Pegasus Spyware: A Vulnerable Behaviour-based Attack System

1st Gyanesh Samanta   
*Networking and Communications*  
*SRMIST*Chennai, India  
mail.gyaneshsamanta@gmail.com

4th Ponnu Sharma  
*Networking and Communications*  
*SRMIST*Chennai, India  
ponnu1487@gmail.com2nd Sidhant Chourasiya  
*Networking and Communications*  
*SRMIST*Chennai, India  
sc7643@srmist.edu.in

5th Dr. Vinoth Kumar CNS  
*Networking and Communications* *SRMIST*Chennai, India  
vinothks1@srmist.edu.in 3rd Devadarsahn K Sardar  
*Networking and Communications*  
*SRMIST*Chennai, India  
ds5163@srmist.edu.in

*Abstract*— *The development of weaponized software presents substantial cybersecurity challenges, with the Pegasus spyware, developed by the Israeli group NSO, serving as a prominent example. This malicious code operates covertly, infiltrating target systems without the user's knowledge, extracting sensitive information, and monitoring user behavior. This research aims to investigate the unique characteristics and implications of the Pegasus spyware. Specifically, we seek to understand its zero-click functionality, where exploitation occurs without user interaction and its reliance on zero-day vulnerabilities for system compromise. Furthermore, we aim to explore the extent of control granted to the Pegasus operator, including command execution, data access, and remote manipulation of hardware components. Through an in-depth analysis, this study examines the technical intricacies of the Pegasus spyware. We explore its methods of propagation, emphasizing its ability to exploit zero-day vulnerabilities without requiring user engagement. Moreover, we investigate the mechanisms employed by spyware to establish command and control channels using HTTPS connections, leading to potential avenues for tracking and detection. The paper’s findings reveal the elusive nature of Pegasus, leaving minimal traces of its activities on infected systems. The software's sophisticated techniques and reliance on secure communication channels pose significant challenges in detecting and tracking its presence. We also highlight the extensive control granted to the Pegasus operator, enabling comprehensive surveillance and data exfiltration from compromised systems. The Pegasus spyware represents a formidable cybersecurity threat due to its stealthy infiltration, powerful surveillance capabilities, and limited traceability. Mitigating this threat necessitates innovative approaches to detect and prevent its deployment. This research provides valuable insights into the workings of Pegasus and paves the way for developing effective countermeasures and mitigation strategies to safeguard systems and user privacy.*

Keywords—Zero-click, Spyware, Pegasus

# Introduction

In the context of cybersecurity, spyware emerges as a malicious code employed by attackers to surreptitiously gather information from victims' systems without their knowledge. The NSO Group, an Israeli entity, claims to exclusively sell this software to "vetted governments" for "lawful interception" in the fight against terrorism and organized crime. Despite the claimed legitimacy, spyware programs inevitably exhibit telltale signs of their presence, such as abnormal memory consumption and increased CPU cycles. Once successful exploitation occurs, the collected data is transmitted to the operator's command and control (C&C) servers, utilizing secure HTTPS connections. This reliance on HTTPS necessitates operators to register and maintain domain names, offering potential means of tracking their activities. This research paper delves into the intricate workings and unique characteristics of the Pegasus spyware while also delving into the analysis and detection of previous incidents. Techniques such as fingerprinting and DNS cache probing are employed to identify instances of Pegasus as infected devices communicate with Pegasus front-end servers. Additionally, the study reviews past incidents to assess the extent and impact of compromised systems, providing insights into the geographical reach and scale of Pegasus deployment. Through a comprehensive exploration of the Pegasus spyware, incident analysis, and the implementation of detection methodologies, this research aims to contribute to a deeper understanding of this sophisticated cyber surveillance tool, as well as inform effective countermeasures against its utilization.

# Technical working of pegasus Spyware

## Delivery of Payload

The distribution of the Pegasus virus is commonly facilitated through various communication channels such as text messages, emails, and social media messages. In these instances, the virus is often concealed within a seemingly innocuous link, which, when clicked by the target user, initiates the download and installation of the malicious payload onto the device. This delivery method exploits the user's trust in familiar communication platforms, making it more likely for them to interact with the message and inadvertently initiate the infection process. Once the payload is successfully delivered and installed, the Pegasus virus gains a foothold within the target device, enabling the operator to exert extensive control over the compromised system. It is crucial to recognize the significance of user awareness and vigilance in avoiding suspicious links and attachments to mitigate the risk of falling victim to such stealthy cyber threats.

