PEGASUS

Devadarsahn K Sardar   
Department of Networking and Communications, SRM Institute of Science and Technology, Chennai – 603203, India  
[ds5163@srmist.edu.in](mailto:ds5163@srmist.edu.in)

Gyanesh Samanta   
Department of Networking and Communications, SRM Institute of Science and Technology, Chennai – 603203, India  
@srmist.edu.in Sidhant Chourasiya   
Department of Networking and Communications, SRM Institute of Science and Technology, Chennai – 603203, India  
sc7643@srmist.edu.in

Dr. Vinoth Kumar CNS   
Department of Networking and Communications, SRM Institute of Science and Technology, Chennai – 603203, India  
vinothks1@srmist.edu.in

Ponnu   
Department of Networking and Communications, SRM Institute of Science and Technology, Chennai – 603203, India  
@srmist.edu.in

*Abstract*— *An Israel group named “NSO” developed weaponised software pertaining to cyber security and they have designed one spyware called “Pegasus”. Spyware is labelled as malicious code that installs itself on the target system and collects information regarding your behaviour and usage without the end-users knowledge. To monitor a system using Pegasus, the Pegasus operator does not even have to make the user click a link or give any input like in previous exploits. This is zero-click spyware where the target system can get infected without even clicking anything. The link is usually shared in the form of email or texts or it can be sent to the user in any way it seems valid to the user. When an operator sends a message to the target system the  Pegasus spyware implements exploits to the system which attacks the zero-day vulnerabilities in the system without giving any knowledge of this to the end-users. Once this is done the operator will have complete access to the target system and the operator will be able to execute commands, view data, etc. It will also enable hardware access to the operator who can even turn on the camera and microphone remotely. This is a technically challenging problem that we are currently facing as such software leaves little to no trace of its activity on the target system hence making it difficult to track.*

Keywords— Spyware, Pegasus, Zero-Click Attack.

# Introduction

In the context of cyber security, spyware is malicious code that is used by attackers to gather information about the victim’s system without any knowledge of the victim. According to the NSO Group, they only sell this software to “vetted governments” for “lawful interception”, which translates to battling terrorism and crime rackets. All programs will have certain indications for its presence like memory consumption, CPU cycle, etc. After the exploits, the data will be sent to the operator's C&C servers that use HTTPS, and since it uses this they have to register and maintain domain names which in turn can be used to track them for incidents. This paper predominantly covers the working and the different properties of the software. We also aim to analyse and detect the incidents that have occurred in the previous years. This can be done by fingerprinting and DNS cache probing. We will also detect where this spyware has been used and this is made possible because the devices infected with Pegasus will look up the Pegasus front-end servers. We also aim to review the incidents that have occurred over the previous years and find the number of nodes that have been compromised.

This paper will assist us to acquire appropriate knowledge about the Pegasus tool, by understanding some specific points

1. Working
2. How to check for compromise
3. Finding compromised nodes to see impact

# Technical working of pegasus spyware

## Delivery

The Pegasus virus frequently transmits via text message, email, or social media message to the target device. Frequently, includes a link that, when clicked, downloads the virus into the target device.

## Exploitation

Once installed, Pegasus exploits vulnerabilities in the operating system or other apps on the device to gain access to the device's data and functions.

## Privilege escalation:

Pegasus seeks to escalate its privileges on the device, granting it more extensive access to the device's data and functions.

## Data collection

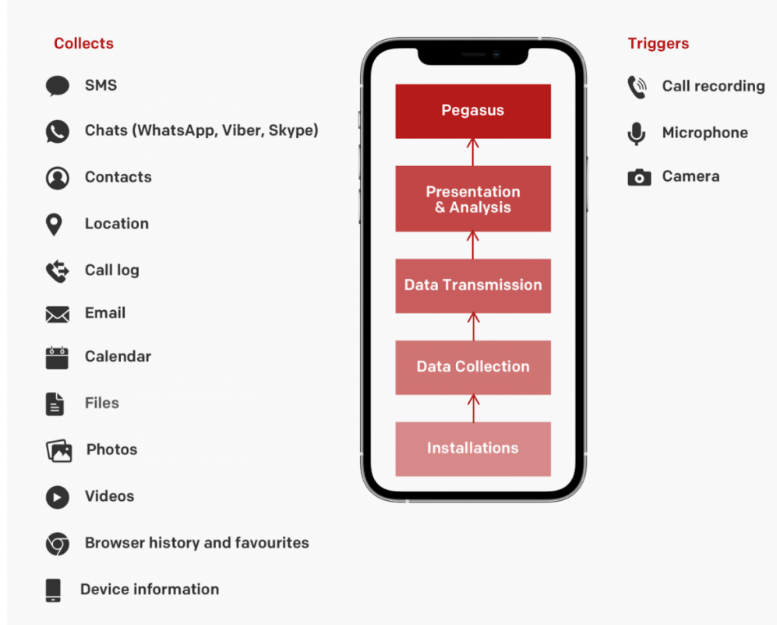
Pegasus then begins collecting data from the device, including messages, emails, photos, and contacts. It can also record conversations and track the device's location.

