The Recent Controvereies around Pegasus Spyware

Natalie Hardwicke
Department of Cybersecurity
Old Dominion University
Norfolk, Virginia
nhard010@odu.edu

***Abstract*— A group from Israel called NSO has made a spyware called Pegasus. Spyware is a type of malware that infects a host and then has the ability to monitor/steal the information from the victim [7]. A majority of the time people do not realize they have been infected with spyware and likely never will. Pegasus has the ability to steal information from those infected with it and continuously see the data of the victim. NSO has sold this spyware to many countries, and there have been many problems because of it. Pegasus can be remotely installed onto a phone in several ways which makes it more dangerous. Privacy concerns of citizens have been brought up and if Pegasus is legal or ethical for countries to use. One focus will be the recent controversies in India and how the courts are trying to handle the situation.**

Keywords – NSO Group, Pegasus, Spyware, India, Privacy Concerns.

I. INTRODUCTION

Introducing new technology, software, and the Internet of Things (IoT) has helped solve numerous problems and provided a new era of information sharing. Yet, with this new technology comes a load of problems such as malware, social engineering, privacy concerns, spyware, and much more. Technology expanded so rapidly that many laws, security features, and necessary privacy protections have not caught up. This has and will continue to cause problems in the cyber realm. One problem that has affected several countries over the past couple of years is a software called Pegasus spyware which was made by the NSO Group. This spyware has called into question many things such as privacy rights, what NSO has access to, who the company is selling the software to, and much more. It is important to take a look at this malware to see exactly what it is, how it works, what can be done to prevent it, and the problems it has caused.

II. WHAT IS PEGASUS SPYWARE?

A. How NSO Group Describes Pegasus

The NSO Group is a company that is based in Israel. Throughout the scandals, outrage, and court cases surrounding Pegasus, the NSO Group maintains its innocence and that its software is used by governments for good. This company has made statements about the software and maintains a hard stance on its product.

NSO maintains it only sells surveillance software to other governments. There is an approval process done by the Israeli Military of Defense to gain a license to prevent the software from falling into the wrong hands. Plus, the company has consistently stated they do not control the systems that are given to these governments nor do they have access to the data of the targets of Pegasus [2].

These claims are the tip of the iceberg when it comes to the NSO Group trying to maintain their innocence and justify selling this horrific software. The NSO Group seems to promote Pegasus as a tool to help governments stop crime. Yet, based off of their statements, a person can only wonder how the company believes giving out this software can help countries and their citizens without harming them. Human rights seem unimportant to the company, when governments are handed this cyber tool and allowed to use it as they please. Even the Gulf Corporation Council believes that when countries acquire Pegasus, there is a huge risk for human-rights violations [5]. There is a thin line between government surveillance and abuse of power, which is the side Pegasus seems to be on.

B. What Devices Can Pegasus Infect?

Currently, Pegasus can infect mobile phones and other devices with certain operating systems. The two main operating systems that can be infected are Apple's iOS and Google's Android [1]. Devices with these operating systems are at risk because there are several vulnerabilities that Pegasus can take advantage of to gain access to download the software. Below are examples laid out by the Indian Future Foundation of vulnerabilities on the iOS system that Pegasus uses to download.

- CVE-2016-4657: Memory Corruption in WebKit - A vulnerability in Safari WebKit allows the attacker to compromise the device when the user clicks on a link [9].
- CVE-2016-4655: Kernel Information Leak - A kernel base mapping vulnerability that leaks information to the attacker that allows him to calculate the kernel's location in memory [9].
- CVE-2016-4656: Kernel Memory corruption leads to Jailbreak - 32 and 64-bit iOS kernel level vulnerabilities that allow the attacker to silently jailbreak the device and install surveillance software [9].

The above vulnerabilities are what allow Pegasus to discreetly download onto a target's phone either using clicked on links, which is what the older version of Pegasus relied on, or newer methods. These vulnerabilities are just a piece of how

Pegasus works. The next section will describe how the newest version of the spyware works.

