachments. They can propagate to other computers as attachment.
* Worms are self-propagating programs. They are difficult to be find way into the host but once the vulnerability is exposed, it is quick and easy for them to spread to many computers without human intervention.
* Trojan horse disguise as a legitimate program and once it finds its way it starts attacking the computers.

**Payloads:**

The malwares after getting into the host, execute the piece of code called Payloads. They can do extensive damage like-erase and encrypt the hard drive, turn the computer into a spam or pornography server, act as spyware to collect the login credentials, credit card number theft and identity theft.

**Hacking:**

Human’s accessing the resources unauthorized or in excess of authorization is termed hacking. This is considered to be more dangerous than the malwares because humans can break-in using variety of methods than a malware.

**Denial-of-Service Attack:**

The goal of this attack is to make the entire network unavailable for the legitimate user. The attacker called botmaster installs a malware called bot on many computers which then called botnet. Bot is given an attack command to flood the victim with packets. The adversary sends orders to the command-and-control server, which then sends the attack commands to the bots.

**Advanced Persistence Threats:**

The adversaries have multiple objectives that they pursue to attack for longer period. The attackers try to gain access to the network infrastructure, using malware like trojan horse and then used advanced penetration and exploitation methods. They are expensive to mount.

**How should these types of attacks be considered when implementing a network design solution?**

The article “5 Ways to Stop Network Security Threats” (2020), discusses that the most effective way to protect the network is by implementing the protective measures. Which includes

* Boost physical security
* Educating employees about the security measures
* Reinforcing the security access control
* Use network protection method
* Install network monitoring software

**Boost physical security**

If the enterprise has a server room, it needs to be secured using a reliable digital lock or hiring a security guard, to discourage the intruders from accessing them.

**Educating employees about the security measures**

Training all the employees with the various types of security attacks, ways to identify them and updating the contact information.

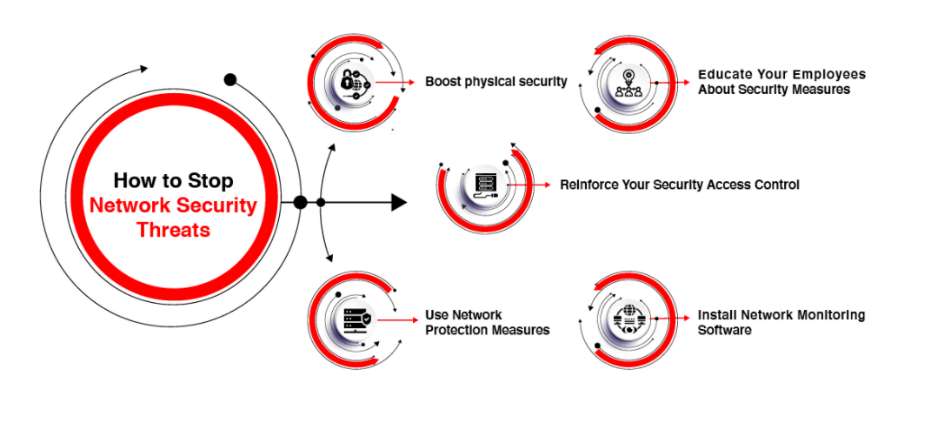
**Reinforcing the security access control:**

Network breaches occurs when an unauthorized access is gained using the passwords. So, focusing on multilevel authentication, changing passwords frequently are some of the few measures that need to be followed.

**Use network protection method**

It includesupdating the software’s regularly, installing firewalls, track potential packet floods, use network segmentation and installing virtual private network.

*Figure 1:*

*How to stop Network Security Threats*

*Note*: The picture suggests five different ways to protect the network in an organization against the security threats. Adapted from *How to Stop Network Security Threats* by EC-Council Blogs. Retrieved, April 23,2021. ( <https://blog.eccouncil.org/5-ways-to-stop-network-security-threats/>)

**Install network monitoring software**

These software’s provide early warnings by monitoring the entire IT infrastructure by establishing contact with all devices and systems. It monitors the entire security system, measures bandwidth bottlenecks and inspects environmental parameters.

**SolarWinds Attack-A case Study**

Advanced attackers use the identity and access management tools as a target. According to Firstbrook (2021), in the article “Top 10 Lessons Learned from the SolarWinds Attack, the attackers used the Golden SAML technique and modified trusted domains, abused privileged roles, stuffed credentials and hijacked Azure Active Directory (AD).

Another major target were the Linux machines used by the developers and the codes were compromised using the spear phishing technique. The Linux Machines were excluded from the End point detection and response tool (EDR). Moreover, the administrators disabled some security products and were using the outdated tools, regular auditing and updating the security configuration would have provided additional check.

**Key take away from the case study:**

Security analytics and extended detection and response (XDR) tools need to be incorporated in the directory and authentication data. For most of the operations and security solutions the corporations are accessing API cloud applications like Microsoft Azure and sales force. (Firstbrook,2021). Focus need to be paid on storing the digital keys, certificates that act as a machine identity because losing them would be a disaster. It was very clear that the privileged accounts were the target, so it is good to use privileged access management (PAM) tools, which secures the password, limits the access to authorized users, and monitors the use of privileged accounts. Developers were the key targets and they should be included in the endpoint protection policies.

**Conclusion**

The attackers are using the advanced tools to break the defense mechanism, more data for the organizations are in the cloud. Being on high alert, foreseeing the problems, and consistent checks with innovative solutions can help control the security breaches. As security expert Bruce Schneier has said, “Security is process, not a product”, the security and risk management teams should understand the implications to improve their defenses.

**References**

EC Council Blog(n.d.). *5 Ways to Stop Network Security Threats.*Retrived April 22,2021, from <https://blog.eccouncil.org/5-ways-to-stop-network-security-threats/>

Firstbrook, Peter (February 17, 2021). *Top 10 Lessons Learned from SolarWinds Attack.* Gartner.

Publication ID G00718590.

Panko, R. and Panko, L. (11th Ed.). (2018). *Business Data Networks and Security.* Pearson Publications.

CompTIA Network+ - Network Security (Threats and Attacks). Retrieved April 20, 2021 from <https://www.youtube.com/watch?v=tk-J2b5Rb34>

Webinar: Protecting Your Business: Network and Data Security Solutions for Entrepreneurs Retrieved April 20,2021 from youtube.com/watch?v=trgtLf5zrog

Common Network Attacks and Countermeasures (CISSP Free by Skillset.com). Retrieved April 20, 2021 from <https://www.youtube.com/watch?v=DLiP7y51OAQ>