**An analysis of Network security, Attacks, and Pegasus spyware**

**Deep Patel**

**Cybersecurity (B.S)**

**CYSE 280**

**Professor: Dr. Rashid Khan**

**Old Dominion University**

Table of Contents

[Abstract 3](#_Toc100216406)

[An analysis of network security, attacks, and Pegasus spyware 4](#_Toc100216407)

[Introduction 4](#_Toc100216408)

[Network Security 4](#_Toc100216409)

[Pegasus Spyware 4](#_Toc100216410)

[Figures 8](#_Toc100216411)

[References 9](#_Toc100216412)

**Abstract**

Millions of devices are connected a systems or networks. Networks around the world are constantly getting attacked. Cyber criminals and attackers are always discovering new ways to gain access to network or to disrupt network. Intentions of attacking are different but, in the end, they cause significant loss to businesses, consumers, governments, and the public. This paper discusses and analyzes network security, network attacks, vulnerabilities, ransomware, and Pegasus spyware. Analysis of how these attacks cause damage and disrupt critical functions. Cybercriminals attack the most vulnerable in order to gain network access.

Keywords: Network attacks; Pegasus Spyware; Ransomware; BGP; Vulnerabilities

An analysis of network security, attacks, and Pegasus spyware

# Introduction

Companies and organizations all around the world depend on their networks. Network downtimes cause serious problems and damages. There are various malicious that target the vulnerabilities in a network. Attackers aim to gain network access and alter, delete, or cause the shutdown of the network. Vulnerability can be as simple as having a weak password or using default fault for devices. Pegasus spyware is the most powerful spyware developed. Once a device is infected it can turn into a surveillance device and can be accessed anytime.

## Network Security

Network security is an integral part of cyber security and information technology. Networks and systems contain valuable data. Organizations use hardening process to take actions to prevent network attacks. Users must utilize security features provided by their operating system and use antivirus software. Users must use caution and beware of phishing attacks and malicious links. Border Gateway Protocol is susceptible to many different attacks, including Denial of service, sniffing, and routing traffic to malicious networks. Implications of BGP can lead to disruption and network shutdowns. It also disrupts global networks. Ransomware attacks use various techniques to capture and hijack organization or user’s files. According to Reshmi, ransomware attackers are using crypto currency to take ransom as it is an untraceable payment method and conceals the attacker’s identity.

Pegasus Spyware

Pegasus spyware is one the most dominant spyware developed. Once a device is infected it can turn into a surveillance device and can be accessed anytime. Pegasus spyware is developed by an Israeli company NSO Group. The spyware can get access your entire phone. It can see all your messages, photos, files, and call logs. It can also activate your phones camera and microphone without user knowledge. The spyware is very powerful and can track your location and location history. Pegasus can be installed on a device through malicious links and other vulnerabilities in common applications. The spyware can also be installed using a wireless transmitter if the target is nearby or manually if the attackers get access to the device.

Pegasus uses zero-day vulnerabilities and security loopholes to infect devices. Both android and iOS devices are vulnerable to Pegasus spyware. One its installed on a device, it can copy any data and transmit it to the attacker. The spyware can see text messages, emails, apps, WhatsApp chats, activate microphone, record phone calls, see call records, track location, and activate camera. The spyware gives an attacker the access to the entire phone and even administrative privileges. In almost all cases it is hard to prevent this attack and to stop it since its easily installed and the attacker can delete data thus preventing the owner from finding out. In my opinion Pegasus spyware has changed security of phones and individual privacy forever. The spyware is powerful and can access all data on a device without the owner’s knowledge. If Pegasus gets in hands of criminals, they can steal a lot of information and cause lot of loss to organizations and people.

NSO says that its software is law enforcement, military, and governments and is intended to use against criminals. There is nothing stopping government or other officials with the access to the spyware to use it for their benefit or other unintended reasons. Many journalists and activists around the world have been targeted. Pegasus is being used in forty countries and there are many allegations against NSO of enabling governments to target certain people wrongfully. NSO has put out statements saying they were not involved or that they do not track how their clients use their technology. Journalists and activists that speak out against governments or government officials committing crimes fear for their life. They fear due to the power of Pegasus and how much information it can collect, access, and send to the attacker.

Currently Pegasus has been a trending topic in US and around the world due to its power, privacy, and misuse concerns. NSO has suspended access of its software to some countries for misusing it. US government has put NSO on entity list, which blocks sale and use of American technology to NSO. Software updates and security patches itself cannot prevent an attacker form infecting your device with Pegasus. Pegasus spyware should be carefully used and monitored to prevent any misuses.

