PEGASUS SPYWARE SOFTWARE: IS IT A THREAT TO THE RIGHT TO PRIVACY

Lakshyadeep Verma, UPES, Dehradun

ABSTRACT

The more we know about technology, the of we came to know about its flaws of it. When they came to know about the very same, they start misusing them. Similarly, was done by the NSO group developed spy software that was stealing civilians' data without their permission.

So, through this, we will be knowing what are the impacts of this software and how it is affecting society, and what precautions we should take. As stealing personal data is a violation of the right to privacy. So, we will discuss what are the precautions we had to take while using the technology and how this software has affected the right to privacy.

Apart from this, we had to also discuss what are the preventive measures we had to take against such software and what are the steps which are being taken now by the government.

Introduction

In this current scenario, everyone is moving toward technological development and advances to use new software and apps which make their work more efficient. In this move towards technological advancement, we sometimes make such big mistakes whose consequences can be too dangerous. Similarly in the year of 2011, software was made by the Israeli cyber-arms company NSO Group which was named Pegasus spyware software. This software can be easily installed on mobile phones running most versions of iOS and Android. Pegasus was capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps. The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones. 2011 saw the first development of Pegasus 1. According to the NSO Group, the malware was developed to aid governments in their fight against terrorism and crime. Researchers at the University of Toronto made the initial discovery of the spyware in 2016 with the aid of the software provider Lookout. A false SMS message was sent to Ahmad Mansoor, an Arab human rights campaigner, which led to the discovery.

Over 1,400 phones were hacked using WhatsApp in 2019 thanks to spyware. The Israeli cyber-arms business, NSO Group, which was mentioned above, created Pegasus. Pegasus had access to a target's smartphone, microphone, and camera as of 2022, and it could read text messages, monitor phone calls, gather passwords, and use position tracking. This software has a very negative impact on the society. The Pegasus spyware has also had a negative impact on India's national security. This software can use someone’s data for blackmailing him and misuse the data of her against herself only. This software is violating the right to privacy of the citizens and misusing their data for their use and demanding a large sum of money from them.

How this software works and impacts society?

The noticeable thing here is that it follows the zero-click method i.e., the device owner even isn’t required to click on the message, mail, link, etc., or to give any input to make the malware work. On top of that, if the user finds something suspicious and deletes the message – the spyware would still infect the device. And once the Pegasus gets into your smartphone, now your text messages & emails, contacts, photos, passwords, etc. can be accessed by the other party. The access is given to such an extent that even your device mic or camera can also be

operated by the one who is spying on you very conveniently. The Pegasus Spyware can even access end-to-end encrypted messages or files as it can now steal them before the encryption or after the decryption.[1] This software operates in the following ways:

- Initial Infection: Pegasus typically infects devices through social engineering techniques, such as sending a malicious link via SMS, email, or messaging apps. When a user clicks on the link, the device becomes infected with the spyware.

- Device Exploitation: Pegasus takes advantage of undisclosed vulnerabilities, known as "zero-days," in the device's operating system or installed applications. These vulnerabilities allow Pegasus to bypass security measures and gain deep-level access to the device.

- Stealth Installation: Once the device is compromised, Pegasus installs itself silently without the user's knowledge or consent. It disguises its presence by using advanced evasion techniques, such as encrypting its code, hiding in system files, and regularly changing its file names.

- Remote Control and Monitoring: Pegasus establishes a covert communication channel with a command-and-control (C&C) server operated by the attacker. Through this channel, the spyware receives instructions and sends back the collected data from the infected device.

- Surveillance Capabilities: Pegasus has extensive surveillance capabilities. It can access various features and data on the compromised device, including calls, messages, emails, contacts, calendar events, browsing history, location data, microphone and camera usage, and even encrypted communications.

- Continuous Updates: NSO Group regularly updates Pegasus to include new exploits and bypass security patches released by operating system developers. This allows the spyware to remain effective against the latest defense, making it challenging to detect and remove.

[1] GeeksforGeeks, https://www.geeksforgeeks.org/what-is-pegasus-spyware-and-how-it-works/ (Last visited July 09, 2023).

