

FOURTH DIMENSION TECHNOLOGIES INC

Cyber Attacks 2024

Part - 4

fourdtech.com | info@fourdtech.com



Highlights

Key events we will be discussing:

New Malware Alert: SamsStealer on the Rise!

FakeBat Loader Malware Incident

Mailcow Flaw Incident

»» Pegasus Virus

Pegasus Virus

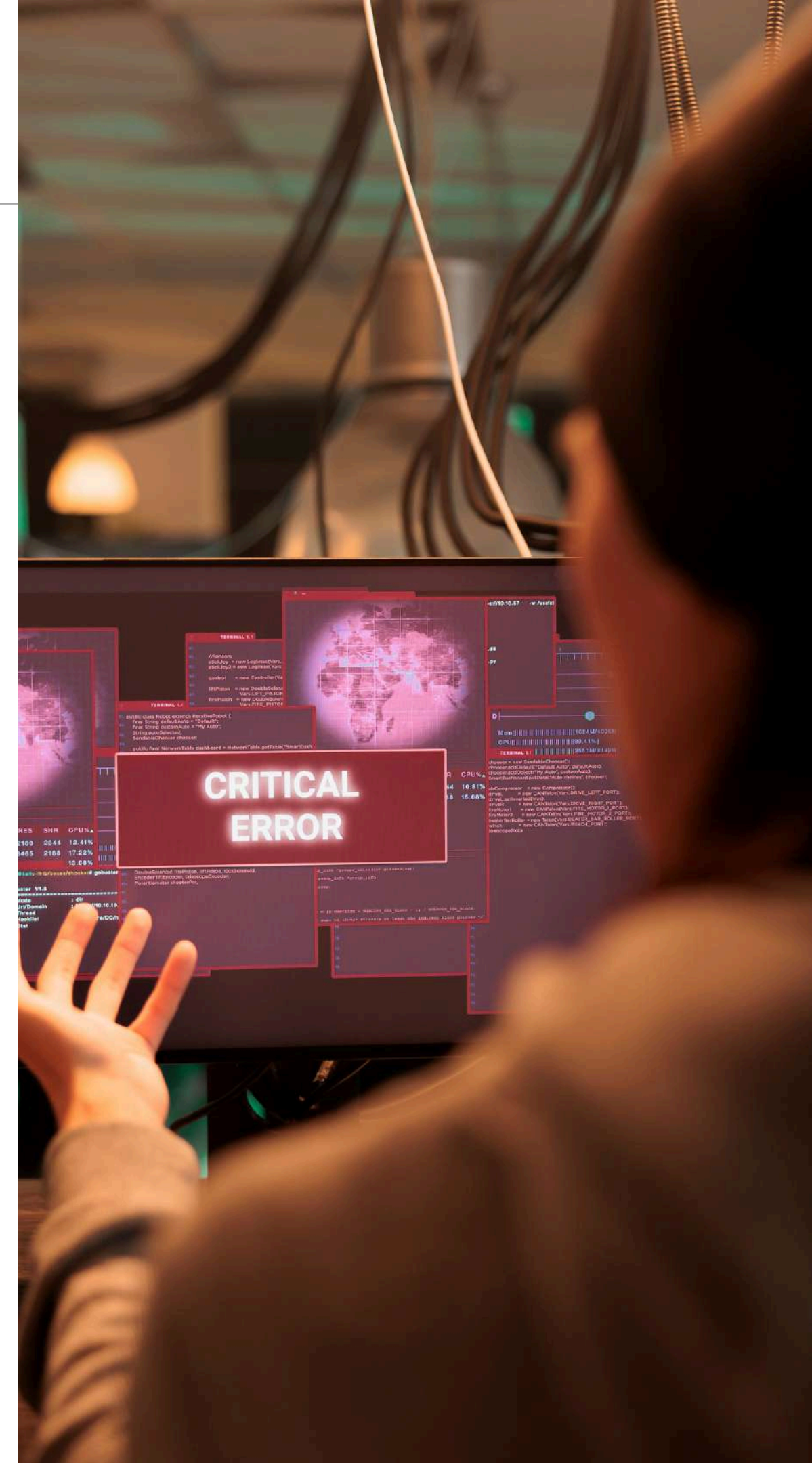
The Pegasus virus was developed in 2016 by the Israeli cybersecurity firm NSO Group. It is a sophisticated spyware designed to infiltrate smartphones and extract sensitive information. Pegasus has been used by various governments for the surveillance of activists, journalists, and political figures. This report explores the capabilities of Pegasus, its potential risks, and strategies to avoid detection and mitigate its impact.

