The Recent Controversies around Pegasus Spyware

Quintin Sumpter

CS462

04/24/2022

***Abstract*—This paper will discuss the Pegasus spyware created by an NSO group based in Israel and how this spyware is possibly being used in multiple countries to target one another.**

I. Introduction

Technology has been an amazing wonder for the world coming with a multitude of benefits such as advanced communication, improved productivity, advancement in modern medicine, better mobile options, finding answers to complex solutions, etc. With such an amazing evolution of technology comes many negative effects with the biggest issue possibly being data corruption and hackers. End-to-end encryption is a solution to help keep messages secure during the passage from sender to recipient. End-to-end encryption is a solution to help keep messages secure during the passage from the sender to the recipient [3]. Having encryptions such as this is very useful so innocent citizens will not be watched as if they are criminals. An NSO group that is located in Israel created technology to bypass these encryptions allowing for all to be watched. The device is spyware technology by the name of Pegasus and is being purchased by all willing to pay, even by government officials.

II. Pegasus

A. How Pegasus is used

As explained in [1] Pegasus is spyware technology that will be given a specific target, once sent it will either be activated by the touch of the recipient or is self-activated. Call logs, contacts, automatic video capturing, automatic audio capturing, and location data are all captured from cell phones.

B. About Pegasus

Originally introduced in 2011, Pegasus aided Mexican officials in the capture of the infamous El Chapo. Pegasus also continued to show case its ability when used in Europe when aiding in the capture of multiple terrorists, organized criminals and putting a stop to a global child abuse ring by identifying suspects within 40 different countries as stated in [2,3]. The world of crime was proven to be more difficult to handle nowadays because of the difficulty that government investigators are now having when attempting to decrypt criminal databases as said in [2].

III. Why People Would be Affraid

Pegasus has proven to be something extremely extraordinary and amazing, but it is very dangerous within the wrong hands. With the ability to hack into technology without being prompted to activate and forcefully capture all audio and visual images without the device owner even noticing before it's too late.

This is meant to aid in the prevention of criminal activity and also help capture criminals that are hiding in the open public. Though this is helpful, it can become an unwanted invasion of privacy since those in use of technology are automatically at risk of being seen in their most vulnerable state, in the supposed "comfort" of their privacy. Naturally, everyone would be scared and afraid when their deepest and darkest secrets are being recorded without them knowing. Some people have personal rituals they practice or messages between a significant other not meant for prying eyes. This device was supposedly made with good intentions, but in the eyes of the public this could gain negative feedback causing an uproar among the citizens.

A. Advancement of Pegasus

Pegasus is a highly advanced system with what could almost be considered limitless capabilities. The spyware is not limited to simple hacking of live camera footage, Pegasus can read and understand screenshots then provide feedback on those screenshots to the controller [1].

B. Pegasus of capabilities (all capabilities are direct intext citations from reference[1])

- Intercept calls: Transparently monitor voice and VoIP calls in real-time
- Bridge intelligence gaps: Collect unique and new types of information (e.g., contacts, files, environmental wiretap, passwords, etc.) to deliver the most accurate and complete intelligence
- Handle encrypted content and devices: Overcome encryption, SSL, proprietary protocols and any hurdle introduced by the complex communications world
- Application monitoring: Monitor a multitude of applications including Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)
- Pinpoint targets: Track targets and get accurate positioning information using GPS

- Service provider independence: No cooperation with local Mobile Network Operators(MNO) is needed
- Discover virtual identities: Constantly monitor the device without worrying about frequent switching of virtual identities and replacement of SIM cards
- Avoid unnecessary risks: Eliminate the need for physical proximity to the target or device at any phase

C. Possible AI Solution

In reference [6,7] a fully controlled AI cyber defense was tested. An AI defense could be the necessary resource to handle not only Pegasus spyware but also a multitude of other cyber-attacks. Having a cyber-defense that can react to various cyber-attacks and also provide information on where attacks are more likely to strike has the ability to be the next high-end technology. If done properly, this AI cyber defense could maybe eliminate a few hackers and cyber-attack situations. I believe that this could possibly provide the upper hand needed to really make cyberspace a safer place for the innocent. This could hopefully be the advancement needed to force hackers into a cave with the struggle of getting passed an AI defense prevention.

