New ‘SharkBot’ Android Banking Malware Hitting U.S., UK and Italy Targets

A new Android banking trojan has been found, targeting international banks from the United Kingdom and Italy (including in the U.S.). and five different cryptocurrency services. Twenty-two instances have been discovered, but more are expected.

The malware, first detected at the end of October 2021, appears to be new and still being developed. It was discovered by Cleafy, a Milan, Italy-based online fraud detection and prevention firm. Cleafy calls it ‘SharkBot’, named after the frequency of the word ‘sharked’ in its binaries.

SharkBot is not found in Google’s official marketplace. This means it must be sideloaded by delivering the APK to the device and ensuring it is manually loaded. In a technical analysis of the malware, Cleafy notes that it poses as a legitimate application using common names and icons.

If the deception succeeds and the malware is installed, it immediately attempts to enable Android’s Accessibility Services by delivering fake pop-ups to the victim – such as ‘Allow Media Player to have full control of your device’. If this is successful, SharkBot has all the permissions it needs.

Once accepted the malware can enable keylogging (to steal typed credentials), intercept SMS messages (to circumvent MFA), deliver overlay attacks (to steal login credentials and credit card information) and remotely control the device because permissions were granted via the fake pop-up. “Basically,” comments Corey Nachreiner, CSO at WatchGuard Technologies, “the malicious Accessibility Services can read

anything a user can read and can recreate any action a user can on the device."

Notably, SharkBot also attempts a relatively novel technique known as an Automatic Transfer Systems (ATS) attack. "This technique has been seen recently from other banking trojans, such as Gustuff," explains Cleafy. "ATS is an advanced attack technique (fairly new on Android) which enables attackers to auto-fill fields in legitimate mobile banking apps and initiate money transfers from the compromised devices."

The ATS functionality is contained in a module downloaded separately from the C2. "Given its modular architecture," comments Cleafy, "we don't exclude the existence of botnets with other configurations and targets."

[READ: Android Trojan Targets Banks, Crypto-Currencies, e-Commerce]

The assumption is that ATS is used by SharkBot to bypass the behavioral detection measures used by many financial institutions. If ATS is used on what is a trusted device, a 'new device enrollment' phase is not necessary, SMS-based MFA can be bypassed, and behavioral biometrics are not effective.

Although relatively few instances of SharkBot have been discovered in the wild, Cleafy suspects that the threat will grow. This is partly because it is new, and apparently still being developed.

"The implications of becoming infected with SharkBot could be severe, so it's important," says Nachreiner, "to avoid being infected altogether." This is not yet easy. The malware is new and not well detected by existing detection means. Apart from the DGA for its C2s, it also uses anti-analysis techniques including obfuscated strings and emulator detection.

The best solution is to avoid side-loading religiously. Without 100% certainty in the authenticity of the application

and the validity of its source, simply do not install it.

Related: Android Banking Trojan 'Vultur' Abusing Accessibility Services

Related: Android Trojan Targets Banks, Crypto-Currencies, e-Commerce

Related: Automatic Transfer System Evades Security Measures, Automates Bank Fraud

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend:

Tags:

https://www.securityweek.com/new-%E2%80%98sharkbot%E2%80%99-android-banking-malware-hitting-us-uk-and-italy-targets