THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Pegasus: Transforming Phone Into A Spy

*** Manjugouda R Patil ** Dr. C.F.Mulimani**

*Research scholar, Department of Criminology and Forensic science, Karnatak Science College, Dharwad, Karnataka.

**Research supervisor, Associate professor, Department of Criminology and Forensic science, Karnatak Science College, Dharwad, Karnataka.

ABSTRACT

Pegasus is spyware that can be installed on devices running certain versions of iOS, Apple's mobile operating system and android devices, developed by the Israeli cyber arms firm, NSO Group. It is believed to have broken through encrypted communication systems such as WhatsApp, Skype, Facebook etc. The company has stated that, it only sold its technology to licensed government intelligence and law enforcement agencies to help them fight terrorism and serious crime. Pegasus is a modular malware that can initiate total surveillance on the targeted device & can extract calls, contacts, messages, emails, photos, files, locations, passwords. The Spyware enters the phone even if the call is not answered & the report of that call log also gets erased. To ensure that it is never found out, Pegasus is designed to never use more than 5% of the free space on your phone. Security experts have repeatedly advised against downloading suspicious files by clicking on unknown links. The Facebook-owned messaging service listed the *two* precautionary measures in a message to users it believed were affected by the sophisticated Pegasus spyware. "*How to stay secure*: Always use the latest version of WhatsApp & keep your mobile operating system updated to receive the latest security protections" it read. Ironically, these instances point out to a weakening of India's cyber sovereignty. If the Indian state plans to leverage offensive and defensive cyber capabilities, it needs to get serious about cyber security, both for its own narrow, political interests as well as those of its citizenry.

KEYWORDS: Pegasus, Spyware, Smartphones, Operating System.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

1. INTRODUCTION

Security and privacy issues are in the focus like never before. New viruses, security compromising software bugs and various forms of malicious software threatens the integrity of our data as well as our own on a daily basis. Most of these threats have been around for quite some time but the last few years a new type of threat has become more and more frequent. In this paper, we will examine what spyware really is and how it relates to other forms of malicious software such as viruses and trojans.

2. SPYWARE

Malware is short for malicious software and used as a single term to refer to virus, spyware, worm etc. Malware is designed to cause damage to a stand-alone device or a networked device. So wherever a malware term is used it means a program which is designed to damage your device. It may be a virus, worm, spywares or trojan. Spyware is a type of program that is installed with or without your permission on your personal device to collect information about users, their browsing habits, tracks each and everything that you do without your knowledge and send it to a remote user. It also can download other malicious programs from the internet and install it on the device. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware type program or application. Spyware can be divided into several categories but the major ones are:

- Personal Espionage

  The primary use of spyware is to spy on a spouse. Other common areas of use are parental supervision of children to protect them from online crime and children spying on their parents to find out credit card information or to avoid the parental control.

- Corporate Espionage

  In many work environments with strict demand for security, communication monitoring is used to protect company secrets. It is however much debated whether it is ethical (or even legal) to monitor your employees or not. Some claim that the personal integrity risk outweighs the possible benefits while others think that the one who pays the salary should be able to confirm that it is well spent. One spyware application on a key machine in a company can reveal a wealth of sensitive information, trade secrets and contacts. In spite of this, surprisingly many corporations do not take corporate data theft seriously.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

- Mass Espionage

  A very common form of spyware is the non target specific one. Instead as many people as possible are targeted, often to show advertisements but also to gather demographical and behavioral data. Although it can be argued that the directed forms of spyware are the most serious ones, maybe compromising very sensitive data, it is probably the 'mass espionage' that constitutes the overall largest nuisance.

2.1 PEGASUS

Pegasus, the spyware sold by Israel's NSO Group and Q Cyber Technologies that is believed to have broken through encrypted communication systems such as WhatsApp, can concurrently monitor about 50 smartphones i.e the spyware can monitor up to 500 phones in a year, but can only track a maximum of 50 at one go. WhatsApp recently confirmed that a spyware was being used by Israel based company NSO Group to spy on government officials, journalists, activists, lawyers, and various countries globally, including India.