The impact of Pegasus spyware on society is significant and raises serious concerns regarding privacy, security, and human rights. Here are some of the key societal impacts associated with the use of Pegasus:

- Invasion of Privacy: Pegasus is capable of collecting extensive amounts of personal information from infected devices, including sensitive data such as private conversations, emails, location history, and more. This invasion of privacy infringes upon individuals' rights to keep their personal information confidential.

- Surveillance and Suppression: Pegasus has been used to target journalists, activists, lawyers, and human rights defenders, among others. This can have a chilling effect on free speech and the freedom of the press, as individuals may fear being monitored, leading to self-censorship and a restriction of democratic principles.

- Threat to Dissent and Democracy: Pegasus enables governments and other entities to monitor and gather information on political opponents and dissenting voices. By surveilling and suppressing opposition, it undermines democratic processes and institutions, hindering the ability of individuals to express their opinions and participate in public discourse freely.

- Human Rights Violations: The use of Pegasus has been associated with human rights abuses. Activists and journalists have been subjected to harassment, intimidation, and even physical harm as a result of the information gathered through spyware. This poses a direct threat to fundamental human rights, including the rights to privacy, freedom of expression, and freedom of association.

- Cybersecurity Risks: The existence of powerful surveillance tools like Pegasus highlights the potential vulnerabilities in mobile operating systems. The discovery and exploitation of zero-day vulnerabilities by such spyware expose individuals and organizations to cyber threats. This necessitates a greater focus on strengthening security measures and ensuring prompt patching of vulnerabilities to protect against similar attacks.

- Trust and Credibility: The proliferation of spyware like Pegasus erodes public trust in technology and digital systems. When individuals and organizations fear that their

devices can be compromised and their privacy violated, it undermines confidence in the digital infrastructure and raises concerns about the integrity and security of communication channels.

Impact of the Software on the Right to Privacy

In a landmark decision on August 24, 2017, the Supreme Court of India declared the right to privacy act to be a fundamental right protected by the Indian Constitution. The Court's decision, holding that this right comes from the fundamental right to life and liberty, has far-reaching consequences.[2] This fundamental right is stated in Article 21 of the Indian Constitution. The right to privacy upholds an individual's autonomy to make decisions about their personal life, relationships, and lifestyle choices free from unwarranted interference. This right also states the individual right to their data. Even this right allowed communicating with someone else and keeping it confidential. Digital communications, personal gadgets, and online activities of persons are all covered by the right to privacy, which also protects them from unauthorized access, data breaches, and surveillance.

In the case of Justice **K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors**.[3] The Supreme Court held that the Right to Privacy is a fundamental right protected under Article 21 and Part III of the Indian Constitution. This spy software affects the day-to-day life of an individual. This software without your permission accessed your data which had an adverse effect on the right to privacy of the citizens of India in various ways:

- Pegasus violates the privacy of selected individuals by breaking into their devices without authorization and gathering copious amounts of personal data. This includes information from private conversations, emails, internet history, and more. Such invasive surveillance infringes the person's right to privacy since it impairs their ability to protect the confidentiality of their personal information.

- Free speech and freedom of expression are made more difficult by Pegasus and other related spyware. People may self-censor or stop expressing their thoughts openly when they are aware that their conversations and actions could be monitored. This limits their

[2] K. S. Puttaswamy (Retd.) and Anr. v. Union of India, (2017) 10 SCC 1.
[3] Indian kanoon, https://indiankanoon.org/doc/127517806/ (last visited July 09, 2023).

right to privacy and restricts their freedom of expression.

- Pegasus has been linked to the unlawful surveillance of a variety of people, including journalists, activists, attorneys, and human rights defenders. Pegasus violates the right to privacy and makes it possible to monitor people who are involved in legitimate and legal activities by focusing on people based on their political opinions or participation in particular activities.

- Pegasus attacks computers without the user's knowledge or permission. The notion of informed consent, a key component of privacy, is violated by this. Pegasus undermines people's right to control and knowledge over what is installed on their devices by functioning secretly and without permission.

