‘Nexus’ Android Trojan Targets 450 Financial Applications

The Nexus Android banking trojan is being promoted on underground forums as a new botnet, under the malware-as-a-service (MaaS) business model, according to fraud prevention firm Cleafy.

The trojan was initially announced in June 2022, but was active months before that. Starting January 2023, however, its authors started promoting it as a botnet, at $3,000 per month for a MaaS subscription.

Although still in development stages, the malware appears to be used by multiple threat actors, mainly in attacks aimed at taking over banking and cryptocurrency accounts. The threat can intercept SMS messages and steal credentials, targeting roughly 450 financial applications.

Nexus is promoted as a completely new trojan, but Cleafy identified connections with the Sova banking trojan that point at code reuse. In fact, Sova’s author has been claiming that Nexus’ developer is a former affiliate that rented the malware to steal its source code.

Cleafy also discovered that both malware families check for a device’s geographical location in a similar manner, that they both ignore devices located in the same countries, and that the two share API similarities related to command-and-control (C&C) communication.

The Nexus trojan appears specifically designed to conduct

account takeover attacks: it can overlay on top of target applications, can log the victim’s key presses, can steal two-factor authentication (2FA) codes delivered via SMS, and can abuse Accessibility Services to steal crypto-wallet information, Google Authenticator 2FA codes, and browser cookies.

Between August 2022 and January 2023, the malware developers added to Nexus the ability to delete received SMS messages and a feature to enable and disable the 2FA stealer module.

The trojan’s developers also packed it with an auto-update mechanism and appear to be working on enabling encryption capabilities, either to hide its malicious activities on infected devices, or in preparation for a ransomware module, Cleafy says.

Nexus developers manage the malware and data collection operations from a centralized interface that provides information on infected devices and the botnet’s status, and allows them to create customized samples.

The panel also allows malware operators to create custom injections targeting the applications of 450 different financial institutions.

Related: Godfather Android Banking Trojan Targeting Over 400 Applications

Related:‘Schoolyard Bully’ Android Trojan Targeted Facebook Credentials of 300,000 Users

Related: Hack-for-Hire Group Targets Android Users With Malicious VPN Apps

https://www.securityweek.com/nexus-android-trojan-targets-450-financial-applications/