iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44824

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Article on Role of Cyberspace in Geopolitics- Pegasus

Apoorv Yadav[1], Kumari Aanchal[2], Harsh Modi[3]
[1, 2, 3]*VIT University*

Abstract: ***In the sphere of information technology, cyber security plays a critical role. In today's world, protecting information and data security has become one of the most difficult tasks.***
Today in Geopolitics cyberspace has also become very important as it is the new warzone which can not only temper their internal security but economy too. Use of spywares, trojans and many malicious worms has increased exponentially, so we have tried to write an article by our own on one such spyware which was also a hotshot topic few times back "Pegasus".
Today, a cyber-attack will affect more people than any conventional attack .Though various steps have been taken in India to combat these attacks, but still there are some cyberweapons which are affecting the privacy and cyberspace at international level. There are some spywares which became popular like Stuxnet, DUQU, Botnet etc.as they became a threat to Confidentiality, Integrity and Availability of a nation.
Keywords: Pegasus Confidentiality Integrity Availability Data Security

I. INTRODUCTION

Today we live in the modernized world which is very competitive in every aspect and every countryor organization wants their supremacy over their arch rivals. With the popularity of cyber techniquesaround the world, cyberspace has taken the placeof war fields not entirely but majorly because through it we not only can easily disrupt internal security of any nation or organization but it can also temper their economic condition. In recent past, we have seen many such cases like Australia being attacked by China, US affecting Venezuela'scondition Israel developing Pegasus and many more.
It sums that every nation is investing in developing their cyberspace stronger because everyone knows that it plays a vital role in today's geopolitics. According to many researches it's found that primarily spywares have been used in many high- profile global instances.
Spyware is a malicious code, which enters your computer device, steal information and secretly deliver it to the third party without the consent of the user. Spywares can obtain owner's private information. It can have a list of websites visited , lists of passwords and credit card numbers .
Pegasus is a piece of malware categorized as spyware. The initial version of it adopted the mobile-first strategy." Pegasus" is the name of the winged horse of Greek Mythology. It is analogical to the winged horse as it is a kind of Trojan horse that can be sent "flying through the air " to infect phones secretly and specifically android and iOS versions. Pegasus uses zero-day vulnerabilities (weakness or error in the system which is disclosedbut not yet patched), code obfuscation (to make code difficult to understand), and advanced encryption. The user does not need to click on the message or anything to activate the malware.
According to the NSO group founders, it was said that "We're a total ghost", which means claiming tobe invisible. The intention behind the development of this Pegasus software is to help government bodies to prevent criminal activities. Gmail, Facebook, WhatsApp, Telegram, Apple's built-in messaging, and email applications are all vulnerable to it. It can be installed without the phone owner ever knowing. It is designed for mobile devices to gain access to the device and retrieve the data from the device without the user's consent. After stealing the data, it is delivered to the third party i.e. NSO's group server.

II. WORKING

At initial, it `used to gain access through a maliciousweb link through messages or email then it used to get installed automatically on clicking the link.
After some updates , it can be installed automaticallyeven by giving a missed WhatsApp call. It uses the framaroot technique which is capable of rooting android devices without the need of a computer or any other devices. In iOS devices, it relied on Zero- Day Vulnerabilities.

Let's take the example of WhatsApp. In a normaldevice, the communication is like
WhatsApp Kernel.
But if the device is infected by Pegasus, then thechange in communication will be like
WhatsAppPegasusKernel
which means all the information will be passed fromthe Pegasus first.

The workflow of Pegasus software is as follows:-

1) The attacker enters the contact details of thevictim.
2) It first goes with vulnerability. Using the vulnerabilities of the device, it can have fullaccess to the device.
3) Through spear phishing, the attacker sends theinstallation request to the victim via text or mail.
4) The victim will click on the received request.
5) After clicking on the link, the malicious codeof the spyware will start installing.
6) Then it will check whether the device is OSsupported? If it is OS supported, then it willinstall a spy agent on the device.
7) When the installation process is completed, it will be ready to collect and transmit data to anunknown location.
8) It can easily access our end-to-end encrypted files as well as messages and can decrypt withease.
9) It can leak the information to the third-partyserver.