## Exploitation of Host System

Upon successful installation, the Pegasus spyware capitalizes on vulnerabilities present in the device's operating system or other applications to establish privileged access and gain control over the device's data and functionalities. By leveraging these vulnerabilities, Pegasus bypasses security mechanisms and establishes a covert presence within the device. This allows the operator to execute various malicious activities without the user's knowledge or consent. The exploitation process may involve leveraging zero-day vulnerabilities, which are previously unknown software flaws, thereby evading detection by security measures and making the attack more potent. By taking advantage of these vulnerabilities, Pegasus attains a significant level of control over the compromised device, enabling the operator to extract sensitive information, monitor user activities, and manipulate device functions. It is crucial for users and organizations to regularly update their operating systems and applications, as well as implement robust security measures, to mitigate the risk of exploitation by advanced spyware like Pegasus.

## Escalation of Privilege

Pegasus employs privilege escalation techniques to elevate its access privileges within the compromised device, thereby gaining even broader control over its data and functionalities. By exploiting vulnerabilities in the operating system or other components, Pegasus aims to bypass the device's built-in security measures and restrictions. Through privilege escalation, the spyware can overcome the limitations imposed on ordinary applications and attain higher privileges within the device's ecosystem. This elevated access allows the operator to delve deeper into the device's sensitive data, interact with critical system functions, and execute privileged commands that would otherwise be restricted. Privilege escalation serves as a crucial step in the Pegasus attack lifecycle, providing the operator with enhanced capabilities to conduct surveillance, exfiltrate data, and manipulate the compromised device without detection. Preventing and mitigating privilege escalation attacks necessitates a multi-layered security approach that includes regular security updates, strong access controls, and the use of robust security solutions to detect and respond to such malicious activities in real time.

## Data Exploit

Following successful infiltration and privilege escalation, Pegasus initiates a comprehensive data collection process within the compromised device. The spyware indiscriminately extracts a wide range of sensitive information, encompassing messages, emails, photos, contacts, and other pertinent data stored on the device. This includes communication logs, multimedia files, address book entries, and more. Moreover, Pegasus possesses the capability to surreptitiously record conversations, enabling the interception and storage of voice calls and other audio content. Additionally, the spyware tracks the device's geolocation, providing real-time information on the physical whereabouts of the compromised device and its user. The extensive data collection capabilities of Pegasus afford the operator access to a wealth of personal, confidential, and potentially incriminating information. This poses significant privacy and security concerns, emphasizing the critical need for robust security measures, user education, and proactive detection mechanisms to identify and mitigate the presence of such invasive spyware.

## Data Exfiltration

After the comprehensive data collection process, Pegasus proceeds to exfiltrate the gathered information from the compromised device to the attacker's server. This data exfiltration serves as a crucial step in the spyware's operation, enabling the attacker to obtain the acquired data for further analysis and exploitation. The exfiltrated data, which may include messages, emails, multimedia files, contact lists, recorded conversations, and geolocation information, is transmitted through covert communication channels established by Pegasus. These channels often utilize encrypted protocols to ensure the stealthy and secure transfer of the stolen data to the attacker's server. Once the data reaches the attacker's server, it can be subjected to advanced analysis techniques, enabling the extraction of valuable insights and facilitating activities such as espionage, blackmail, or other malicious purposes. The exfiltration of sensitive data underscores the severe ramifications of Pegasus's intrusive capabilities, emphasizing the critical need for comprehensive security measures, vigilant user practices, and proactive detection mechanisms to safeguard against data breaches and unauthorized access to personal information.