- The public's faith in technology and digital systems is damaged by the usage of Pegasus. Individuals trust in the digital infrastructure is damaged when they are unable to be certain that their communications and equipment are safe from unauthorized surveillance. The exercise of private rights is hampered by this decline in confidence, which may have wider societal repercussions.

- Pegasus' discovery and use of vulnerabilities expose potential flaws in mobile operating systems and the necessity of strong cybersecurity measures. This underlines the significance of safeguarding privacy against future cyber threats that could take advantage of such weaknesses in addition to targeted malware.

Precautions that one should take against this spy software's

In the present scenario, cyberattacking activities have increased too much due to which the citizens as well as the whole nation had to suffer. By keeping all these activities in Mind, the Government of India has taken certain steps:

- Cyber Surakshit Bharat Initiative: It was launched in 2018 to spread awareness about cybercrime and build capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

- National Cyber Security Coordination Centre (NCCC): In 2017, the NCCC was developed to scan internet traffic and communication metadata (which are little snippets

of information hidden inside each communication) coming into the country to detect real-time cyber threats.

- Cyber Swachhta Kendra: In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.

- Indian Cyber Crime Coordination Centre (I4C): I4C was recently inaugurated by the government.

- National Cyber Crime Reporting Portal has also been launched pan India.

- Computer Emergency Response Team - India (CERT-IN): It is the nodal agency that deals with cybersecurity threats like hacking and phishing.

By keeping all these activities in mind, we had to take some preventive measures against them:

- Use Strong Passwords: Use the different password and username combinations for different accounts and resist the temptation to write them down.

- Keep Your social media accounts private: Be sure that you keep your social networking profiles (Facebook, Twitter, YouTube, etc.) private. Be sure to check your security settings. Be careful of what information you post online. Once it is on the Internet it is there forever.

- Secure your Mobile Devices: Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources. It is also crucial that you keep your operating system up-to-date. Be sure to install anti-virus software and use a secure lock screen as well. Otherwise, anyone can access all your personal information on your phone if you misplace it or even set it down for a few moments. Someone could even install malicious software that could track your every movement through your GPS.

- Protect your data: Protect your data by using encryption for your most sensitive files such as financial records and tax returns.

- Protect your identity online: When it comes to protecting your identity online it is better

to be too cautious than not cautious enough. It is critical that you be cautious when giving out personal ID such as your name, address, phone number, and/or financial information on the Internet. Be certain to make sure websites are secure when making online purchases, etc. This includes enabling your privacy settings when using/accessing social networking sites.

- Keep your computer current with the latest patches and updates: One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.

- Protect your computer with security software: Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defense. It controls who and what can communicate with your computer online. You could think of a firewall as a sort of "policeman" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic such as attacks from ever reaching your computer.[4]

For detecting this software, the government has also taken some steps against it like, establishing a technical committee to investigate the allegations of misuse of Pegasus spyware. The committee was headed by former Supreme Court judge Justice R.V. Raveendran and submitted its report in December 2021. The report found that Pegasus spyware had been used to target a number of Indian citizens, including journalists, activists, and politicians. Introducing new laws and regulations to govern the use of surveillance technology. In 2022, the Indian government passed the Personal Data Protection Bill, which sets out new rules for the collection and use of personal data. The bill also includes provisions that specifically address the use of surveillance technology. Launching a public awareness campaign about the dangers of Pegasus spyware. The campaign aims to raise awareness of the signs that a device may be infected with Pegasus spyware and how to protect oneself from infection.

[4] Swati Shalini, how to prevent cybercrime in India? Myadvo (July 09, 2023, 23:32), https://www.myadvo.in/blog/cyber-crime-in-india/

Conclusion

Even after watching too many incidents of cyberattacking which affects the entire nation. We must take a lesson from them. In the need of knowing the latest technology we sometimes do things that affect our security. After this, we had to be stressed and had to suffer a lot. So, it is better we must take a lesson from the previous incidents and use the technology which we got in our hands like mobile phones, laptops and use them very carefully. Even a small mistake can be brought us into trouble. So, it is better that we should use this technology in the ways which had been discussed above.