Security Analyst Summit 2023: key research

usa.kaspersky.com/blog/sas-2023-research/29254/

Kaspersky named "top player" in APT protection market by Radicati Group

At the international Security Analyst Summit conference last week, our Global Research and Analysis Team (GReAT) experts presented some extremely exciting research. Here's a brief outline the most interesting findings.

StripedFly spyware platform

This looks almost like a detective story about malware that was previously detected as a regular Monero cryptocurrency miner, but was in fact a cover for a complex modular threat capable of infecting computers running both Windows and Linux. Various StripedFly modules can steal information from a computer, take screenshots, record audio from a microphone, and intercept Wi-Fi passwords. However, it's used not only for spying — it's also got modules that can function as ransomware and for cryptocurrency mining.

What’s interesting is that the threat can spread using the EthernalBlue exploit — even though that vector was patched back in 2017. In addition, StripedFly can use stolen keys and passwords to infect Linux and Windows systems with an SSH server running. A detailed study with indicators of compromise can be found on the Securelist blog.

Operation Triangulation details

Another Security Analyst Summit report was dedicated to the completion of the investigation of Operation Triangulation, which, among other things, targeted our employees. A detailed analysis of the threat allowed our experts to detect five vulnerabilities in the iOS system used by this threat actor. Four of them (CVE-2023-32434, CVE-2023-32435, CVE-2023-38606 and CVE-2023-41990) were zero-day vulnerabilities. They affected not only the iPhone, but also iPod, iPad, macOS, Apple TV and Apple Watch. It also turned out that in addition to infecting devices via iMessage, attackers could attack the Safari browser. In this post you can read the details of how our experts analyzed this threat.

New Lazarus campaign

The third report by GReAT experts was devoted to new attacks carried out by the Lazarus APT. This group is now targeting software developers (some of which have been attacked multiple times) and is actively employing supply chain attacks.

Through vulnerabilities in legitimate software for encrypting web communications, Lazarus infects a system and deploys a new SIGNBT implant — the main part of which operates in memory only. It serves to study the victim (getting network settings, and names of processes and users), as well as launch an additional malicious payload. In particular, it downloads an improved version of the already known LPEClient backdoor, which also runs in memory and in turn launches malware capable of stealing credentials and other data. Technical information about the new tools of the Lazarus APT group, as well as indicators of compromise, can also be found on the Securelist blog.

TetrisPhantom attack

Our experts provided details of the TetrisPhantom attack aimed at government agencies in the APAC region. TetrisPhantom relies on compromising a certain type of secure USB drive that provides hardware encryption and is commonly used by government organizations. While investigating this threat, experts identified an entire spying campaign that uses a range of malicious modules to execute commands, collect files and information from compromised computers, and transfer it to other machines also using secure USB drives. Some details about this campaign can be found in our quarterly report on APT threats.