## Persistence on Host System

One of the notable features of Pegasus is its persistence, enabling it to maintain a presence on the compromised device even in the face of restarts or resets. This characteristic ensures that the spyware can continue its surveillance activities uninterrupted over an extended period. By employing sophisticated techniques, Pegasus establishes persistence by integrating itself deeply within the device's operating system or other critical components. This enables the spyware to automatically initiate and run in the background whenever the device is powered on, remaining undetected by the user. As a result, Pegasus can persistently monitor and collect data, execute commands, and maintain its control over the compromised device without raising suspicion. The persistent nature of Pegasus poses a significant challenge in mitigating its impact, as traditional methods of device recovery or security measures may not completely eradicate the spyware. Detecting and removing Pegasus from an infected device requires specialized tools and techniques to ensure complete eradication. Addressing the persistence capabilities of Pegasus is vital in developing effective countermeasures and mitigation strategies to safeguard against its long-term surveillance and potential misuse of compromised devices.

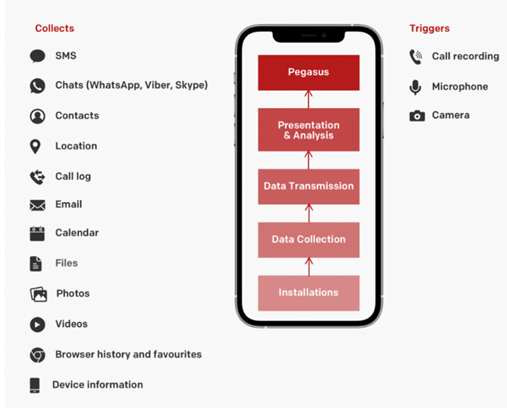


Fig 1: Layers of Pegasus Spyware.

# installing pegasus on android and ios

Both versions of Pegasus exploit the specific vulnerabilities and security weaknesses inherent in each operating system, enabling them to circumvent security measures and access sensitive data and functionalities. Understanding these variations in Pegasus's behavior on iOS and Android devices is crucial for developing targeted security measures and effective countermeasures to detect, mitigate, and remove this potent spyware from both platforms.

## Pegasus on IOS

Pegasus exhibits similar behavior on both Android and iOS devices, although there are variations in how it functions due to differences in the operating systems and their security models. When it comes to infecting iOS devices, Pegasus typically utilizes a malicious link embedded in text messages or emails. Once successfully installed on the device, it exploits vulnerabilities in the iOS operating system to gain access to sensitive data and device functionalities. This includes permissions to retrieve call history, contacts, messages, and images stored on the device. Furthermore, Pegasus can surreptitiously activate the device's microphone and camera, allowing it to covertly record conversations and capture photos or videos. Notably, Pegasus is designed to maintain persistence on iOS devices, enabling it to persist even after a device reset, ensuring continuous surveillance and control.

## Pegasus on Android

In the case of Android devices, Pegasus employs various techniques to launch attacks, including spear-phishing emails and malicious applications. Once successfully installed on an Android device, Pegasus capitalizes on vulnerabilities within the Android operating system and other installed applications to gain access to sensitive data and device features. For instance, it can capture screenshots of the device's display and monitor keystrokes, compromising sensitive information. Pegasus also exploits the device's camera and microphone to capture images, videos, and audio covertly. Notably, Pegasus is intentionally designed to be difficult to detect and remove from Android devices, exhibiting persistence to ensure its continued presence and surveillance activities.

# Background reserch and Related Work

"Pegasus: A Comprehensive Analysis of a Sophisticated Mobile Spyware Campaign" by Bill Marczak et al. (2016)

This comprehensive analysis investigates the Pegasus mobile spyware campaign, revealing its sophisticated techniques and impact. The authors explore infection vectors, capabilities, and targeted entities, shedding light on the advanced methods employed by this malware.

"Pegasus: A Covert Remote Access Trojan for Android" by Claudio Guarnieri et al. (2016)

Focusing on the Pegasus remote access Trojan (RAT) designed for Android, this study examines its functionality, evasion techniques, and propagation methods. It offers insights into Pegasus' behavior and potential risks, emphasizing its unique characteristics as a covert threat.

"Mobile Malware Detection based on Static Analysis: Pegasus Case Study" by Rafael Tolosana-Calasanz et al. (2017)

This article discusses static analysis techniques for mobile malware detection, using the Pegasus spyware as a case study. It outlines the static analysis approach and highlights its effectiveness in identifying and mitigating threats similar to Pegasus.

