The Recent Controversies around Pegasus Spyware

Alysia Beckles
CYSE 462 Cyber Fundamentals
Old Dominion University
Chesapeake, USA
Abeck012@odu.edu

***Abstract*— *Although technological advancements mean to assist in enhancing people's lives, it has become a gateway to more evolved crimes that endangers the welfare of the public and domestic and financial security. There needs to be a defensive and offensive mechanism that will facilitate the necessary methods and procedures to tackle it. Pegasus spyware means to address this problem since it is sophisticated software that will discreetly perform its functions. This paper will examine Pegasus spyware and its intended purpose when introduced to the market. When using this software, the topic of privacy is contested between government organizations and users. Provides information on devices that are susceptible to the sophisticated attack and methods and precautions necessary to lessen the risk of it being performed on a user's device. There are some implications regarding maintaining privacy when Pegasus spyware performs its services.*

Keywords—Pegasus, spyware, zero-day, vulnerabilities, NSO Group, technology, security, government, smartphone, threat agents, cyberattack

I. INTRODUCTION

Around twenty years ago, the term spyware was coined by technology company Microsoft. Malicious software is known to be a combination of hostile and intrusive developed by hackers. Once the malware injects itself into devices, it will do all kinds of hostile actions, including modifying or destroying files and installing spyware that amasses sensitive information [1]. Spyware is defined as malicious software that is designed to obtain sensitive information and take control of devices from users without them knowing that it happened [2]. It is sophisticated software that examines users. Pegasus is a type of spyware that circumvents detection and conceals its tasks. The Israeli technology company, NSO Group, developed Pegasus in 2011 [3]. The name NSO Group derives from the first initials of the creators of the technology company, Niv Carmi, Shalev Hulio, and Omri Lavie [4]. Their purpose was to create technology that would aid governmental organizations to combat and analyze terrorism and crime to reduce their impacts [3]. It deploys as a defensive security measure rather than an offensive attack for those who use it ethically. It will eliminate the need for government organizations and others to ask a wireless service provider to give them information on the suspecting individual's device [4]. Originally in order to counter political adversaries and other threats, national governments would use traditional methods. These methods are conventional weapons such as guns, tanks, etc., to subdue them; they rarely use technology to collect information on adversaries and other threats. Technology has created and expanded industries that are further developing technical improvements. It comprises both benefits and challenges in security; there is an emerging threat as technology advances, especially when it comes to the security of a nation's critical infrastructure.

For political adversaries and other threat agents, the advancement of technology provides an avenue for promoting their cause and criminality, whether it be economic growth, state power, or political insecurity [6]. Although NSO Group wanted Pegasus spyware to help governments around the world, its intent to aid governments became overshadowed by threat agents and its misuse by the governments themselves. It is efficient and highly effective spyware that gives threat agents and governments the ability to have possession of the user's device, including text messages, passwords, call logs, emails, etc. [7]. The public scrutinized governments for utilizing this spyware since they would secretly gather information on those, they deemed suspicious, such as journalists, politicians, activists, etc.

This paper will discuss how spyware, Pegasus, operates and impacts security for users and governments. Section two (II) will be on how Pegasus spyware will target devices, while section three (III) will be the type of devices that will be compromised by it. The following section, section four (IV), relates to concerns over users' right to privacy. Then section five (VI) discusses issues of using the spyware to aid governments, and section five (V) are my final thoughts on the topic overall.

II. HOW DOES PEGASUS SPYWARE COMPROMISE DEVICES

A. The vulnerability it exploits

Pegasus spyware is considered to be one of the most sophisticated malicious software. There are three modes to install this type of spyware on users' devices, in person, by text, or by push notification. It is very destructive spyware since it focuses on a cyberattack, zero-day vulnerability. Zero-day vulnerabilities enable threat agents and government organizations to target devices or systems that have the disadvantage of not being up to date or patched promptly; it is undiscovered. It is named zero-day vulnerability because it is being referred to the number of days available to the software or hardware vendor to create a patch for this type of vulnerability [8]. When a someone utilizes a zero-day attack, they will target users that are considered high-profile and will target large businesses. Initially, there is not enough information on the vulnerability and how to approach it. Sometimes, zero-day vulnerabilities are not easily detected once the device is compromised since it does not have an available signature or a tool to prevent it [8]. The vulnerabilities that a zero-day cyberattack exploits are usually bugs, damaged algorithms, missing permissions, and concerns over the protection of passwords.