2.2 WORKING OF PEGASUS

Pegasus is spyware that can be installed on devices running certain versions of iOS, Apple's mobile operating system, developed by the Israeli cyberarms firm, NSO Group. Pegasus is said to be around for about three years and it is not your ordinary spyware. Traditionally, Pegasus works by sending a link, and if the target user clicks on it, it is installed on the user's device. Once installed, it begins to contact control servers which allow it to relay commands so one can gather data from the infected device. It has the potential to steal your passwords, contacts, text messages, calendar info, as well as voice calls made through messaging apps, in this case, WhatsApp. It can even let the hacker have access to your phone's camera, microphone and GPS to track live locations. Pegasus has been around for at least three years and it was also believed to have been used to target Indians earlier as well. The spyware targeted vulnerability in WhatsApp, VoIP stack which is used to make video and audio calls. By just giving a missed call on someone's WhatsApp number allowed Pegasus to gain access to the device. It can also be used to track Android, iOS, BlackBerry OS and Symbian devices, and extract contacts, messages, emails, photos, files, locations, passwords, processes list. It can also be used to access password-protected devices

ISSN:0971-1260
Vol-22- Issue-14-December-2019

without leaving any trace and even self-destruct in case it is exposed. Pegasus can also retrieve any file from a device for deeper analysis. Once on your phone, Pegasus has access to data that's already on your phone, including photos, videos, text messages, email apps, browsing history, contact list, location, files, other messaging apps (like Viber, Skype, Messenger) etc. It can also listen to you and sounds around you through the phone's microphones, record incoming and outgoing calls, capture screenshots and use the phone's camera to take photos. Further, Pegasus doesn't transmit data when a smartphone is on roaming unless it's on WiFi. This is of course done to hide its tracks, since users might notice high data usage bills while roaming. Instead, the spyware collects and stores data on your phone in an encrypted buffer, waiting to transmit it once you're out of roaming. It does the same when the phone doesn't have an active Internet connection or is at under 5% battery. To ensure you never find out, Pegasus is designed to never use more than 5% of the free space on your phone. So, if you have 10GB of free space the malware will use only about 500MB at a time, something that's near impossible to detect on a smartphone, even if you're checking. Pegasus removes data on a first in first out basis if it hasn't been able to transmit to its servers for a while. NSO has created an "intuitive" front-end for users of Pegasus to parse through the data they gather. This allows operators of the programme to easily sift through the tonnes of data they might be getting through Pegasus. Interestingly, there's no real way to avoid a Pegasus attack other than the regular best practices. Security experts have repeatedly advised against downloading suspicious files, clicking on unknown links etc. and those remain the best way to fight this malware.

2.3 OTHER FAMOUS SURVEILLANCE PROGRAMS

- **RCS Android:** An Android surveillance tool designed by Milan-based company, Hacking Team. It is a data collection tool sold to law enforcement and government agencies. It was disguised as a news app on the Play Store and somehow escaped Google's security scans.
- **DROPOUTJEEP:** A program which was revealed to have been the go to tool for the US' National Security Agency (NSA), allowing it to compromise Apple's iPhones. It could access files on the device, read SMS texts, voicemail messages and more.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

- **XKeyscore:** The NSA, in its training material, called this its “widest reaching" system for gathering intelligence off the Internet. XKeyscore was amongst the programs revealed by whistleblower Edward Snowden.
- **Livestrong:** An exploit used by the US Central Intelligence Agency (CIA) to compromise devices running on Android 4.4 KitKat, revealed by WikiLeaks as part of the famous Vault7 data dump.

3. SPYWARE PREVENTION MEASURES

- Use anti-Spyware software, keep virus definition files updated, and scan your system for Spyware: By using anti-Spyware software or antivirus software, you can prevent Spyware from being installed and executed. Note, however, that the software and its definition files should be kept up-to-date. If any software (or part of the program) installed intentionally by a user is regarded as Spyware, he (or she) needs to remove it by himself, which means that such software should be used at the user’s own risk. Most of the recent antivirus software products are capable of detecting Spyware. However, not all Spyware can be detected and removed by these products. Although vendors of antivirus software and Anti-Spyware are striving to develop new detection methods and improve their programs in an attempt to deal with even unknown viruses (or Spyware), there is nothing perfect in this world; you should not rely too much on these products.
- Keep your device up-to-date: The existence of a Spyware program entering devices by exploiting vulnerabilities (security holes) has been disclosed. To mitigate vulnerabilities, it is important to keep your device up-to-date. Vulnerabilities can exist in not only the operating systems that are primary software programs, but other applications.
- Be careful about suspicious sites and emails: Do not access any suspicious sites that are retrieved by search engines, provided in Spam mail messages, or displayed on pop-up windows. If necessary, tighten up the security settings on browser. As in the case of virus mails, Spyware can be installed by opening a file attached to an email, or visiting a Web site whose URL is presented in an email message. Bear in mind the following points: Do not open any files attached to a suspicious email & Do not access any links presented in a suspicious mail message.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