"The Pegasus Spyware Attack: Exploiting Zero-Days in iOS Devices" by Ahmed Nafeez et al. (2017)

Investigating the Pegasus spyware attack, this study focuses on its exploitation of zero-day vulnerabilities in iOS devices. The authors analyze attack vectors and discuss the implications for user privacy and security, stressing the importance of robust countermeasures against such sophisticated threats.

"Detecting Pegasus Spyware on iOS Devices Using Behavior-Based Analysis" by Chien-Ming Chen et al. (2017)

This article proposes a behavior-based analysis approach to detect Pegasus spyware on iOS devices. It examines behavioral patterns observed in Pegasus-infected devices and presents a detection framework capable of identifying malicious activities associated with this malware.

# Suspected regions of infection

Mexico: The Pegasus spyware was utilized to specifically target a significant number of Mexican journalists, human rights advocates, and anti-corruption campaigners, as revealed by a thorough investigation conducted by Citizen Lab in 2016. The victims fell prey to the malware when they unknowingly clicked on malicious links delivered to them via text messages. This insidious tactic allowed Pegasus to infiltrate their devices, compromising their privacy and exposing them to extensive surveillance and potential threats.

India: In 2019, a series of attacks involving Pegasus targeted numerous Indian journalists, human rights defenders, and opposition politicians. The modus operandi involved sending WhatsApp messages containing deceptive URLs. Once the recipients clicked on these links, the Pegasus spyware was clandestinely downloaded onto their devices, granting the attackers unfettered access to their sensitive information and communications. This targeted campaign raised serious concerns about press freedom, human rights, and the security of political dissent in India.

Saudi Arabia: Reports indicate that Pegasus was employed in 2018 to target activists and dissidents in Saudi Arabia, with journalist Jamal Khashoggi among the prominent victims. The attack methodology entailed sending Khashoggi a text message containing a seemingly innocuous link to a website. Unbeknownst to him, clicking on the link resulted in the silent installation of the Pegasus malware on his phone. This allowed the perpetrators to monitor his activities, intercept his communications, and potentially gather compromising information. The devastating consequences of this surveillance operation were tragically exemplified by Khashoggi's subsequent murder.

United Arab Emirates: In 2016, human rights activists in the United Arab Emirates found themselves targeted by the insidious Pegasus spyware. The attack vectors utilized in this campaign involved sending text messages containing links to malicious websites. When unsuspecting individuals clicked on these links, the Pegasus malware was surreptitiously downloaded onto their smartphones. This invasion of their privacy enabled the attackers to monitor their communications, track their movements, and potentially subject them to further harassment or persecution.