## Data exfiltration

The collected data is then exfiltrated, or sent to the attacker's server, where it can be analyzed and used for espionage or other purposes.

## Persistence

Pegasus is designed to be persistent, meaning that it can remain on the device even if the device is restarted or reset. This allows it to continue its surveillance activities over an extended period of time.



1. Different Layers of Pegasus

# How pegasus install on android and ios

Pegasus works similarly  on both Android and iOS devices, but there are some differences in how it functions on each platform because the operating systems and security models are different.

## Pegasus On ios

Pegasus usually infects iOS devices by way of a malicious link in a text message or email. Once installed, it can access the device's data and features by taking advantage of flaws in the iOS operating system. For instance, it has access to the phone's call history, contacts, messages, and images. It can also keep an eye on the microphone and camera on the smartphone, allowing it to secretly record conversations and take pictures or videos. Pegasus is intended to be persistent on iOS devices, which enables it to stay put even after a device reset.

## Pegasus On Android

Pegasus can attack Android devices through a number of techniques, such as spear-phishing emails and malicious apps. Once installed on device, Pegasus can access the device's data and features by taking advantage of flaws in the Android operating system and other installed application. As an example, it can record screenshots of the device's display and keep track of keystroke. It can also use the device's camera and microphone to take pictures and videos and record audio. Pegasus is made to be difficult to find and uninstall on Android devices by being persistent.

# *Suspected regions of infection*

Hungary: Pegasus allegedly used to target a variety of Hungarian journalists, opposition lawmakers, and public figures in 2020. Sending text messages with links to a malicious website that, when clicked, would download the Pegasus spyware onto the target's device was how the assault was carried out.

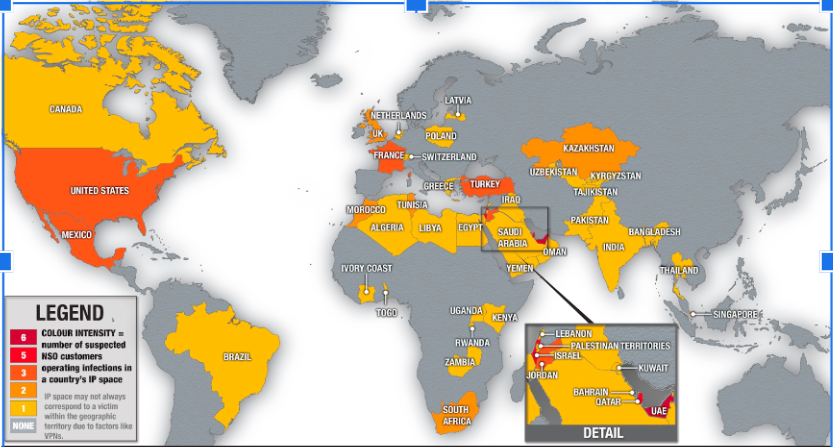


Fig 2. Suspected region of Pegasus

Mexico: Pegasus was used to target a number of Mexican journalists, human rights advocates, and anti-corruption campaigners, according to a Citizen Lab investigation from 2016. The Pegasus malware was installed on the victim's devices when they clicked on links that were sent to them through text message.

India: Pegasus was allegedly used to attack a variety of Indian journalists, human rights defenders, and opposition politicians in 2019. The assault involves sending WhatsApp messages with malicious URLs that, if clicked, would download Pegasus onto the target's device.