III. AFFLICTION

It can do all different things like going through messages, checking videos, making phone calls, accessing call logs, tracking the location, can also turnon the microphone and camera as well as can have access to deleted content.
It can even give root access to the third party, which means they can easily also give access to the mic andcamera to them.
It can be installed on the device via physical touch,Text or email, or a message.
It is undetectable and untraceable because it leaves zero footprints of hacking. After adding the maliciouscodes through missed calls, it deletes call logs immediately.
It has a watch on the battery status of the device.
It analysis the current connection status, to transferdata across the web.

IV. WORKFLOW IN IOS

Firstly, it downloads some zip files on the device. Then it creates a fake Certificate of Authority to trust data encrypted by the attacker. iOS does not allow those codes which are not verified by a third party. To avoid this, the attacker installs a JavaScript file that executes the unverified code at the reboot time to jailbreak the device. To remain undetected in the memory occupied by running programs, Pegasus injects its code into the running process. After that, to monitor your running programs traffic, it installs the sniffer tool. A program named Daemon is installed by Pegasusitself to share the files present in the system to the outside server. It then installs the self-destruct feature, which makes Pegasus untraceable. Then it switches off the iOS device's deep sleep mechanism.

V. WORKFLOW IN ANDROID

It is known as Chrysaor meaning the one who has a golden sword. It is the name of the brother of Pegasus. It uses an android rooting approach called framaroot. It is third-party software. It asks the user for permission to access by pretending itself as trusted software. After the installation, it will remove the system update app and disables the automatic update. It disables the WAP push feature means we cannot go to a specially encoded message which includes a link to a WAP or WWW address. It then exfiltrates the data and shares the files present in the system with the outsider.

VI. CONCERN FOR MASS

NO, we should not be concerned about this spyware because it is very expensive and thus likely to be used by large organizations, andit also necessitates sophisticated handling. Even after that, if you believe you may become a victim of this spyware, doing the following can protect your device from attackof Pegasus-

1) One of the most fundamental approaches is to keep the device's operating system and other apps up to date.
2) Only open links or messages sent to you by recognized and trusted contacts on your device.
3) You should avoid using public Wi-Fi services.
4) Always keep a backup of any importantdata on your device.

5) Avoid downloading the apps from the third party resources .
6) When any app asks for permission , don't give special authorisation to it even if it claims.
7) Think before you click.