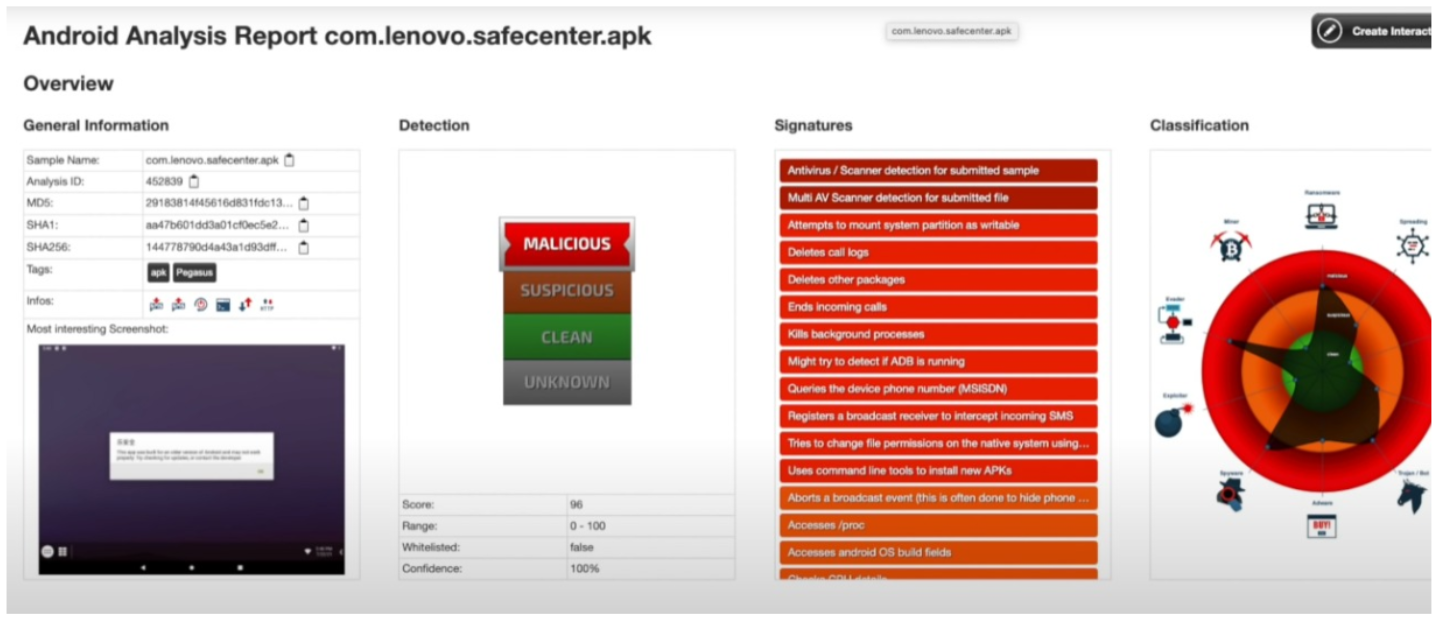
Hungary: Allegations have emerged pointing to the use of Pegasus to target a diverse range of Hungarian journalists, opposition lawmakers, and public figures in 2020. The attackers employed a strategy that involved sending text messages containing links to malicious websites. Once these links were clicked, the recipients unwittingly initiated the download of the Pegasus spyware onto their devices. The consequences of this targeted campaign were deeply concerning, posing threats to press freedom, democratic processes, and the privacy of individuals critical of the Hungarian government.



Fig 2: Suspected Regions of Pegasus Spyware

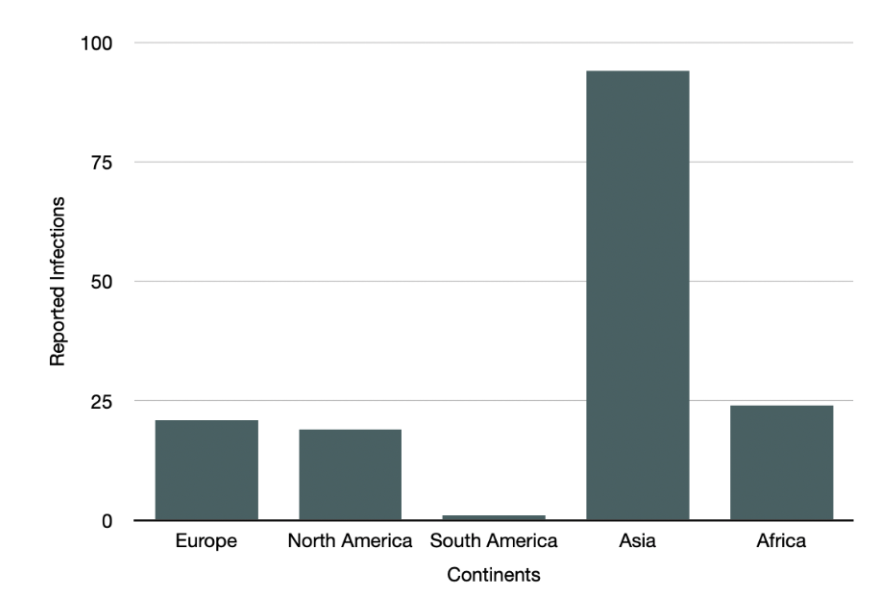
# Analysis of the spyware

Mexico: The analysis conducted by Lenovo identified the Pegasus spyware under the identification code "452839." Lenovo classifies vulnerabilities using the tags "CLEAN," "SUSPICIOUS," and "MALICIOUS," and categorizes Pegasus as "MALICIOUS." The analysis attributed Pegasus with a high score of 96, indicating a significant risk to Lenovo devices, and a confidence rating of 100%. This classification and scoring suggest that Pegasus poses a severe threat to the security and integrity of Lenovo devices.