Saudi Arabia: Pegasus was reportedly used in 2018 to target activists and dissidents in Saudi Arabia, including the journalist Jamal Khashoggi. The attack involved sending Khashoggi's phone a text message with a link to a website that would download the Pegasus malware.

United Arab Emirates: Pegasus was allegedly used to target human rights activists in the United Arab Emirates in 2016. The assault entailed sending text messages with links to a malicious website, which, if clicked, would download the Pegasus malware onto the target's smartphone.

# Background Research and Analysis

## Spyware

Spyware is software that installs Itself on a victim’s computer and started observing the computer’s accessible application. This malware collects the data from the device and sends them to the mediator in the absence of the owner’s notice. It uses device data for business purposes. It first Penetrates into the device through a malicious website or file extension then it observes and record device data its send the recorded data to the mediator. The antivirus software program makes use of spotting and deletion of spyware software that has been so far installed on the device.

## Zero-click Attack

It is a cyberattack where a system can be compromised without any voluntary action of the user. The zero-click attack doesn't require social engineering, bad links or phishing rather it exploits the existing vulnerabilities of the operating system. Hence making a no click malware much more difficult to identify.

Any software that parses the data/information it receives to check its authenticity is vulnerable to zero-click attacks.The reduced interaction in no click or zero click attacks means there are fewer ways of determining the traces of the malicious deed.

Often, Cyber criminals  attacks target apps that provide messaging or voice calling since these services are designed to receive and interpret data from unknown sources. Attackers usually tend to use the specially formed data like a  hidden text message or an  image file, to inject the code that puts the device at risk.

NSO is an Israel based group of  hackers that have been operating for many years. They provide software like Pegasus to many different countries and has claimed their software was an asset in the capture of El Chapo. A Toronto based lab announced the discovery of a zero-click attack where the  hackers had installed Pegasus malware on victim's devices including all the apple devices,using a malicious PDF that automatically executes code rendering the infected devices as listening spyware. Apple has since developed a patch for this vulnerability through iOS 14.8 for iPhones and iPads, and watchOS 7.6.2 for the Apple Watch Series 3, and above.

*Zero-Day Exploit*

Zero-Day exploits are used to attack systems that have zero-day vulnerabilities. These are vulnerabilities that are have either not been detected or they have been detected but the developers don’t have a patch ready for it yet. It is basically a flaw in in the system. Generally when someone like a bug bounty hunter detects a vulnerability in a system they report it to the developer and if given enough time the developers will release a a patch for it before hackers have time to develop an exploit. This is not the case when it comes zero-day vulnerabilities. These type of exploits are also burdensome to detect as these type of attacks don’t generally have a particular attack signature developed yet.

## Megladron

Trojan malware deceives the user of its true purpose. Megladon is a very sophisticated trojan that acts like a Remote Access Tool and a key-logger.  This trojan usually uses email phishing campaigns to trick the end-users. It implements phishing by sending a large number of emails stimulating the end-user to open the files that are attached (they are mostly Excel documents).  Mostly the attachments will be disguised as accounts or finance related documents. It infiltrates the target system by first copying its set of files to the target systems hard disk. After this it creates a startup key with some filename (random).exe.