C. How Does Pegasus Work?

As mentioned in the section before, the older version of Pegasus relied on the user to click on links sent using social engineering that enabled the spyware to be downloaded [9]. Now, the updated Pegasus software does not have to rely on the user to do anything, which makes that much more intrusive and not easily detectable. The NSO Group relies on zero-day vulnerabilities to be able to install the software with ease since, at that time, there was currently no patch or update that could fix it. The target is then sent a message or phone call. Even if the target does not answer or respond to the message, the malware is still able to install itself on the target's device. This process is known as "zero-click" attacks because the user does not have to interact with the spyware in any form [1].

Once installed, Pegasus has access to the target device's operating system. This access is what allows the spyware to hide, control certain aspects, and have access to an extreme amount of personal information on the device. Although missed phone calls or messages to the device itself are what normally occurs, Pegasus can also use apps to exploit vulnerabilities and install itself such as WhatsApp [4]. Below, Fig. 1 describes how a device is hacked and malware installed.

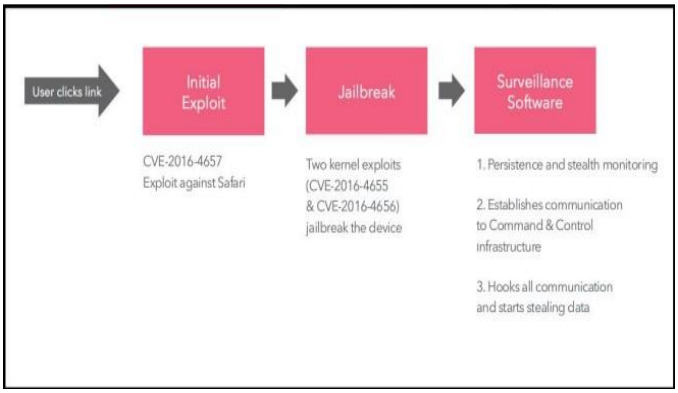

Figure 1: How a Pegasus Infected Phone Works [9]

D. What can be Monitored After Installation?

Since Pegasus has access to the operating system, a lot of sensitive information can be extracted or monitored. Many sources have detailed the amount that this spyware allows the hacker to see such as: [1], [8], [9]

- GPS location
- Calls
- Texts
- Apps (even encrypted ones like WhatsApp)
- Emails
- Access audio
- Access camera
- Website history
- Files
- Passwords
- Contacts

Fig. 2, from the Indian Future Foundation, shows a picture example of how Pegasus has a hook into every aspect of the mobile device. Before the information can get to the main Kernel of the mobile device, Pegasus has it first. The software monitors everything on the device and gather or extract any information the controller thinks are necessary.

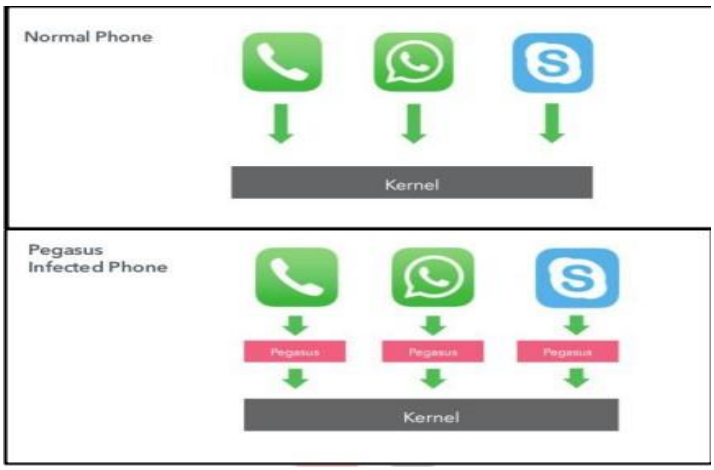

Figure 2: What a Pegasus Infected Phone Looks Like [9]

This malware can collect or extract data from almost all sensitive areas of a device. Even if the software is being used to help government institutions, the amount of control that is held by the hacker is immense. In these situations, the privacy of the user is violated and the government abuses the power they hold. In the world will live in today, people's whole lives are on their phones. People store sensitive information on it whether it is their social security number or just simple photos. Regardless of the reason a target's device is being looked at, citizens deserve privacy of their devices without fear of being illegally hacked by their government.