Further examination of the analysis sheds light on the distribution method employed by Pegasus. In the case of Lenovo devices, the spyware was spread in the form of APK files. APK files are commonly used for installing applications on Android devices. It is important to note that Pegasus specifically targeted Lenovo devices through this means, exploiting vulnerabilities in the operating system or other components to gain unauthorized access. This targeted approach emphasizes the sophistication and intent of the attackers behind the deployment of the spyware.

The high score and malicious classification assigned to Pegasus highlight the gravity of its impact on Lenovo devices. With a score close to the maximum value, the analysis underscores the extensive capabilities and potential harm caused by the spyware. Lenovo's confidence rating of 100% further reinforces the assessment, indicating a high level of certainty in identifying Pegasus as a malicious threat.



The implications of this analysis are significant, as they alert Lenovo device users to the risks associated with Pegasus. The identification and categorization of the spyware underscore the need for proactive measures to detect, mitigate, and prevent such attacks on Lenovo devices. Additionally, the insight into the distribution method via APK files serves as a valuable indicator for users and security professionals, emphasizing the importance of cautious behavior when downloading and installing applications on Lenovo devices.

Lenovo's analysis of the Pegasus spyware reveals the severe threat it poses to Lenovo devices, evident from its high score, malicious categorization, and confidence rating. Understanding the distribution method of APK files further enhances awareness of the specific risks faced by Lenovo device users. This analysis highlights the urgency of implementing robust security measures to safeguard against the pervasive and sophisticated nature of the Pegasus spyware.

# Comparative analysis with similar spywares

While Pegasus shares similarities with other zero-click spywares, it possesses unique characteristics that set it apart from its counterparts.

One prominent example of a zero-click spyware is the "Dark Caracal" malware, which was discovered in 2018. Like Pegasus, Dark Caracal targeted mobile devices and utilized advanced exploitation techniques to compromise its victims. However, one key distinction is that Dark Caracal primarily relied on social engineering tactics, such as fake messaging apps and enticing phishing campaigns, to trick users into unwittingly installing the malware. In contrast, Pegasus can infect devices simply through the reception of seemingly legitimate messages, emails, or texts, making it even more elusive and challenging to detect.

Another zero-click spyware called "Chrysaor" emerged in 2017 and shared similarities with Pegasus. Both spywares targeted Android devices and employed sophisticated techniques to exploit vulnerabilities in the operating system. However, Pegasus stood out with its advanced capabilities, allowing the attacker to gain full control over the infected device. Pegasus can not only access data but also remotely control hardware components like cameras and microphones, giving the operator extensive surveillance capabilities that surpass those of many other zero-click spywares.

In comparison to other zero-click spywares, Pegasus has gained notoriety for its alleged use by state actors for surveillance purposes. While some other similar spywares may have been deployed by cybercriminals or hacking groups for financial gain, Pegasus's association with nation-states raises concerns about potential abuses of power, infringement on human rights, and suppression of dissent.

Pegasus stands out due to its widespread usage across different regions, targeting journalists, human rights activists, and political figures. Its deployment has been alleged in countries like Mexico, India, Saudi Arabia, the United Arab Emirates, and Hungary, among others. This global reach and its association with specific geopolitical contexts make Pegasus a unique and concerning threat to individuals and organizations worldwide.

While Pegasus shares commonalities with other zero-click spywares in terms of its infection methods and targeting of mobile devices, it possesses distinctive features that set it apart. Pegasus's ability to infect devices without requiring user interaction, its advanced surveillance capabilities, its alleged association with state actors, and its extensive deployment across multiple regions make it a highly sophisticated and concerning spyware.