# ***analysis by Lenovo***

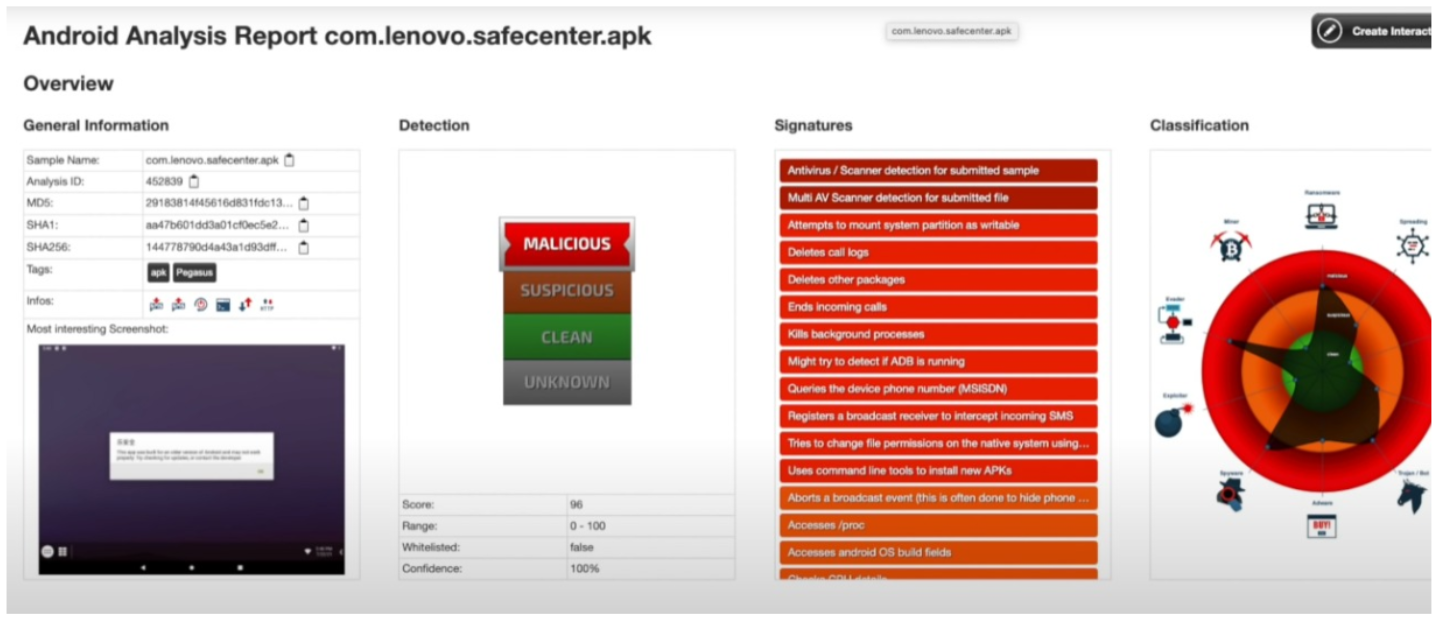


Fig 3: Analysis report by Lenovo

The analysis ID given by Lenovo for the same is “452839”. Lenovo categorises the vulnerabilities by the tags “CLEAN”, “SUSPICIOUS” and “MALICIOUS”. For the Pegasus spyware, it was categorized as “MALICIOUS”. They gave it a score of 96 with a confidence of 100%. From the analysis provided above, we can conclude that Pegasus got one of the highest scores on the basis of its risk to Lenovo devices. The second takeaway from the analysis is the fact that pegasus was spread in the form of APK files for Lenovo devices.

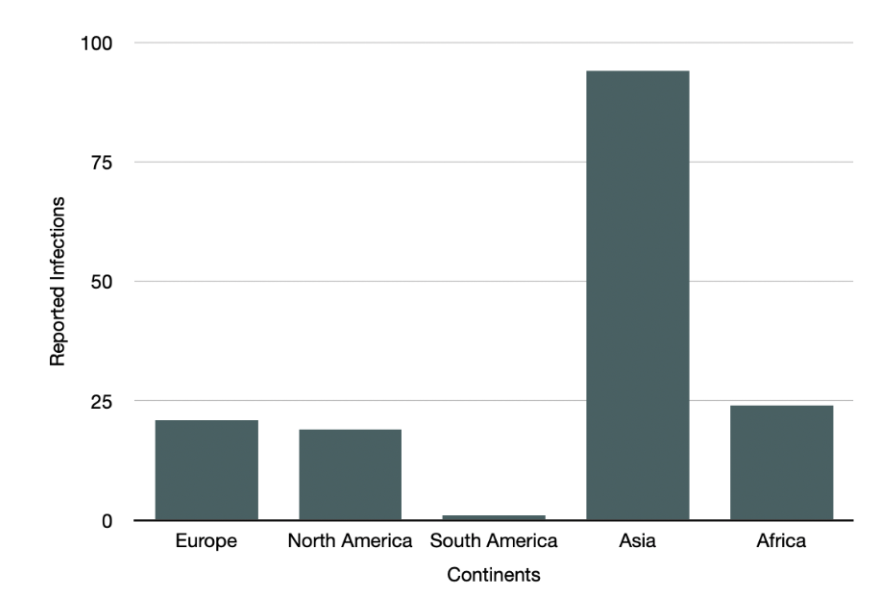


Fig 4: Continent-wise Reported Infections

*versions of Pegasus:*

Pegasus has been operational for well over 8 years but the first version were only identified by 2016. In the initial versions of the spyware the targets had to click on a link that was propagated to them through one of the messaging platforms.

