Pegasus Software and Recent Controversies

Clarence V. Kimbrell Jr.

Cybersecurity

Old Dominion University

Yorktown, York County

ckimb002@odu.edu

***Abstract* – Pegasus software has come to everyone's attention surrounding recent controversies around the world in many different countries. Pegasus software is referred to as spyware that enters a person's cellphone without detection. Then have full control over crucially private things such as microphones and cameras. This is especially disturbing because the reliance on technology has never been so high. Over the years the method of entry has varied drastically and becoming more developed still with little to no detection.**

Keywords* – *Spyware, Spear Phishing, End User Agreements

I. INTRODUCTION

Pegasus Software is classified as spyware[1]. The first use of spyware can be denounced to the traditional hidden camera in a plant example. As more of the world was becoming connected through technology this means of these techniques and strategies of spying had to develop as well. The first recorded record of modern spyware was in 1999 by Steven Gibson [1]. He found that the software on his computer was tracking and stealing personal and secret information. Then he retaliated by creating something that most people will be aware of and that is an anti-spyware program [1]. Many of our devices are built with these anti-spyware and anti-virus programs to elevate potential victimization. This does not eliminate the problem for example Pegasus software has been operating since 2011[11]. Many cybersecurity professionals state it has reached 50 countries worldwide, and infected normal citizens, CEOs of companies, and political figureheads [11].

II. CYBERWARFARE

Cyberwarfare is a fairly new domain of combat in which spyware lies. Cyberwarfare attacks do not need to follow ordinary requirements and regulations. For example, chains of command and rules of engagement are standard for traditional warfare, but the exact opposite is true for cyberwarfare. It crosses multiple international borders even ones that are not even a part of what is occurring. This new domain started in the early 2000s when government agencies could operate within their borders and still fight for what they wanted to achieve thousands of miles away. This opened the door to many organizations jumping to prevent this from occurring in their systems. Then there are the hacker groups that also found a new way to wage war on any target. In the past, it was common for nations to wage war on each other with their respective militaries. Now, it can be any ordinary individual with the knowledge to potentially take down a nation. This has raised the alarm bells to quickly find and prevent any means of cyberwarfare.

III. CREATION

Pegasus Software was created in 2011 by a company in Israel named the NSO Group [11]. They are most known for their spyware Pegasus, which gives them access to smartphones. The original intent of Pegasus was to create spyware that would benefit governments to monitor and track crime and terrorist attacks [11]. The internet has put them in the spotlight for stepping out of their boundaries. Despite preventing multiple terrorist attacks and organized crime, companies and government officials employ them to conduct searches on ordinary people and figures of authority [5]. The company's ideology is similar to many others around the world.

IV. WHAT DEVICES ARE VULNERABLE

The spyware software specifically targets mobile devices. Our reliance on mobile devices has drastically changed everyone's lives who owns them. It makes accomplishing

[1] Spyware is defined according to the Oxford Dictionary as "software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive."

tasks much easier than before. So, most people struggle or feel the need to look back at it when it is removed. Most people use mobile devices for essential activities such as to monitor workout progress or to get directions from their phones' GPS. Then the more widely accepted use of mobile devices is for entertainment. So, the NSO group concluded that most people cannot live without mobile devices. Then came the realization that everyone carries their phone with them practically at all times. Pegasus software created a parasite for mobile phones that is unseen by humans and attaches essentially to the human aspect as well to observe and collect data from said phone and by extension the human behind the screen. Mobile phone companies are trying to crack down on spyware and create ways to defend their customers, but as time progresses so do new ways for mobile devices to become vulnerable.

V. HOW IT OPERATES

Pegasus spyware software has developed over the years. The first main practice for accessing someone's phone remotely was spear phishing emails [3]. These are malicious mimics of emails that carry infectious malware that can be activated by simply clicking a link or just by opening the email itself. Many businesses have required training for phishing exercises on a weekly or monthly basis to inform their employees of the potential harm they could cause. Then missed phone calls became the newest wave observed, just by simply calling back a missed call from a number is enough to infect one's device [3]. This is dangerous for an ordinary person because they receive many unknown phone calls per day. So simply just trying to figure out who can try contacting you if enough to have installed spyware on one's device. The methodology will change again in the future due to an increased number of aware individuals, similar to what occurred with phishing emails. This is not to say these methods will become obsolete in the future because that is the furthest from the truth. More developed and intrusive ways of accessing one's mobile device will be created. According to TECH2 NEWS STAFF, it can intercept calls, handle encrypted information, and pinpoint targets [14]. NSO can learn a lot about a person very quickly with the use of Pegasus software. Intercepting calls is a more developed way than the traditional bugged phone. Collecting calls while they are in transit between destinations is far more effective than trying the traditional archaic practice. We learned that Pegasus spyware seeks to find encrypted information that is then collected and studied, if the information has life-threatening contents actions are taken immediately to prevent such an event [11]. Then last but certainly not least is the pinpoint targets, we discussed that many of us nearly always carry our phones with us at all times [14]. This is good news for NSO but not so much for the one who is being tracked and targeted our phones are beacons that could potentially let the world around us know exactly where we are, at any given time.