Network Attacks

Cyber exploitation is worse than a cyber-attack since cyber exploitation is often more long-term and can-do significant harm to a person's physical safety and disrupts professional life and mental health. Exploit is way cybercriminals deliver malware. An exploit is a program or code that is designed to gain access to a victim's computer and steal personal information. Cyber exploitation can go undetected and cause a lot of damage. We hear and read about cyberattacks every day in the news, and they constantly happen all around the world. A cyber-attack is a malicious attempt by a person or organization to breach the network and systems of another individual/organization to gain benefit by disrupting their network. Cyber-attacks are also harmful because they cause substantial financial and data loss to organizations and personal data theft to individuals. Attackers also demand money to free systems or resources in some instances. (Figure 1) below shows the worldwide security spending by different segment during the years 2018 to 2020. The figure shows the spending in millions in U.S dollars on security in different segments. It costs a lot to prevent network attacks but it costs a significantly more to recover from an attack.

Different types of vulnerabilities exist, some are digital, and some are physical. Digital vulnerabilities are ones based on code or networks, and physical vulnerabilities include the physical safety of networking and computing devices. One vulnerability can lead to giving access to another part of the system. To fix or not to fix a known vulnerability depends on its type and severity. Cyber professionals should access all risks and have plans in place to prevent any breaches. Costs of fixing may be high in some cases, but if it's a high-risk vulnerability, then it needs to be fixed right there because a data breach due to that vulnerability will cost a lot more to the organization. In certain situations, you need the vendor to come fix security patches, but if it is not fixed on time, then it is a major risk. Regularly update all software and OS to keep all security patches up to date. Hackers target all vulnerabilities to gain access to systems.

**Conclusion**

Networks are highly targeted and with more devices connected we must ensure we follow best cybersecurity practices when using systems. Hackers are constantly evolving and using new methods to outsmart security measures in place. Users must ensure that all security features are used to prevent themselves from being an easy target. Antivirus software help detect viruses and malware on your computers. Operating systems and all software must get updated periodically to patch any security vulnerability. Network security will prevent damages and data loss.

Figures

Figure 1. Image. (2022). Embroker. https://www.embroker.com/blog/cyber-attack-statistics/

References

BBC. (2021, July 19). Pegasus: Spyware sold to governments 'targets activists'. BBC News. Retrieved November 30, 2021, from https://www.bbc.com/news/technology-57881364. Dana Priest, C. T. (2021, July 19). Private Israeli spyware used to hack cellphones of journalists, activists worldwide. The Washington Post. Retrieved November 30, 2021, from https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Guardian News and Media. (2021, July 18). What is pegasus spyware and how does it hack phones? The Guardian. Retrieved November 30, 2021, from https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

Harkins, Malcolm, and Anthony M. Freed. “The Ransomware Assault on the Healthcare Sector.” Journal of Law & Cyber Warfare, vol. 6, no. 2, [Daniel Garrie, Lexeprint Inc.], 2018, pp. 148–64, http://www.jstor.org/stable/26441292.

Mahmoud, Khalid Walid. Cyber Attacks: The Electronic Battlefield. Arab Center for Research & Policy Studies, 2013, http://www.jstor.org/stable/resrep12651.

Noor, Sitara. “Cyber (In) Security: A Challenge to Reckon With.” Strategic Studies, vol. 34, no. 2/3, Institute of Strategic Studies Islamabad, 2014, pp. 1–19, https://www.jstor.org/stable/48527537.

Palmer, Michael J. Hands-on Networking Fundamentals. Course Technology/Cengage Learning, 2013.

Shankland, S. (n.d.). Apple sues pegasus spyware developer: What you need to know. CNET. Retrieved November 30, 2021, from https://www.cnet.com/tech/mobile/apple-sues-pegasus-spyware-developer-what-you-need-to-know/.

Third Way. 2020 Thematic Brief: US Cybersecurity Efforts. Third Way, 2020, http://www.jstor.org/stable/resrep26169.

T.R. Reshmi, Information security breaches due to ransomware attacks - a systematic literature review, International Journal of Information Management Data Insights, Volume 1, Issue 2, 2021, 100013, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2021.100013. (https://www.sciencedirect.com/science/article/pii/S2667096821000069)