In August 2016, NSO Group has created a specific version of the Pegasus spyware specifically for the US Government which had 1-click ability for all types of mobile phones except Blackberry phones which could be exploited with a zero click attack.

By 2019, Pegasus had taken advantage of a vulnerability in WhatsApp where the operators only had to call the target phone using WhatsApp call and even if the phone wasn’t answered by the target, the spyware would exploit the targets mobile phone.

Since 2019, Pegasus started to exploit iPhones by depending on a vulnerability in iMessage to exploit target systems.

By 2020, NSO group has made the spyware switch towards zero-click attacks. These were very efficient as it required no interaction from the target and the operator could easily gain control of the target system. In terms of forensic evidence, it left no detectable signatures.

# *CONCLUSION*

In conclusion, Spyware are software that can steal information on a hacked computer and send the data back to the hacker. Pegasus spyware was a popular spyware as it was zero click in operation and required as little as a phone number to penetrate a system. The forms in which it was transmitted range of android apps, ios applications or even emails. The exact damage caused by this software is still not known.

##### References

1. Mayank Agrawal, Gagan Varshney, Saumya, Kaushal Pratap Singh, Manish Verma.“Pegasus: Zero-Click spyware attack - its countermeasures and challenges”

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

1. Pegasus Snoopgate – 2021: Right to Privacy and State intrusion

https://www.juscorpus.com/wp-content/uploads/2021/10/69.-Naman-Tarun-Khulbe.pdf

1. Pegasus: The New Global Weapon for Silencing Journalists, Forbidden Stories, 2021 https://forbiddenstories.org/pegasus-the-new-globalweapon-for-silencing-journalists
2. Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries, The Citizen Lab, University of Toronto, 2018 https://citizenlab.ca/2018/09/hide-and-seek-tracking-nsogroups-pegasus-spyware-to-operations-in-45-cou
3. Forensic Methodology Report: How to catch NSO Group’s Pegasus, Amnesty International, 2021 https://www.amnesty.org/en/latest/research/2021/07/forensicmethodology-report-how-to-catch-nso-groups-pegasus/
4. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. <https://tspace.library.utoronto.ca/handle/1807/102557>

7. Pegasus Spyware – 'A Privacy Killer' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=389065>

8. V. J. Raymond and R. J. R. Raj, "Android malware detection and build model using support vector machine,"

<https://ieeexplore.ieee.org/author/37086246971>

1. JDetection and elimination of spyware and ransomware by intercepting kernel-level system routines by avaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018).             https://doi.org/10.1109/access.2018.2884964
2. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware <https://tspace.library.utoronto.ca/handle/1807/102557>
3. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
4. How does the Pegasus spyware work, and is my phone at risk?   https://ro.ecu.edu.au/ecuworkspost2013/10942/
5. Protect Yourself from Powerful Pegasus Spyware, Hank Schless, Lookout, 2021 https://blog.lookout.com/protect-against-pegasusspyware

Here’s how to check your phone for Pegasus using Amnesty’s tool, Mitchell Clark, The Verge, 2021. https://www.theverge.com/2021/7/21/22587234/amnestyinternational-nso-pegasus-spyware-detection-tool-ios-androidguide- windows-mac

1. Pegasus Spyware – 'A Privacy Killer' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=389065>
2. V. J. Raymond and R. J. R. Raj, "Android malware detection and build model using support vector machine,"

<https://ieeexplore.ieee.org/author/37086246971>

1. JDetection and elimination of spyware and ransomware by intercepting kernel-level system routines by avaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018).             https://doi.org/10.1109/access.2018.2884964

1. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware <https://tspace.library.utoronto.ca/handle/1807/102557>
2. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
3. How does the Pegasus spyware work, and is my phone at risk?   https://ro.ecu.edu.au/ecuworkspost2013/10942/
4. Protect Yourself from Powerful Pegasus Spyware, Hank Schless, Lookout, 2021 https://blog.lookout.com/protect-against-pegasusspyware
5. Here’s how to check your phone for Pegasus using Amnesty’s tool, Mitchell Clark, The Verge, 2021. https://www.theverge.com/2021/7/21/22587234/amnestyinternational-nso-pegasus-spyware-detection-tool-ios-androidguide- windows-mac