VI. WHAT CAN BE LOST

Many believe all hope is lost when they hear the truth about their cell phone being infected but that is not entirely the case. Pegasus aims to target certain aspects of one's phone such as encrypted information, messages, location, and even make phone calls with your number ID [9]. Most importantly, the biggest concern of all is the loss of privacy without acknowledgment. Many people act differently under a spotlight but if it never is shown they will act themselves. This information can be used against them such as political figures speaking about controversial topics and being in locations they are not supposed to be. This type of information gathering is far faster than traditional methods of physical spies and hidden cameras. The use of technology is a gold mine for spyware companies to extract information without immediate repercussions. Spyware in general has phycological factors on humans if they are discovered [13]. Some people might develop social problems and phobias such as social anxiety disorder. This takes away from people being themselves because of malicious hackers and unsafe cybersecurity practices.

VII. PREVENTION

Many cybersecurity professionals have made extensive lists of ways to reduce the chance of installing spyware drastically. Those include the following but not limited to [10].

- Installing anti-spyware and anti-virus software.
- Do not click on unknown links.
- Practice finding phishing emails.
- Reading and understanding End User License Agreements.
- Avoid voice messages and missed calls from unknown users.
- Only accepting cookies from trusted websites.
- Downloading only trusted applications in the App or Google Play stores.

VIII. PEGASUS RECENT CONTROVERSIES

It was reported by the New York Times that the Indian government purchased a two-billion-dollar defense package from Israel [3]. This had a wide range of items in the purchase ranging from hacking programs including Pegasus to missile systems. The report came to light when a yearlong investigation found enough evidence to believe that the Indian government deployed Pegasus to investigate former and current government officials. These investigations did not stop at government officials, they also included members of the Indian military and the judicial systems [3]. Since the report, the Indian government has denied any claims of spying on officials with Pegasus from NSO group in Israel. Its original intent was to study criminals and terrorists. It is thought that the people affected by the Pegasus software came from users of WhatsApp [3]. This is one of the world's leading messaging apps globally that connects countries thousands of miles away. The investigation reported over three hundred Indian mobile phones across the country were on a target list for the use of Pegasus spyware [13]. As discussed earlier this is a breach of privacy that the victims are unaware of. Activists in the country are pushing for this practice to come to an end because it threatens democracy. One thing to note from this story is that stories like these have been reported around the world since the NSO group creation of Pegasus back in 2011. Unauthorized spying on suspects brings a lot of attention to the offenders. Which normally have to change their ways afterward by popular demand.

IX. CONCLUSION

The original intent for the creation of Pegasus spyware software was to investigate criminals and terrorists [4]. Just like many things in life things can be used for different purposes under the disguise of its original. Governments around the world purchase this program to do such that. Unauthorized spying on individuals of authority to bring them into the light for their true opinions and agendas. This creates controversy among governments, then denies their roles in the use of spyware. This has a snowball effect on the country’s population. If we take a look back at India many civilians agree with Rahul Gandhi[2] that it threatens democracy. The use of Pegasus around the world is only going to increase because we live in an age where information is more valuable than natural resources. As more of the world adopts this type of living more users become victims of the use of Pegasus.

X. ACKNOWLEDGMENT

I would like to thank Professor Zehra for providing a great topic to research it has been a pleasure. Then a special thanks to the authors provided below.

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, Ron Deibert, Stephanie Kirchagaessner, Daniel Bennett, Bhanukiran Gurijala, Samuel Woodhams, Mayank Argawal, Saumya Kakandwar, Gagan Varshney, Kaushal Pratap Singh, Ajay Chawla, Rashid Muhammad Usman, Garapati Balakrishna.

XI. REFRENCES

A. Chawla, “Pegasus spyware – 'A privacy killer',” *SSRN*, 09-Aug-2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890657. [Accessed: 23-Apr-2022].

