Experts Detail Multi-Million Dollar Licensing Model of Predator Spyware

Dec 21, 2023 Newsroom

A new analysis of the sophisticated commercial spyware called Predator has revealed that its ability to persist between reboots is offered as an "add-on feature" and that it depends on the licensing options opted by a customer.

"In 2021, Predator spyware couldn't survive a reboot on the infected Android system (it had it on iOS)," Cisco Talos researchers Mike Gentile, Asheer Malhotra, and Vitor Ventura said in a report shared with The Hacker News. "However, by April 2022, that capability was being offered to their customers."

Predator is the product of a consortium called the Intellexa Alliance, which includes Cytrox (subsequently acquired by WiSpear), Nexa Technologies, and Senpai Technologies. Both Cytrox and Intellexa were added to the Entity List by the U.S. in July 2023 for "trafficking in cyber exploits used to gain access to information systems."

The latest findings come more than six months after the cybersecurity vendor detailed the inner workings of Predator and its harmonious equation with another loader component called Alien.

"Alien is crucial to Predator's successful functioning, including the additional components loaded by Predator on demand," Malhotra told The Hacker News at the time. "The relationship between Alien and Predator is extremely symbiotic, requiring them to continuously work in tandem to spy on victims."

Predator, which can target both Android and iOS, has been described as a "remote mobile extraction system" that's sold on a licensing model that run into millions of dollars based on the exploit used for initial access and the number of concurrent infections, putting them out of reach of script kiddies and novice criminals.

Spyware such as Predator and Pegasus, which is developed by NSO Group, often rely on zero-day exploit chains in Android, iOS, and web browsers as covert intrusion vectors. But as Apple and Google continue to plug the security gaps, these exploit chains may be rendered ineffective, forcing them to go back to the drawing board.

However, it's worth noting that the companies behind mercenary surveillance tools can also procure either full or partial exploit chains from exploit brokers and fashion them into an operational exploit that can be employed to effectively breach target devices.

Another key aspect of Intellexa's business model is that offloads the work of setting up the attack infrastructure to the customers themselves, leaving it with room for plausible deniability should the campaigns come to light (as it inevitably does).

"The delivery of Intellexa's supporting hardware is done at a terminal or airport," the researchers said.

"This delivery method is known as Cost Insurance and Freight (CIF), which is part of the shipping industry's jargon ('Incoterms'). This mechanism allows Intellexa to claim that they have no visibility of where the systems are deployed and eventually located."

On top of that, Intellexa possesses "first-hand knowledge" of whether their customers are performing surveillance operations outside their own borders owing to the fact that the operations are intrinsically connected to the license, which, by default, is restricted to a single phone country code prefix.

This geographic limitation, nonetheless, can be loosened for an additional fee.

Cisco Talos noted that while public exposure of private-sector offensive actors and their campaigns have been successful at attribution efforts, it has had little impact on their ability to conduct and grow their business across the world, even if it may affect their customers, such as governments.

"It may increase the costs by making them buy or create new exploit chains but these vendors appear to have seamlessly acquired new exploit chains, enabling them to remain in business by jumping from one set of exploits to another as a means of initial access," the researchers said.

"What is needed is the public disclosure of technical analyses of the mobile spyware and tangible samples enabling public scrutiny of the malware. Such public disclosures will not only enable greater analyses and drive detection efforts but also impose development costs on vendors to constantly evolve their implants."

Breaking News