Summary

Pegasus is a powerful spyware targeting iOS and Android devices by exploiting system vulnerabilities. Delivered through malicious links, SMS, and zero-click attacks, it can access nearly all data on an infected device, posing a significant threat to privacy and security. The following sections analyze Pegasus's functionalities, risks, and mitigation strategies.

Malware Overview:

Name	Pegasus
Type	Spyware/Malware
Target	iOS and Android Operating Systems
Distribution Method	Malicious links, SMS, and zero-click attacks.



ATT & CK IDS:

- T1071.001 – Application Layer Protocol: Web Protocols
- T1082 – System Information Discovery
- T1005 – Data from the Local System
- T1105 – Ingress Tool Transfer
- T1070.004 – Indicator Removal on Host: File Deletion
- T1113 – Screen Capture
- T1123 – Audio Capture
- T1056 – Input Capture
- T1059.003 – Command and Scripting Interpreter: Windows Command Shell

File Stealing Capabilities:

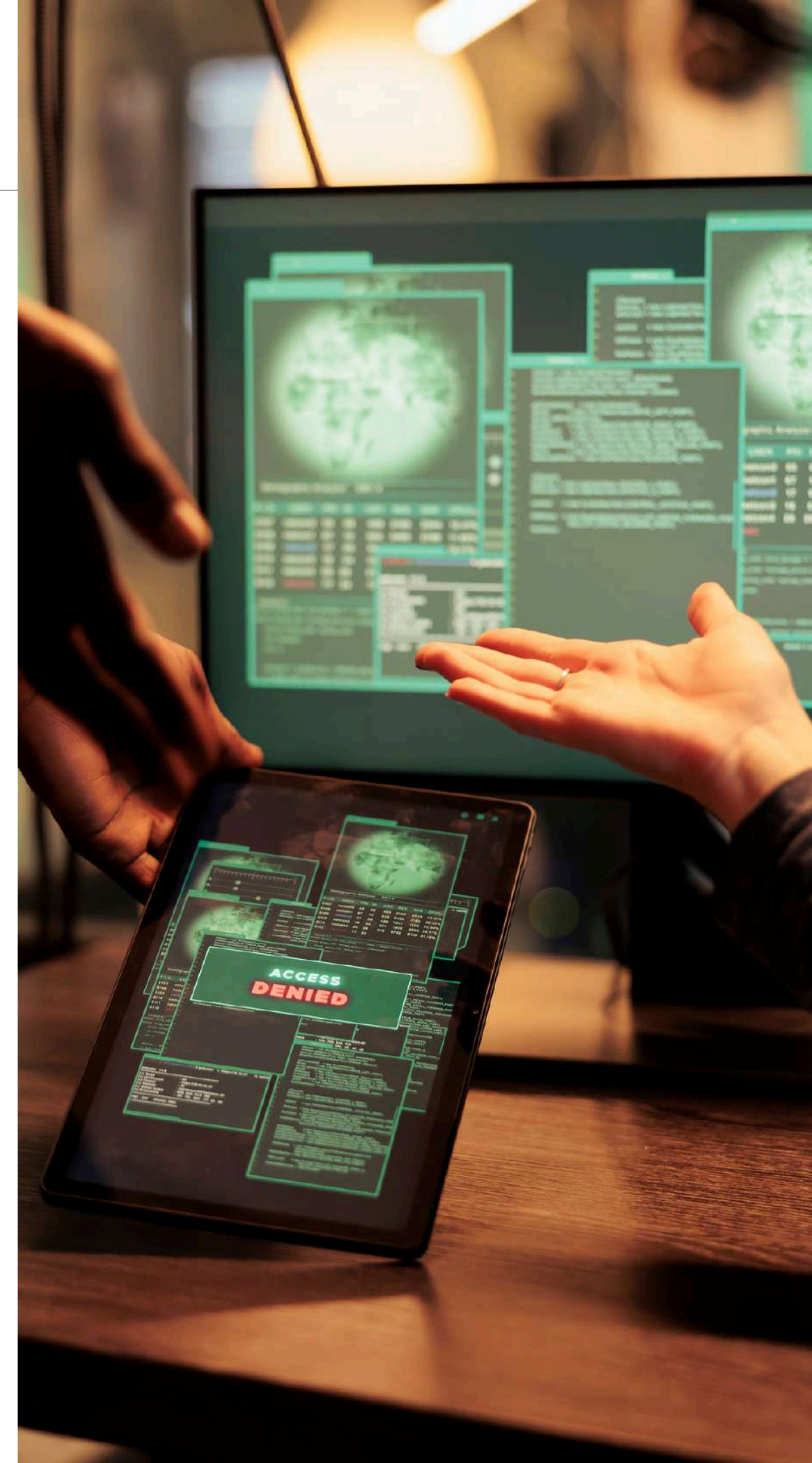
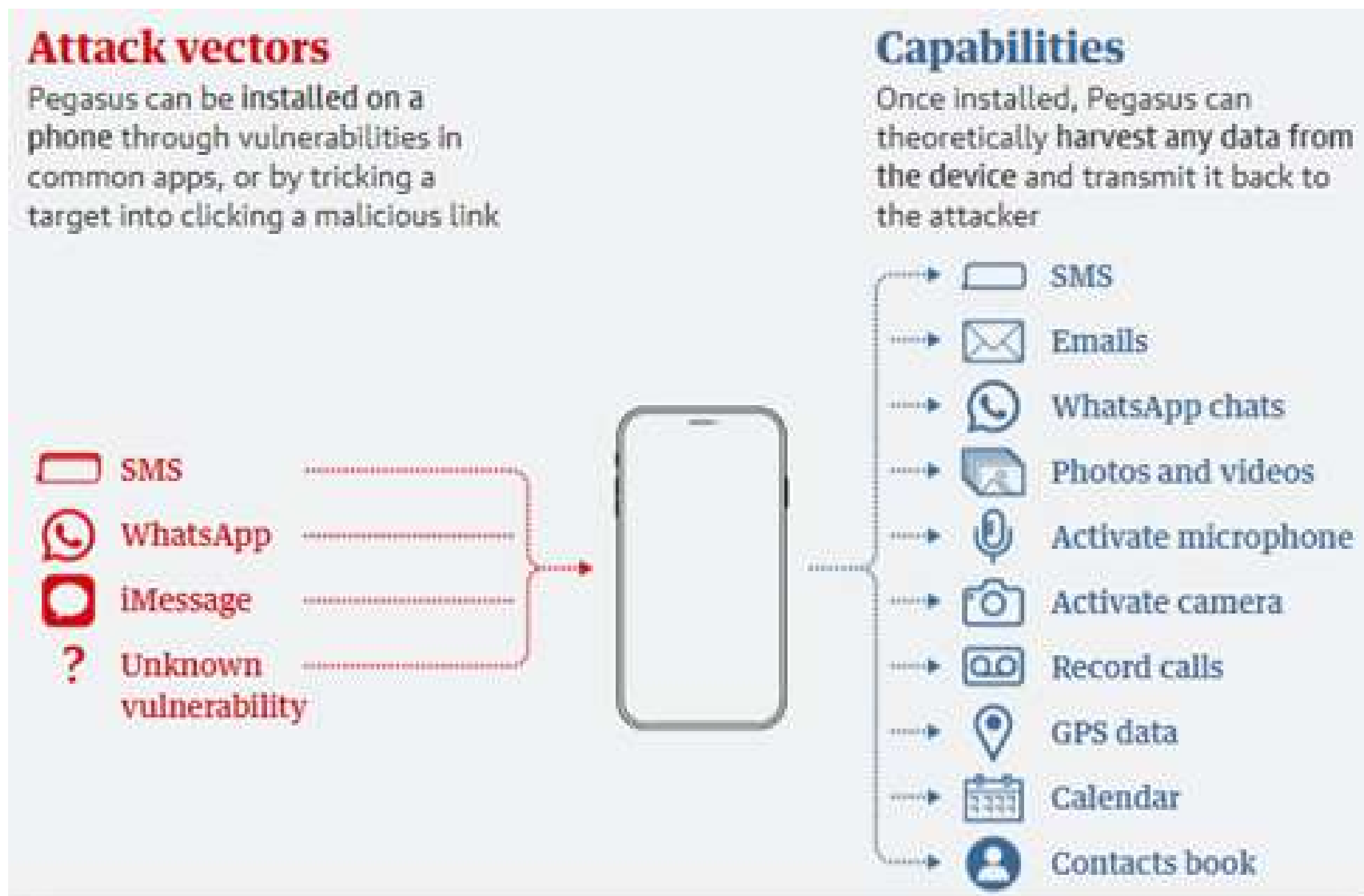
Access to Personal Files: Photos, Videos, Documents, and Other Personal Files.

Cloud Storage Access: Infiltrates cloud storage services linked to the device.

Communication Interception: Intercepts and exfiltrates data from messaging apps like WhatsApp, Signal, and iMessage, even if encrypted.