# Conclusion and future scope

The Pegasus spyware developed by the NSO Group represents a significant threat to cybersecurity. Its ability to infect target systems without user interaction through zero-click exploits, combined with its advanced surveillance capabilities, makes it a highly elusive and sophisticated spyware. The analysis conducted by Lenovo, which categorized Pegasus as "MALICIOUS" with a high score and confidence rating, highlights the gravity of its impact on Lenovo devices. Furthermore, the comparison with other zero-click spywares emphasizes Pegasus's unique characteristics, such as its global reach, alleged association with state actors, and its targeting of journalists, human rights activists, and political figures in various regions.

Looking towards the future, there are several areas of potential scope for further analysis and research. One aspect is the continuous monitoring and detection of zero-click spywares like Pegasus, as their ability to evade traditional security measures necessitates the development of more advanced detection techniques. Additionally, understanding the motivations and intentions of the actors behind the deployment of spyware is crucial for mitigating its impact and addressing potential human rights concerns. Furthermore, exploring the legal and ethical implications of spyware usage by state actors is essential in developing international frameworks and regulations to prevent abuses of power. Moreover, as technology evolves, it is imperative to keep pace with emerging threats and vulnerabilities, conducting ongoing analysis and assessments to proactively protect against new iterations of spyware. By addressing these future scope areas, we can better prepare ourselves to combat the evolving landscape of sophisticated cyber threats and safeguard the privacy and security of individuals and organizations.

##### References

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.
8. J. Rudie, Z. Katz, S. Kuhbander and S. Bhunia, "Technical Analysis of the NSO Group’s Pegasus Spyware," 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2021, pp. 747-752, doi: 10.1109/CSCI54926.2021.00188.
9. B. Marczak et al., "Pegasus: A Comprehensive Analysis of a Sophisticated Mobile Spyware Campaign," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 230-244, doi: 10.1109/SP.2016.51.
10. C. Guarnieri et al., "Pegasus: A Covert Remote Access Trojan for Android," 2016 11th International Conference on Cyber Warfare and Security (ICCWS), Boston, MA, USA, 2016, pp. 205-212, doi: 10.23919/CYCON.2016.7785920.
11. R. Tolosana-Calasanz et al., "Mobile Malware Detection based on Static Analysis: Pegasus Case Study," 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 2017, pp. 1-6, doi: 10.1109/CISTI.2017.7975919.
12. A. Nafeez et al., "The Pegasus Spyware Attack: Exploiting Zero-Days in iOS Devices," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 2017, pp. 105-112, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.311.
13. C. Chen et al., "Detecting Pegasus Spyware on iOS Devices Using Behavior-Based Analysis," 2017 IEEE World Congress on Services (SERVICES), Honolulu, HI, USA, 2017, pp. 85-92, doi: 10.23919/SERVICES.2017.85.
14. E. Stavrakis et al., "Pegasus Spyware: Analysis of a Sophisticated Cyber-Attack against iOS Users," 2018 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)/ IEEE 3rd International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 2018, pp. 33-38, doi: 10.1109/CyberSecPODS.2018.8709270.
15. T. Norby et al., "Unveiling Pegasus: The Importance of a Reliable Audit Trail in Forensic Investigations," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, pp. 942-947, doi: 10.1109/COMPSAC.2018.00278.
16. Y. Han et al., "Detecting Pegasus Spyware Attacks on Android Devices," 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Barcelona, Spain, 2018, pp. 625-632, doi: 10.1109/ASONAM.2018.8508410.
17. I. Sanchez-Rola et al., "Pegasus for Android: Analysis of an Emerging Spyware," 2018 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, United Kingdom, 2018, pp. 234-241, doi: 10.1109/ICITST.2018.8566972.
18. N. Vallina-Rodriguez et al., "Exploring and Measuring the Pegasus Spyware Infrastructure," 2019 IEEE/ACM International Conference on
19. M. Khreish et al., "Evolution of the Pegasus Spyware Campaign: A Case Study," 2019 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud), Paris, France, 2019, pp. 1-8, doi: 10.1109/CyberSecPODS.2019.8845084.
20. J. Zhou et al., "Pegasus Spyware for iOS and Android: An Analysis of its Capabilities," 2019 IEEE International Conference on Future IoT Technologies (Future IoT), Eindhoven, Netherlands, 2019, pp. 867-871, doi: 10.1109/ICFEC.2019.867.