With Pegasus spyware, it will deceive the zero-day vulnerability and enable threat agents and government organizations to take complete authority over the user's device [9]. They will be able to collect information such as location, deleted content, phone calls, photos, etc. NSO Group's data server will store the information collected by Pegasus spyware. Those who utilize the spyware will have the ability to put up to at most fifty devices under surveillance at the same time [10].

B. *Scenario*

In order to execute this cyberattack, a possible scenario would be that Pegasus spyware will gain access to the user's device with a missed call through WhatsApp, a messaging application. The user with the compromised device will not have any knowledge of their device having Pegasus embedded in it. Another reason why the spyware is undetectable is that it does not take up a lot of space it is around five percent of the device's storage [10]. Since a zero-day vulnerability enables threat agents and government organizations to utilize the spyware, there will be little to no interaction between the user and their device by using the zero-click technique; it will initiate the tasks themselves [8].

If a user considers the message questionable and tries to get rid of it, the spyware will persist and compromise the device. Once Pegasus spyware installs on the user's device, the hacker will be able to infiltrate the device and gain access passwords, texts, emails, contacts, calls and send it to a third party. The malicious software, Pegasus spyware, can access encrypted files in the devices easily and efficiently, and will decrypt it and deliver it to a third party, NSO Group's data server [9]. They can filter through the information collected by Pegasus spyware and send to the data server [10]. The spyware can also incorporate hostile codes when calls are missed on the user's device and will delete traces of it occurring since call logs are removed instantly and Pegasus will self-destruct.

C. *Countermeasures*

Although Pegasus spyware will be difficult to properly mitigate since it uses a zero-day vulnerability, there are some ways that a user can do to avoid it. If a user is suspicious of a cyberattack compromising their device, there is an expensive option available. Having a forensic screening done by security experts that will examine the transfer of information going in and out the device will be helpful to see if Pegasus spyware is the cause. There needs to be a proactive approach in regards to avoiding this issue. In order to ensure security and create a fail-safe for information, there are some techniques required too. Devices on the public and unencrypted network will be susceptible to Pegasus. In order to prevent this from occurring, it is best for the user to have a virtual private network [9]. Another method to prevent this from happening is to make sure that devices are up to date and download the latest patches from the devices' vendors. Installing up to date anti-spyware software will ensure the protection of devices too [10]. Also, another countermeasure for Pegasus spyware is for users to configure their device. Using the default settings of a device will make it more susceptible to being vulnerable to spyware. Configuring the Firewall to disable specific traffic to filter through the devices, blocking certain protocols will help and add an extra layer for security.

III. What Devices Are Compromised By Pegasus Spyware

A. *Android Operating System*

With the Pegasus spyware, most of the devices targeted were smartphones. Pegasus spyware can compromise android smartphones since it depends on a rooting method that is not one hundred pc dependable [11]. Devices with the operating system android are open source this enables them to have extra features and optimize performance. Since there is a variety of devices that run on the operating system android, it is more susceptible to having unpatched devices. As a result, it will be easier for Pegasus to gain entry to android smartphones. Although smartphones can be compromised by Pegasus spyware since the software has a variety of hardware and software, there will be issues with executing a sole malicious mechanism to a vast user base [11].

B. *iOS Operating System*

In devices that had the operating iOS are Apple products such as iPhones, Pegasus would utilize the zero-day vulnerabilities CVE-2016-4657, CVE2016-4655, and CVE-2016-4656 [9]. Revealed cyber vulnerabilities are given a common vulnerabilities and exposures (CVE) numeral. CVE-2016-4657 is a safari exploit, while CVE2016-4655 and CVE-2016-4656 are two kernel exploits that can jailbreak the smartphone [9]. When there is a vulnerability in the safari browser for iOS, Pegasus spyware will have the ability to access the smartphone and take control over it. The spyware will embed the device with zipped files and install a root certificate that establishes a fraudulent certificate of authority. Although iOS devices have enhanced security and will not permit unsigned codes, Pegasus can create a code that will prevent it from being detected by the smartphone's programs and functions. It will listen to and record the traffic of programs running on the smartphone and share it with those who initiated the Pegasus. Then, it will turn off the deep sleep tool and create a self-destruct feature [9].