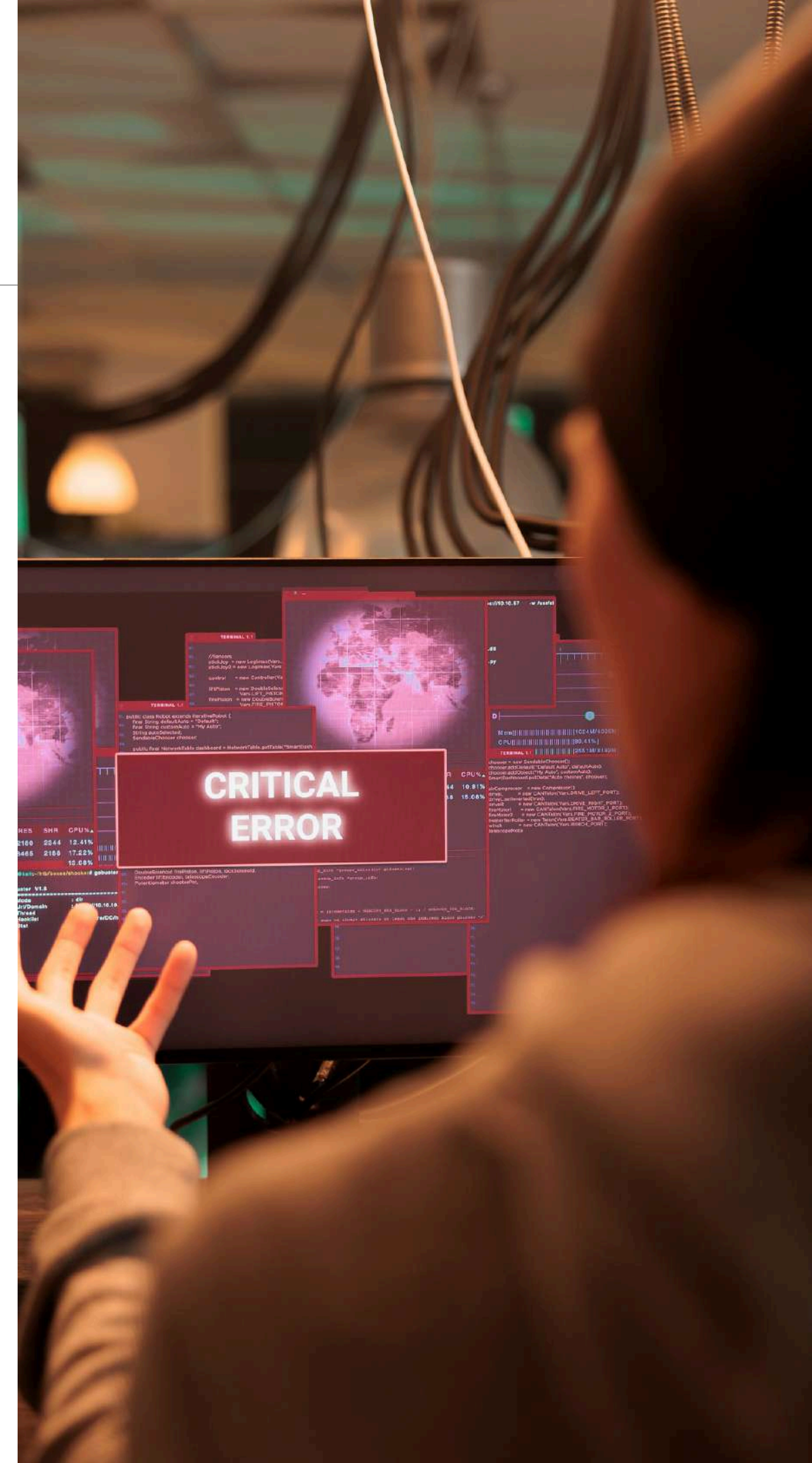


How Pegasus infiltrates a phone and what it can do:



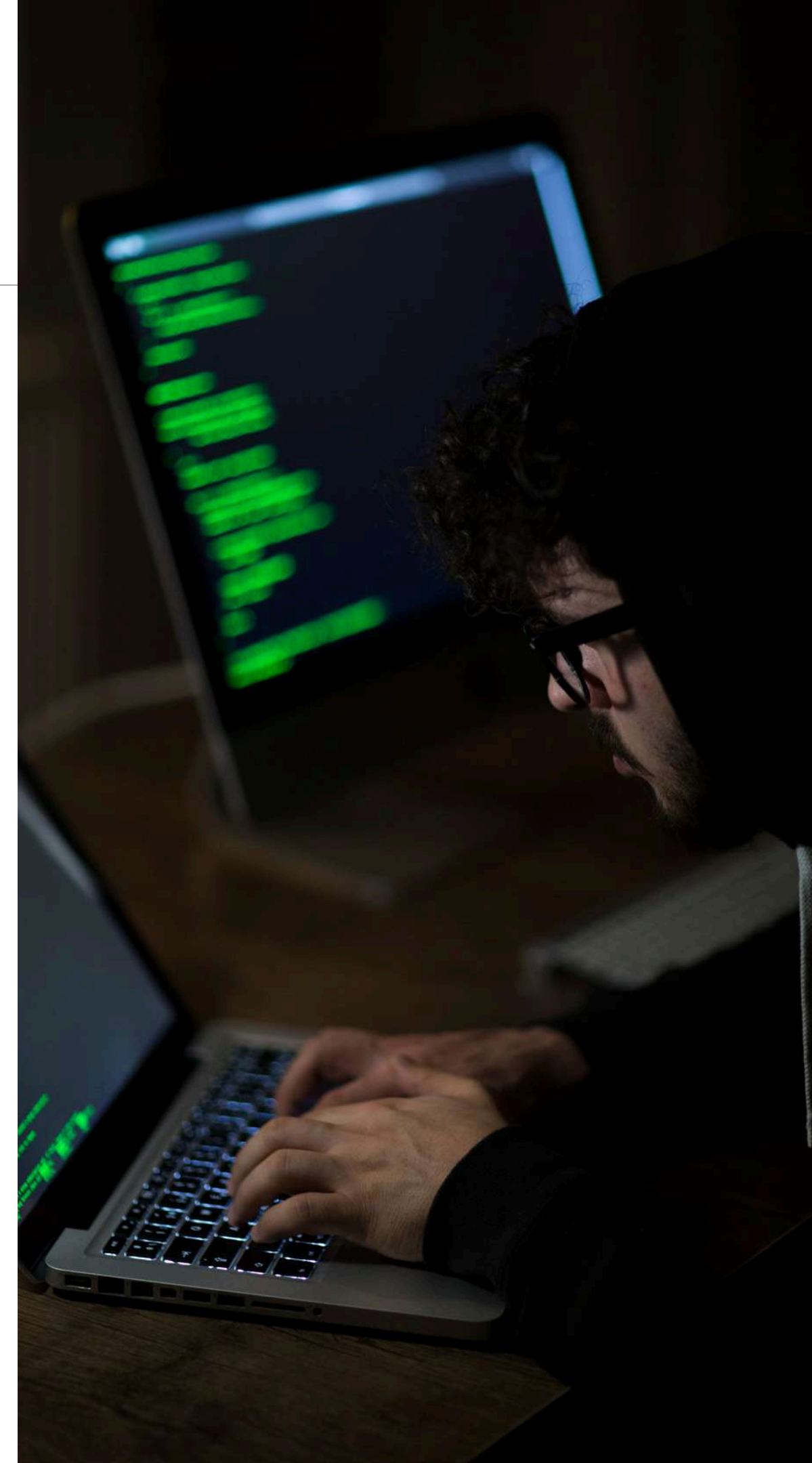
General Recommendations to Avoid Detection:

- 1. Regular Updates:** Ensure that your device's operating system and all installed applications are up to date to protect against known vulnerabilities.
- 2. Security Software:** Use reputable antivirus and anti-malware solutions to detect and prevent spyware infections.
- 3. Phishing Awareness:** Be cautious of unsolicited messages and avoid clicking on links from unknown sources.
- 4. App Permissions:** Regularly review app permissions and restrict access to sensitive data and functionalities.
- 5. Device Monitoring:** Use tools that monitor your device for unusual behavior, such as unexpected battery drain or data usage.



Potential Risks:

1. **Privacy Invasion:** Unauthorized access to personal information and communications.
2. **Identity Theft:** The potential for stolen personal information to be used for identity theft.
3. **Surveillance:** Government or third-party surveillance of individuals without consent.
4. **Data Breaches:** Compromise of sensitive corporate or governmental information.
5. **Legal and Ethical Implications:** Unauthorized spying can lead to legal consequences and ethical dilemmas.



Mitigation Strategies:

- 1. Implement Strong Security Policies:** Organizations should enforce robust security policies that include regular updates, security audits, and employee training.
- 2. Encryption:** Use end-to-end encryptions for all communications to protect data integrity and confidentiality.
- 3. Network Security:** Employ network security measures such as firewalls, intrusion detection systems, and VPNs to safeguard data transmissions.
- 4. Incident Response Plan:** Develop and maintain an incident response plan to quickly address and mitigate the effects of a Pegasus infection.
- 5. Public Awareness Campaigns:** Raise awareness about the risks of spyware and educate the public on how to protect their devices and data.