III. Privacy Concerns in India

A. Pegasus Scandal in India

In 2020 several reports came out that the Indian government as well as several other government entities, had used Pegasus software to spy on journalists, activists, and those with opposing views. Some of these figures had their phones professionally examined and it was determined that traces of Pegasus spyware were evident. Yet, when these reports came out, the Indian government refused to answer whether or not they had bought or used Pegasus software on Indian residents. To make matters worse, the NSO Group refused to acknowledge if the Indian government was a client and refused to release the identity of any clients of the company [2], [3].

B. The Indian Supreme Court Takes a Stand

After the reports about the Pegasus incident surfaced, government officials did not have an actual response or explanation for them. A statement given by the Indian Minister of Electronics and Information Technology goes as follows, "these attempts to malign the Government of India for the reported breach are completely misleading" [2]. Many responses by other government representatives were similar

and gave the people no insight as to what happened. These statements felt as if the Indian government was trying to deflect blame and keep its image clean. However, after reviewing the material about the Pegasus incident, the Indian Supreme Court officially ordered an investigation into the matter with an independent company [8]. This step taken by the Indian Supreme Court is a big win for Indian citizens. If this investigation is successful and proves the Indian government illegally spied on residents using Pegasus software, it could lead to better privacy protections. Plus, the Supreme Court could curtail the abuse of power held by the current government administration.

IV. Can citizens prevent Pegasus spyware

Pegasus spyware uses many different methods to install onto an individual's mobile device, so there is only so much someone can do. Since Pegasus relies on zero-click attacks and zero-day vulnerabilities, there is nothing a person or software developer can do to protect themselves against those types of attacks. However, there are certain precautions that users can take against older Pegasus spyware attacks along with other malware. Different sources have detailed several ways to prevent Pegasus plus other intrusive malware that are listed below [1], [9].

- Install latest updates or patches
- Never click on an unknown link
- Try not to connect to free or open Wi-Fi
- Use encryption for communication
- Ensure the websites you visit are legitimate
- Use anti-virus software for devices it is available on
- Use multi-factor authentication

While these methods can help prevent previous versions of Pegasus spyware and other malware, a true zero-day vulnerability is hard to stop. Prevention is key for known sources of vulnerabilities, but it is almost impossible to stop an attacker from exploiting vulnerabilities unknown to any user or software designer. The most important thing for users to do is try to stay aware of current patches, gain cyber awareness, and take the necessary steps to protect any technological devices from stoppable attacks.

V. Who does the responsibility fall on with Pegasus?

This paper has covered how Pegasus works, privacy concerns, and even what individuals can do to prevent this intrusive software, but who does the responsibility of it all fall on? There are several factors that come into play and different groups do have to hold themselves accountable. Users of smartphones and other mobile devices need to be aware of the cybersecurity risks, privacy concerns and be responsible for updating their technology. Smartphone companies and software developers should be responsible for ensuring their products are safe for users, getting out upgrades or other patches, and trying to make users aware of the risks that can occur in cyberspace. Yet, the biggest responsibility of all falls upon governments when talking strictly about Pegasus spyware.

Pegasus has been described by the Indian Supreme Court as a "military-grade spyware" that is "capable of extremely intrusive surveillance" [8]. Not to mention the fact that the NSO Group markets and sells this product to governments or government entities. So, in regards to Pegasus, it should be a country's government that is responsible for legally and responsibly using this weapon, not the user or the developers. Plus, since Pegasus is regarded as a military weapon how are ordinary people expected to be responsible for trying to prevent such an attack? Deibert describes this situation perfectly saying "the average citizen does not have the resources or expertise to defend themselves against such attacks" [6]. It is up to the government to pass laws, hold officials accountable, and ensure citizens' privacy rights are being protected from any cyberweapons including those they possess.