D. Recent Pegasus Timeline (This is a direct reference from [4])

- July 18, 2021- A global collaborative investigative project revealed that Israeli company NSO Group's Pegasus spyware targeted over 300 mobile phone numbers in India including that of two serving ministers in the Narendra Modi government, three Opposition leaders, one constitutional authority, several journalists and business persons. The Wire reported that the database included at least 300 phone numbers of human rights activists, lawyers, journalists, politicians, and dissidents from across the country.
- • July 19, 2021- The Centre unequivocally denied all 'over the top allegations' of surveillance using Pegasus Spyware. The Union government called the story "sensational", and seemed to be an attempt "to malign Indian democracy and its well-established institutions". Minister for Electronics and Information Technology Ashwini Vaishnaw also said that the reports appearing a day before the Monsoon session of parliament cannot be a coincidence.
- July 19, 2021- The NSO Group claimed that the allegations of snooping were false and misleading. "The report by Forbidden Stories is full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources. It seems like the 'unidentified sources' have supplied information that has no factual basis and is far from reality," the NSO Group said in a statement.
- July 20, 2021- During the monsoon session of Parliament, the Congress demanded a probe by a Joint Parliamentary Committee into the Pegasus snooping controversy. The Congress along with other parties also stalled proceedings of both houses of Parliament while raising the issue.
- July 22, 2021- A petition was filed in the Supreme Court seeking a court-monitored probe by a Special Investigation Team (SIT) into the Pegasus spyware scandal. It also sought prosecution of "all accused persons/ministers for buying of Pegasus and snooping on citizens of India" – including politicians, journalists, and activists – "for their vested political interest since 2017".
- July 22- After the BJP claimed that Amnesty International had said that the list of phone numbers suspected to be under surveillance was not directly related to the Israeli company NSO Group, the global human rights group issued a statement debunking the "false rumors" and "inaccurate media stories". Amnesty International said that it "categorically stands by" the findings of the investigation.
- July 23, 2021- Congress leader Rahul Gandhi accused Prime Minister Narendra Modi of "treason", called for the resignation of Union Home Minister Amit Shah, and demanded a judicial probe into allegations of surveillance using Pegasus spyware
- July 25, 2021- CPI(M) Rajya Sabha member John Brittas approached the Supreme Court seeking a court-monitored probe into the Pegasus spyware controversy by a special investigation team (SIT). The plea urged the court to direct the Centre to conduct an "immediate investigation through a special investigating team" into the allegations "as revealed by The Wire" news website on July 19.
- July 27, 2021- West Bengal Chief Minister Mamata Banerjee announces a commission of inquiry into the alleged surveillance of phones using the Pegasus spyware developed by the Israeli cyber-intelligence company NSO Group. Retired Supreme Court judge Justice Madan B Lokur, and former Chief Justice of Calcutta High Court, Justice (retd) Jyotirmay Bhattacharya, were appointed as members of the commission.
- July 29, 2021- Over 500 individuals and groups wrote to Chief Justice of India (CJI) N V Ramana seeking immediate intervention of the Supreme Court in the snooping scandal. They also sought a moratorium on the sale, transfer, and use of Israeli firm NSO's Pegasus spyware in India.
- August 5, 2021- The Supreme Court heard eight petitions seeking an independent probe into the matter. Describing the allegations of surveillance through the use of the Pegasus spyware as "serious", the Supreme Court wondered why no one had filed an FIR if there was reason to believe that phones had been hacked. It also pointed out that the allegations first surfaced in 2019. The bench did not issue notice to the Centre and instead asked the parties to first supply copies of their petitions to the government counsel after which it would hear the matter again on August 10.
- August 16, 2021- The Supreme Court said it cannot compel the "reluctant" Centre to file a detailed affidavit

on petitions seeking to know if Pegasus spyware was used to snoop on certain citizens and what steps it took to probe the allegations. In an affidavit, the Centre told the SC that "with a view to dispelling any wrong narrative spread by certain vested interests and with an object of examining the issues raised", it would set up "a Committee of Experts in the field which will go into all aspects of the issue".

