Severity

High

Analysis Summary

Finland's Ministry of Foreign Affairs revealed that Pegasus Spyware has infected devices of many Finnish Diplomats.

"Finnish diplomats have been targets of cyber espionage by means of the Pegasus spyware, developed by NSO Group Technologies, which has received wide publicity. The highly sophisticated malware has infected users' Apple or Android telephones without their noticing and without any action from the user's part. Through the spyware, the perpetrators may have been able to harvest data from the device and exploit its features." reads a statement published by the Ministry.

The NSO Group is a leading Israeli cyber- company which made it to the news after 50,000 phone numbers worldwide on a leaked list were linked to its notorious spyware Pegasus. The spyware was used to monitor high-profile targets, including but not limited to the heads of states, journalists, human rights activists, and political rivals, and in this case, Finnish Diplomats.

"The Ministry for Foreign Affairs is continually monitoring events and activities in its operating environment and assessing related risks. The Ministry for Foreign Affairs monitors its services and strives to prevent harmful activities. The preparation of and decisions on foreign and security policy, in particular, are matters that attract much interest, which may also manifest itself as unlawful intelligence." concludes the Ministry. "The Ministry responds to the risk by various means, but complete protection against unlawful intelligence is impossible."

The key futuristic feature of Pegasus spyware is that it can be installed on a targeted phone with just a missed call or text message; it uses a zero-click iMessage exploit to deliver a chain of zero-day exploits to invade security features on the smartphone. The evasion will install the Pegasus spyware without the user's permission and knowledge.

The critical data that is being extracted using Pegasus spyware is:

- Photos and Screenshots
- Microphone recordings
- Video recordings
- Email and SMS
- Live GPS data
- Network Details
- Device Settings Info
- Browsing History
- Contact Details
- Social Networks
- Phone Calls
- File Retrievals
- Keystrokes
- Messaging data exfiltration from common applications including WhatsApp, Skype, Facebook, Twitter, Viber, Kakao
- Email exfiltration from Android's Native Email client
- Contacts and text messages.

The silver lining is that the information has been classified as Level 4 (the lowest level of classified information) or public. However, its sources may be subject to diplomatic confidentiality.

Impact

- Information Theft
- Performance Degradation
- Misuse of Data
- Financial Loss

Indicators of Compromise

MD5

- 4261312a1666ccaeb48d55ddd1d64559
- 530b4f4d139f3ef987d661b2a9f74f5f
- 7c3ad8fec33465fed6563bbfabb5b13d
- 8d4b77fa3546149f25bd17357d41fbf0
- cc9517aafb58279091ac17533293edc1

SHA-256

- 316fac5ae2d4e250b1c0f10b4388fa2c6c3407b118e539a7d865613e373628d9
- fa538fc20af8aa198db5e932b2afaf9710633a49cf3e19b7465175520e3e8b47
- ade8bef0ac29fa363fc9afd958af0074478aef650adeb0318517b48bd996d5d5
- bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
- 9fae5d148b89001555132c896879652fe1ca633d35271db34622248e048c78ae

SHA-1

- 620947ef46f8e8f7efbf9442845b81901c8034b6
- cf1267119890c3b663fbffe5fbf4d8116316d88c
- e5920f3723e62e1850157f09baf556006bf80f74
- 7289737c1dc462726abbe89335a7702c130bbdcc
- 28f570754274db96bffa7ac4a53a5ede3508d82c

Remediation

- It is exceptionally difficult to protect against such sophisticated attacks due to the extensive use of zero-day exploits, but not impossible. Mentioned below are some best practices that can be adopted to safeguard oneself against Pegasus & such attacks to the optimum level of security.
- Use mobile phone EDR aka mobile endpoint detection and response.
- Use a reputable password manager app.
- Use Authenticator app (i.e., Google authenticator app, Microsoft authenticator app).
- For extra security, get a physical authenticator key like YubiKey, that can be used on the
- Phone and laptop.
- Switch to an uncommon but safe web browser.
- Do not use an outlook mail client or any email server that’s inbuilt on your OS. Switch to uncommon but reputable and
- secure email clients.
- Ensure that all your devices and logins are stored in your password manager and use the password generator
- Ensure all your logins are connected to your authenticator app/device.
- Your anti-virus software should be enabled to lock and erase your device if it’s stolen.
- Use Securedrop for document sharing, etc.
- Use a different SMS app (Disable iMessage, or if possible, delete it since it has been abused by Pegasus & other threat
- actors multiple times exploiting zero-day providing the Pegasus an initial access point. It will be not wrong to say it’s
- their favorite attack spot).
- Only open links from known and trusted contacts and sources when using your device.
- Make sure your device is updated with any relevant patches and upgrades.
- Avoid public and free Wi-Fi services (including hotels), especially when accessing sensitive information.
- Do not blindly approve app permission requests.
- Keep checking app permissions.