- Enhance the security level of your device: Spyware can be installed by an external source hacking into your device systems. If configured properly, Firewall can prevent it. Depending on the firewall, data transmitted from an already installed Spyware can be blocked (using functions such as Application Firewall). When surfing the Internet, it is recommended to change the default security settings on your browser.
- In case of emergency, back up important files: In any case, to restore the healthy state of your device, you might have to initialize your system. Considering this, it is important to backup important files on a regular basis. If a malicious program has already been installed or the system has been modified by an attacker, you may have no choice but to initialize the hard drive. It is recommended to back up data on a regular basis.
- Do not input personal information on any device that is not under your control. It is recommended not to input personal information (such as bank account numbers, card information, etc) on any device that is not under your control, including the devices used for Net Café that can be accessed by any number of users. Be careful not to become a victim of a crime.

4. SURVEILLANCE LAWS IN INDIA

- Under both laws namely – the Indian Telegraph Act, 1885, which deals with interception of calls, and the Information Technology (IT) Act, 2000, which deals with interception of data – only the government, under certain circumstances, is permitted to conduct surveillance, and not private actors.
- Moreover, hacking is expressly prohibited under the IT Act. Section 43 and Section 66 of the IT Act cover the civil and criminal offences of data theft and hacking respectively.
- The IT (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules framed in 2009 under the IT Act: The rules state that only the competent authority can issue an order for the interception, monitoring or decryption of any information generated, transmitted, received or stored in any device resource (mobile phones would count). The competent authority is once again the Union Home Secretary or State Secretaries in charge of the Home Departments.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

- The Supreme Court in a landmark decision in August, 2017 (Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Others) unanimously upheld right to privacy as a fundamental right under Articles 14, 19 and 21 of the Constitution.
- The Data Protection Committee under retired Justice B.N. Srikrishna submitted a draft data protection law in 2018 which Parliament is yet to enact.

National Security Without Individual Privacy

- We must all recognize that national security starts with securing the smart phones of every single Indian by embracing technologies such as encryption rather than deploying spyware. This is a core part of our fundamental right to privacy.
- This intrusion by the spyware is not merely an infringement of the rights of the citizens of the country but also a worrying development for India's national security apparatus.
- The security of a device becomes one of the fundamental bedrocks of maintaining user trust as society becomes more and more digitized.
- Such an approach belies appreciating the injury and threats to individuals and the country.
- There is an urgent need to take up this issue seriously by constituting an independent high-level inquiry with credible members and experts that can restore confidence and conduct its proceedings transparently.
- The alleged spying on Opposition leaders and activists in India reminds one of the illegal espionage in the Watergate scandal.
- Given that NSO claims it only sells to governments and the fact that it is mostly critics of the ruling dispensation who have been targeted, some people have alleged that it is the Indian government that was behind the snooping.
- In response, the Union minister of IT Minister alleged that the former Indian government had spied on the then chief of the Indian Army as well as the Union Finance Minister.

5. CONCLUSION

Social media providers must stop chest-thumping, start investing in attribution solutions and be honest with users about the risks involved in their products. Such

ISSN:0971-1260
Vol-22- Issue-14-December-2019

software must be strictly controlled and legal provisions must be inked, so that providers of such technologies are deterred. Needless to say, a relook at laws, technology and ethics is needed, preferably sooner than later. In the digital age, companies will emerge and operate in the grey areas of the intersection between technology and security to make a profit. But national security must not be used as a shield by either governments or private players to justify the violation of fundamental rights. It is incumbent on Parliament, the judiciary and Facebook, the company that owns WhatsApp, to plug the breach of privacy and nail those responsible for it. Indian government must leverage its relationship with Israel to hold NSO to account. Since this attack involves users from a quite a few countries, there is a greater need for global cooperation to a concerted and coordinated investigation. The government has made it clear that it holds a sovereign right over the data of its citizens. The idea of data sovereignty must include a citizen's right to privacy. It must punish anyone found guilty of unlawfully violating the privacy of Indian citizens.

6. REFERENCES

1. Porter A. A day in the life of spies - spyware everywhere. http://www.spywareguide.com/, 2005.
2. Stern R.H. Ftc cracks down on spyware and pc hijacking, but not true lies. IEEE Micro, 25(1):6–7, 100–101, January 2005.
3. https://www.thehindu.com/news/national/what-are-the-surveillance-laws-in-india/article29993602.ece
4. https://www.ipa.go.jp/security/english/virus/antivirus/pdf/Spyware_measures_eng.pdf
5. https://www.ida.liu.se/~TDDD17/oldprojects/2005/final-projects/prj04.pdf