- August 17, 2021- Former RSS ideologue K N Govindacharya moved the Supreme Court urging it to revive a petition filed by him in 2019 – and later withdrawn – seeking registration of an FIR and a National Investigation Agency (NIA) probe against Facebook, WhatsApp, and Pegasus spyware maker NSO Group, over alleged snooping charges.
- August 17, 2021- The Supreme Court issued a pre-admission notice to the Centre on a batch of petitions seeking an independent probe into the scandal, while also observing that it will not ask the government to disclose information that affects national security interests. The apex court said it will discuss and decide the future course of action after the government reiterated that the matter had national security implications due to which it did not want to put the details in a public affidavit.
- September 12, 2012- The Supreme Court reserved its interim order on petitions seeking a probe into the surveillance allegations, with the Centre reiterating that it was ready to have all questions gone into by a committee of experts, but did not want to put it in the public domain for reasons of national security.
- October 27, 2021- Ruling that the state does not get a free pass every time the specter of national security is raised, the Supreme Court appointed a committee to conduct a "thorough inquiry" into allegations of use of Pegasus software for unauthorized surveillance

IV. Possible Solutions to Surveillance Abuse(*This is a direct reference from [5])*

•Governments should impose a moratorium on the sale, export, transfer, and use of surveillance technology until human rights safeguards are in place. They should also disclose any existing contracts or any use of such technology.

• Governments should apply relevant sanctions, such as the EU's global human rights sanctions regime and the US Global Magnitsky Human Rights Accountability Act. This will commercial spyware companies that are responsible for or complicit in serious human rights abuses to cut them off from the financial or technical infrastructure they need to operate. Only if they can demonstrate that they have undertaken specific measures or demonstrated a change of policy that will end the human rights abuses or violations that gave rise to the sanctions. They can then get their connections back.

• Governments should ensure that any use of surveillance technology in their countries is subject to domestic laws. Governments should enforce or reform laws to remove legal or other barriers to effective remedies for victims of unlawful surveillance. They should also ensure that both judicial and nonjudicial paths are available for victims to seek a remedy for the harm surveillance technology may have caused.

• Governments should allow the sale, export, and transfer of surveillance technology to resume only when they have enforceable legal frameworks in place. Governments that have demonstrated disregard for human rights and have a pattern of abusive use of technology should be on a "do not sale" list.

• Governments should also require private companies based in their countries to disclose information on products and services, their sales and exports, and the identity of clients. Governments should establish independent oversight to monitor private companies. Governments should make this information available in public registries. The purchase of surveillance technology by law enforcement in any country should be transparent so that it can be subject to public debate.

• To encourage accountability, the relevant experts associated with the United Nations and regional human rights mechanisms should monitor and investigate the use of spyware by governments and sales of spyware by companies.

V. Conclusion

Pegasus spyware is a cyberspace technological advancement that needs to desperately be treated with caution. Technology such as this is extremely dangerous in the wrong hands and even with it being used by the government properly, the public may not take a liking to being spied upon without consent in the places they should seem safe. There can be many recommended solutions to help the situation, but they need to be put into a plan of action and thoroughly tested. There is still no guarantee that these solutions listed above will be able to fully take away cyber-attacks with the speed of evolution in cyber technology. There could very well be a hacking device to eliminate them, but that is where governments will need to also advance in the cyberspace field to protect their individual countries and keep trust in their people.

References

[1] A. Chawla, "Pegasus spyware – 'A privacy killer'," *SSRN Electronic Journal*, 2021.

[2] R. Bergman and M. Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, 28-Jan-2022. [Online]. Available: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html. [Accessed: 22-Apr-2022].

[3] B. Gurijala, "What is pegasus? A cybersecurity expert explains how the 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: 24-Apr-2022].

[4] "A timeline of the pegasus snooping scandal," *The Indian Express*, 27-Oct-2021. [Online]. Available: https://indianexpress.com/article/india/a-timeline-of-the-pegasus-snooping-scandal/. [Accessed: 24-Apr-2022].

[5] S. Shankland, "Pegasus Spyware and Citizen Surveillance: What You Need to Know," *CNET*, 19-Apr-2022.

[6] S. M. Istiaque, M. T. Tahmid, A. I. Khan, Z. A. Hassan and S. Waheed, "State-of-the-Art Artificial Intelligence Based Cyber Defense Model," 2021 IEEE International Conference on Service Operations and Logistics,

and Informatics (SOLI), 2021, pp. 1-6, doi: 10.1109/SOLI54607.2021.9672393.

[7] K. M. E. N. Mallikarajunan, S. R. Preethi, S. Selvalakshmi and N. Nithish, "Detection of Spyware in Software Using Virtual Environment," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1138-1142, doi: 10.1109/ICOEI.2019.8862547