C. *Android Operating System vs iOS Operating System*

Devices with the android and iOS operating systems have reported several vulnerabilities in the past year. Android smartphones had around eight hundred vulnerabilities reported, while iOS smartphones' total was significantly lower at around three hundred. Although android devices had more vulnerabilities than iOS devices, iOS devices were compromised more by Pegasus [12].

The similarities are that Pegasus can extract information from communication applications such as Gmail, Facebook, and Skype on both operating systems. It also can make code unclear in android and iOS and deactivate updates. But Pegasus impacts a number of features differently in both operating systems [9]. For instance, in order to execute Pegasus spyware, there is way to inject it. For iOS devices, a phishing email or message will be sent to the user while for android devices, the way to inject it is undetermined [9]. The operating system android will have screenshot capture impacted.

IV. Concerns Over Privacy

A. Privacy in general

The spyware created by NSO Group is prone to infringing upon people's rights because of its design and the absence of guidelines and regulations to guarantee that it is being used properly. Pegasus harshly influences the freedom of privacy by design since the spyware is covert, intrusive, and enables the power to accumulate and transfer an infinite choice of confidential information [13]. It will meddle with most aspects of people's everyday lives. Ensuring that a device has protection from interference is imperative to maintain trust amongst users as society tries to implement more technology [10]. People can compromise users' devices and utilize them as a tool for surveillance is not agreed upon when people purchase smartphones. They do not expect their device to obtain sensitive information that is supposed to be known only by them and watch their activities. As previously stated, Pegasus spyware has the capability to not only read encrypted information from a user's smartphone but also send and receive it. Those who execute the spyware will be able to secretly listen to calls and record them [14]. Once People obtain that information it can be used for any purpose whether it is to convict the user or sell that information for nefarious reasons.

V. Pegasus Used By Governments

A. Expectations vs. Reality

As society has become more reliant on technology, there will be some issues that will arise, especially when it comes to the privacy of our information. When the government uses unauthorized techniques to gather personal information on individuals, such as Pegasus spyware. This information could include monitoring activity over the internet, email communications, and bank records. It is often considered to be infringing upon a person's rights to privacy. However, people expect the government to utilize its services to prevent criminal activities and dangerous events from occurring. If people want the government to protect them, there will be some tradeoffs such as their privacy. In order for the government to efficiently protect individuals from encountering terrorism and crime, they need to collect information that will help to deter adversaries. . That is view of government organizations concerning with implementing tools, procedures, and methods that challenge security and privacy.

B. Exposing Governments

Governments use Pegasus spyware to primarily monitor the activities of high-profile individuals, this includes politicians, journalists, activists, etc. Several publications revealed that Pegasus spyware has thousands of smartphones compromised [4]. They were also able to determine which governments use the spyware to put their targets under surveillance such as United Arab Emirates, Hungary, Saudi Arabia, India, etc. For instance, 2020 was a dangerous year for activists and journalists since a journalist had Pegasus spyware installed on their smartphone and people closely associated with him before he got murdered [15]. To justify this invasive and immoral behavior, governments claim that these targets are criminals will threaten their nation's security.

C. Governments Executing Pegasus Inappropieatly

There have been several incidents in which governments have executed Pegasus spyware to obtain confidential information. For instance, the United Arab Emirates government usually uses methods and techniques that will undermine the privacy of its citizens. In 2016 which was the first reported case of using Pegasus spyware inappropriately [16]. They chose a civil rights defender as a target, Ahmed Mansoor, and executed the spyware through an iPhone that is currently convicted. Another instance is when Hungary's government did not use Pegasus software correctly since they were trying to collect sensitive information on the photojournalist's smartphone in 2021 [16]. They chose the target of the photojournalist because they were investigating the prime minister of Hungary's friend. Another example is when Prince Mohammed bin Salman of Saudi Arabia initiated a hacking and misinformation crusade against activists. He would utilize Pegasus software to find activists and compromise their devices [16]. The examples above showcase that the spyware, Pegasus, is used by governments for superfluous reasons that were not for its intended use. Using spyware to monitor those with differing opinions is not terrorism or crime issue.

VI. Conclusion

A. Final Thoughts

Thus, Pegasus spyware is unregulated, and there are no proper guidelines established to solve this issue and hold governments responsible when using the tool. Although the spyware introduces as a security mechanism needed to investigate and compile information to counter security threats to the market, governments fail to recognize how to use it appropriately. A variety of threat agents and governments, especially those who often violate human rights can easily purchase this software. There are many issues surrounding privacy. Pegasus is dangerous since it will discreetly use intrusive techniques such as listening to private communication over the smartphone and collecting text messages. Without limitations and clarity, Pegasus spyware will persist to be used by dictatorial and repressive governments to target the public, activists, politicians, and journalists.