VI. Conclusion

Overall, Pegasus can be used by governments for good, but from reading articles, reports, and other information, it seems to do more harm than good. Government entities in India and other countries have abused the Pegasus software to gain information on those who do not agree with their views. This type of intrusive malware being used by governments around the world has a thin line between legality and abuse. India can be used as an example of the abuse and potential backlash that can occur when a government uses Pegasus without thinking of the privacy or rights of the people. A majority of average people the software would be used on do not have cybersecurity training or awareness of these problems to prevent Pegasus or any other spyware. It is up to the governments of each country to protect the privacy and rights of its citizens. Although "governments are slow to wake up to the urgency of establishing protocols for cybercrime" now is the time to do so [6]. Laws, regulations, and other protocols to prevent cyber-attacks, malware, and other forms of harmful cyberspace operations need to be at the forefront. People need to start talking about these issues now because the cyberworld will continue to advance.

Acknowledgment

Although writing this paper took a lot of time, effort, research, patience, and motivation, I feel as if it has helped me get a different view into the cybersecurity world. I would like to thank Professor Zehra for giving us this paper in the first place and allowing us to write about the topic. Everything I have looked at has given me new insights that I will continue to carry with me into my professional career as well as teach me how to write in IEEE format.

References

[1] A. Chawla, *Pegasus Spyware – "A Privacy Killer."* Modolva, Europe: Eliva Press, 2021. [ebook]

[2] "Anatomy of the Pegasus Spyware in India," sflc.in, Jul. 22, 2021. [Online]. Available: https://sflc.in/anatomy-pegasus-spyware [Accessed Apr. 15, 2022].

[3] A. Dhillon and M. Safi, "Indian supreme court orders inquiry into state's use of Pegasus spyware," *The Guardian*, Oct. 27, 2021. [Online] Available: https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware. [Accessed Apr. 18 2021].

[4] M. Frary, "Tools of the Real Technos: The Current Autocrats Have Technology Bent to Their Every Whim. We're Vulnerable and Exposed," *Index on Censorship*, vol. 48, no. 4, pp. 24-26, Dec. 2019. Available: SAGE Journals, https://journals-sagepubcom.proxy.lib.odu.edu/doi/pdf/10.1177/0306422019895716. [Accessed April 15, 2022].

[5] B. Hassib and J. Shires, "Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy," *Middle East Policy*, vol.29, no.1, pp. 90-103, 2022. Available: Wiley Online Library, https://onlinelibrary-wileycom.proxy.lib.odu.edu/doi/pdf/10.1111/mepo.12616.

[6] R. Deibert, "Investigating targeted espionage: Methods, findings, implications," IEEE International Symposium on Technology and Society, 2021, Keynote Address. [Online]. Available: IEEE Xplore, https://ieeexplore-ieee-org.proxy.lib.odu.edu/stamp/stamp.jsp?tp=&arnumber=9629176. [Accessed April 18, 2022].

[7] A. Mittal. "Resolving the meance of spyware through implementations in apllication layer and network layer," Students Conference on Engineering and Systems, 2012. [Online]. Available: IEEE Xplore, https://ieeexplore-ieee-org.proxy.lib.odu.edu/document/6199053.

[8] The Supreme Court of India, "N. Ram & Anr. V Union of India & Ors." 2021. [Online] Available: https://images.assettype.com/barandbench/2021-08/bfcc2639-b1ec-48fc-a6ce-0aca9548254d/N_ Ram_ v_Union_of_India__Ors.pdf. [Accessed April 19, 2022].

[9] "India Future Foundation's Analysis on Pegasus Spyware," India Future Foundation,2021.[Online]Available: https://www.indiafuturefoundation.com/wp-content/uploads /2021 /08/PegasuS228.pdf. [Accessed April 18, 2022].