Adaware Authors, “The history of spyware – Adaware - support.adaware.com,” *Adaware*, Oct-2021. [Online]. Available: https://support.adaware.com/hc/en-us/articles/360046760131-THE-HISTORY-OF-SPYWARE. [Accessed: 23-Apr-2022].

B. B. C. Authors, “Pegasus: India Parliament opens amid furore over pegasus 'lies',” *BBC News*, 31-Jan-2022. [Online]. Available: https://www.bbc.com/news/world-asia-india-60194265. [Accessed: 23-Apr-2022].

B. Gurijala , “What is pegasus? A cybersecurity expert explains how spyware invades phones and what it does when it gets in,” *The Conversation*, 26-Jan-2022. [Online]. Available: https://theconversation.com/what-is-pegasus-a-cybersecurity-expert-explains-how-the-spyware-invades-phones-and-what-it-does-when-it-gets-in-165382. [Accessed: 23-Apr-2022].

B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak, and R. Deibert, “Hide and seek: Tracking NSO group's pegasus spyware to operations in 45 countries,” *TSpace*, 18-Sep-2018. [Online]. Available: https://tspace.library.utoronto.ca/handle/1807/95391. [Accessed: 23-Apr-2022].

D. Bennett, “Pegasus: A cyber security expert explains how the zero-click spyware can hack phones without user interaction,” *Pegasus: A cyber security expert explains how spyware can hack phones | BBC Science Focus Magazine*, 02-Aug-2021. [Online]. Available: https://www.sciencefocus.com/future-technology/pegasus-a-cyber-security-expert-explains/. [Accessed: 23-Apr-2022].

Kaspersky, “What is spyware?” *usa.kaspersky.com*, 20-Apr-2022. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/spyware. [Accessed: 23-Apr-2022].

M. Agrawal, G. Varshney, S. Kakandwar, and K. P. Singh, “Pegasus: Zero-click spyware attack its countermeasures and ...,” *Research Gate*, 20-Jan-2020. [Online]. Available: https://www.researchgate.net/profile/Gagan-Varshney-2/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges/links/61e9174ec5e3103375a8ff5a/Pegasus-Zero-Click-spyware-attack-its-countermeasures-and-challenges.pdf. [Accessed: 23-Apr-2022].

[2] Member of the Indian National Congress

M. Agrawal, G. Varshney, S. Kakandwar, and K. P. Singh, “Pegasus: Zero-click spyware attack its countermeasures and ...,” *Research Gate*, 20-Jan-2020. [Online]. Available: https://www.researchgate.net/profile/Gagan-Varshney-2/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges/links/61e9174ec5e3103375a8ff5a/Pegasus-Zero-Click-spyware-attack-its-countermeasures-and-challenges.pdf. [Accessed: 23-Apr-2022].

M. U. Rashid and B. Garapati, “Prevention of Spyware by Runtime Classification of End User License Agreements,” *DIVA*, 16-Jun-2009. [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=. [Accessed: 23-Apr-2022].

N. S. O. G. Authors, “NSO Group - Cyber Intelligence for Global Security and ...,” *NSO Group*, 25-Jan-2011. [Online]. Available: https://www.nsogroup.com/. [Accessed: 23-Apr-2022].

S. Kirchgaessner, “FBI confirms it obtained NSO's pegasus spyware,” *The Guardian*, 02-Feb-2022. [Online]. Available: https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware. [Accessed: 23-Apr-2022].

S. Woodhams, “Spyware: An unregulated and escalating ... - skeyesmedia.org,” Aug-2021. [Online]. Available: https://www.skeyesmedia.org/documents/bo_filemanager/CIMA_Spyware-Report_web_150ppi.pdf. [Accessed: 23-Apr-2022].

T. News staff, “Pegasus spyware: A complete guide to what it does and how it can be used to infiltrate all aspects of your digital life- technology news, Firstpost,” *Tech2*, 01-Nov-2019. [Online]. Available: https://www.firstpost.com/tech/news-analysis/pegasus-spyware-a-complete-guide-to-how-it-can-be-used-to-infiltrate-your-phone-7585931.html. [Accessed: 23-Apr-2022].

T. Webdesk, “Tehelka WebDesk,” *Tehelka*, 02-Feb-2022. [Online]. Available: http://tehelka.com/a-new-report-reignites-pegasus-snoopgate-controversy/. [Accessed: 23-Apr-2022].