VII. HOW TO GET RID?

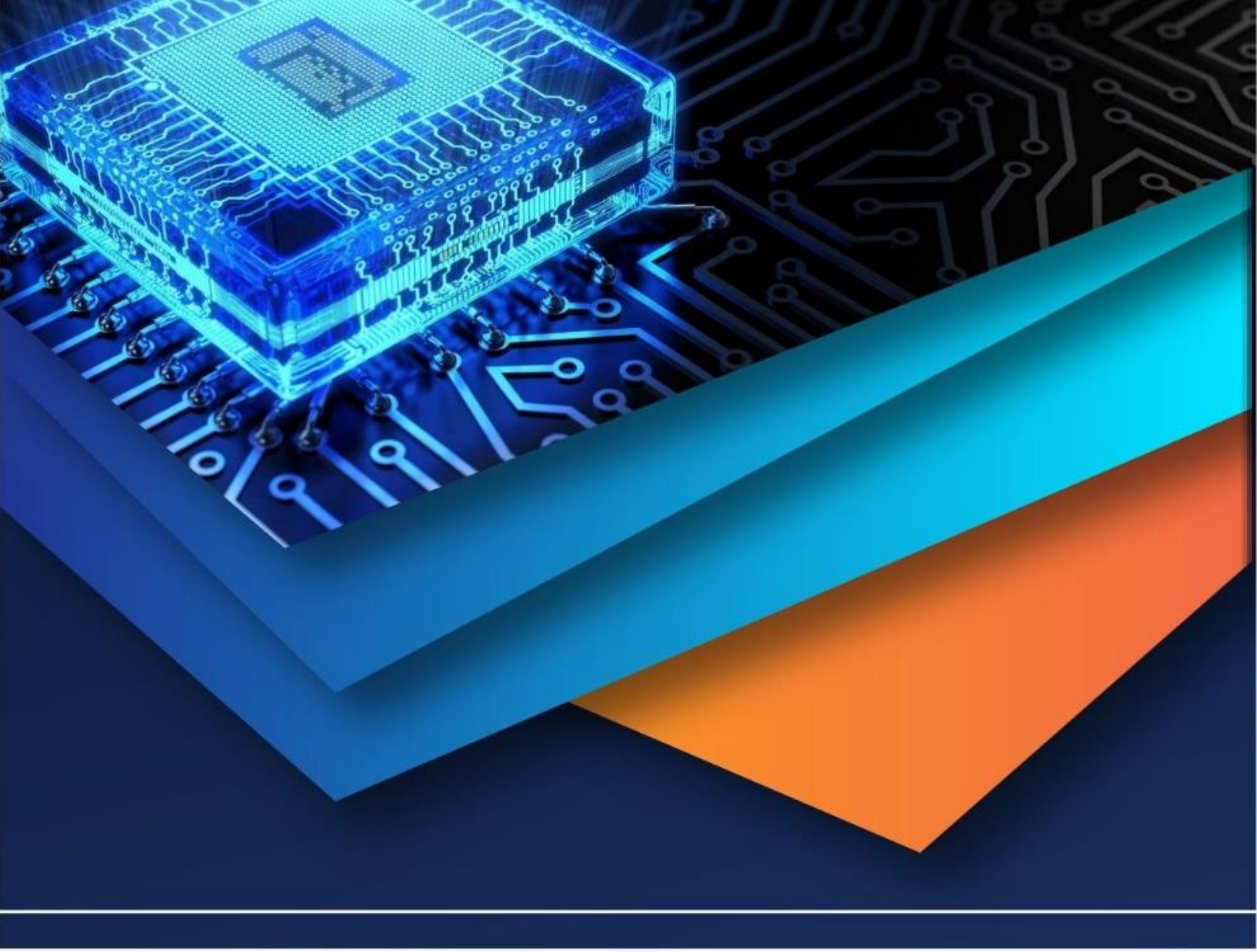
The worst part about Pegasus Spyware is that we can't figure out how it got onto our device. Once inside, it can destroy our privacy, but we can track it down with the help of some forensic tests. Simple steps to remove Pegasus explicitly could include restarting your phone, and that in some cases can temporarily remove the spyware's access to your device. Always install software updates as soon as they become available, and if you are a victim, remove iMessage on your iPhone for the time being.

VIII. CONCLUSION

We rely on our mobile devices to store and access our digital assets, even it is a primary source to transfer money and communication .Attackers see our mobile devices as a very easy target. NSO has generated millions of dollars by selling such a attacking software acting like a cyberweapon dealer. This emphasizes the necessity of keeping our devices up to date with the most recent updates and maintaining awareness about mobile device security.

REFERENCES

[1] https://www.gcsp.ch/global-insights/geopolitics-and
[2] https://www.drishtiias.com/printpdf/pegasus-spyware
[3] India Future Foundation Analysis on PegasusSpyware
[4] https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
[5] https://eurasiantimes.com/pegasus-spyware- controversy-israel-deletes-65-countries-from-its-cyber-export-list/
[6] https://www.researchgate.net/publication/357956844
[7] Pegasus Spyware – "A Privacy Killer" byAjay Chawla



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY