Cybersecurity threat trends show increased vulnerability for Apple devices

In the latest Advanced Persistent Threat (APT) trends report for the second quarter of 2023, Kaspersky researchers analysed the development of new and existing toolsets, the creation of new malware variants, and the adoption of fresh techniques by threat actors.

2023 is seeing expanded malware targeted at Apple devices. Source: cottonbro studio/Pexels

One significant new revelation was the exposure of the long-running “Operation Triangulation” campaign involving the use of a previously unknown iOS malware platform. The assumptions that malware doesn’t really exist for iOS is false and dangerous because the attack surface extends to hundreds of millions of devices with the same level of data encryption.

In more varied ecosystems like Android where there are multiple manufacturers, threats can be less widespread, but not less vulnerable.

Experts also observed other interesting developments that they believe everyone should be aware of. Here are key highlights from the report:

Mysterious Elephant marches on Asia-Pacific

Kaspersky uncovered a new threat actor belonging to the Elephants family, operating in the Asia-Pacific region, dubbed “Mysterious Elephant”.

In their latest campaign, the threat actor employed new backdoor families, capable of executing files and commands on the victim's computer, and receive files or commands from a malicious server for execution on the infected system.

While Kaspersky researchers have observed overlaps with Confucius and SideWinder, Mysterious Elephant possesses a distinctive and unique set of TTPs, setting them apart from other groups.

Senegalese government websites hit with cyberattack

Reuters 29 May 2023

Updated toolsets and new MacOS threat

Threat actors are constantly improving their techniques, with Lazarus upgrading its Mata framework and introducing a new variant of the sophisticated Mata malware family,

MataV5. BlueNoroff, a financial attack-focused subgroup of Lazarus, now employs new delivery methods and programming languages, including the use of trojanised PDF readers in recent campaigns, the implementation of macOS malware, and the Rust programming language.

Additionally, ScarCruft APT group has developed new infection methods, evading Mark-of-the-Web (MotW) security mechanism. The ever-evolving tactics of these threat actors present new challenges for cybersecurity professionals.

Geopolitics is still driving APT activity

APT campaigns remain geographically dispersed, with actors concentrating their attacks on regions such as Europe, Latin America, the Middle East and various parts of Asia.

Cyber-espionage, with a solid geopolitical backdrop, continues to be a dominant agenda for these endeavours.

"While some threat actors stick to familiar tactics like social engineering, others have evolved, refreshing their toolsets and expanding their activities. Moreover, new advanced actors, such as those conducting the 'Operation Triangulation' campaign, constantly emerge," comments David Emm, principal security researcher at Kaspersky's global research and analysis team (Great).

"This actor uses a previously unknown iOS malware platform distributed through zero-click iMessage exploits. Staying vigilant with threat intelligence and the right defense tools is crucial for global companies, so they can protect themselves against both existing and emerging threats."

Shore up your defenses

Avoid falling victim to a targeted attack by:

• Updating your operating system and other third-party software to their latest versions. Maintaining a regular update schedule is essential in order to stay protected from potential vulnerabilities and security risks.

• Upskilling your cybersecurity team to tackle the latest targeted threats. There are excellent online training courses available.

• Implementing an end point detection and response (EDR) solution to detect and investigate incidents.

To read the full APT trends report, visit Securelist.