References

[1] J. F. Kurose and K. W. Ross, “Computer Networks and the Internet,” in Computer networking: A top-down approach, Seventh., Hoboken, New Jersey: Pearson, 2017, pp. 1–824.

[2] H. M. Salih and M. S. Mohammed, "Spyware Injection in Android using Fake Application," 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 100-105

[3] Al Jazeera, “What you need to know about Israeli spyware pegasus,” Spy Cables News | Al Jazeera, 08-Feb-2022. [Online]. Available: https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus. [Accessed: 24-Apr-2022].

[4] J. Mason, “What is information warfare and how is it different from traditional warfare?,” Medium, 05-Dec-2019. [Online]. Available: https://medium.com/socialmedia-writings/what-is-information-warfare-and-how-is-it-different-from-traditionalwarfare-a42294ae8c8d. [Accessed: 24-Apr-2022].

[5] A. Chawla, “Pegasus Spyware – ‘A Privacy Killer.’” [Online]. Available: file:///C:/Users/Alysi/Downloads/SSRN-id3890657.pdf. [Accessed: 24-Apr-2022].

[6] J. Mason, “What is information warfare and how is it different from traditional warfare?,” Medium, 05-Dec-2019. [Online]. Available: https://medium.com/socialmedia-writings/what-is-information-warfare-and-how-is-it-different-from-traditionalwarfare-a42294ae8c8d. [Accessed: 24-Apr-2022].

[7] M. A. Joseph, S. Philip, B. Miranada, A. Deshmukh and N. Singh, "A theoretical workflow for the verification of embedded threats on mobile devices," 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021, pp. 75-80

[8] H. Al-Rushdan, M. Shurman, S. H. Alnabelsi and Q. Althebyan, "Zero-Day Attack Detection and Prevention in Software-Defined Networks," 2019 International Arab Conference on Information Technology (ACIT), 2019, pp. 278-282

[9] M. Agrawal, G. Varshney, Saumya, K. P. Singh, and M. Verma, “Pegasus: Zero-Click spyware attack -its countermeasures and challenges,” ResearchGate, Jan-2022. [Online]. Available: https://www.researchgate.net/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges. [Accessed: 24-Apr-2022].

[10] M. Patil and C. Mulimani, Pegasus: Transforming Phone Into A Spy , vol. 22, no. 14, pp. 7883–7890, Dec. 2019.

[11] P. Haskell-Dowland and R. Musotto, “Pegasus spyware: How it works and how to detect it,” Silicon Republic, 30-Jul-2021. [Online]. Available: https://www.siliconrepublic.com/enterprise/pegasus-spyware-is-my-phone-infected. [Accessed: 24-Apr-2022].

[12] G. Sims, “What is Pegasus and how is it used for spying?,” Android Authority, 25-Jul-2021. [Online]. Available: https://www.androidauthority.com/pegasus-spyware-1646458/. [Accessed: 24-Apr-2022].

[13] “In Bahrain hacked devices of three activists with spyware pegasus: Amnistia internacional: Venezuela,” In Bahrain hacked devices of three activists with spyware Pegasus | Amnistia Internacional | Venezuela, 18-Feb-2022. [Online]. Available: https://www.amnistia.org/en/news/2022/02/20346/in-bahrain-hacked-devices-of-three-activists-with-spyware-pegasus. [Accessed: 24-Apr-2022].

[14] F. Nkusi, “Use of pegasus spyware puts the right to privacy at stake,” The New Times | Rwanda, 21-Feb-2022. [Online]. Available: https://www.newtimes.co.rw/opinions/use-pegasus-spyware-puts-right-privacy-stake. [Accessed: 24-Apr-2022].

[15] S. Dennis, “The pegasus spyware scandal highlights the threats activists and journalists face,” International Republican Institute, 07-Jan-2022. [Online]. Available: https://www.iri.org/news/the-pegasus-spyware-scandal-highlights-the-threats-activists-and-journalists-face/?utm_source=www.democracyspeaks.org. [Accessed: 24-Apr-2022].

[16] R. J. Deibert, “Subversion inc: The age of private espionage,” Journal of Democracy, vol. 33, no. 2, pp. 28–44, Apr. 2022.