Cleafy's Threat Intelligence team tracks down a new generation of Android Trojans targeting banks in Europe

Milan, Italy - November 18th, 2021- At the end of October 2021, the Cleafy Threat Intelligence team discovered a new Android banking trojan targeting banks and cryptocurrency exchanges in Italy, the UK, and the US. Since there were no references to any known families, Cleafy's team decided to dub this new family **SharkBot**.

The main goal of SharkBot is to initiate money transfers from the compromised devices via the Automatic Transfer Systems (ATS) technique bypassing multi-factor authentication mechanisms (such as SCA). These mechanisms are used to enforce users' identity verification and authentication and are usually combined with behavioral detection techniques to identify suspicious money transfers.

"We have observed that once SharkBot is successfully installed in the victim's device, attackers can obtain sensitive banking information through the abuse of Accessibility Services, such as credentials and personal information, but also to perform gestures on the infected device." Said Federico Valentini, Head of Threat Intelligence and Incident Response at Cleafy. "With the discovery of SharkBot, we realized that a new generation of mobile attacks is quickly spreading in the online world, raising the level of risk and uncertainty for businesses and their customers."

SharkBot implements overlay attacks to steal login credentials and credit card information and it also has the capabilities to intercept legitimate banking communications sent through SMS. So far, it appears to have a very low detection rate by antivirus solutions.

In the past few weeks, Cleafy's Threat Intelligence team has worked hard to analyze and gather some deep insights on this new malware, which are collected in the technical report "SharkBot: a new generation of Android Trojans is targeting banks in Europe" published on November 11th on the company's website.

In this report, the team compiled all the relevant information to help industry professionals better understand how the malware works and how it is possible to prevent it from attacking the banking systems. As of today, the report has been cited and shared by several industry magazines, such as The Hacker News, CyberSecurity360, ZD NET Security, The Record by Recorded Future, BankInfo Security, and TECH Times.

As of today, multiple indicators suggest that SharkBot could be at its early stages of development.

To learn more visit www.cleafy.com/labs.

Cleafy S.p.a.
VAT: 02340370226
email: info@cleafy.com
pec: cleafy@legalmail.it
cleafy.com

Headquarters
Via Simone Schiaffino n. 11
20158 Milano, ITALY
Tel: +39 02 49517001
Fax: +39 02 70059905

About Cleafy

We are a team of fraud hunters, cybersecurity experts, data scientists, and software engineers that since 2014 share the same dream: make technology a safer place.
Every day, we work side by side with our customers to help them safely navigate the digital world, while growing their business. And we do it with passion, determination, and constant curiosity about the unexpected.
Our purpose is to make people's life easier and free from the threats hidden in the digital ecosystem.
That's why we designed a technology that identifies and prevents financial frauds in real-time while ensuring a safe and seamless user experience.
Recognized as a market leader by industry analysts, today we protect over 60M+ users of top-tier retail and corporate banks against financial online fraud.

About Cleafy LABS

Cleafy LABS is an initiative launched in 2021 by Cleafy and led by our Threat Intelligence team, a group of fraud hunters whose objective is to study, prevent and identify all possible threats in the cybersecurity world.
Every time our fraud hunters discover a new threat, they share all the information at hand through detailed reports and analyses. The purpose is to spread awareness in the industry and grant a high level of security to online customers.
Information means power, and for us sharing this information means empowering businesses every day to keep their customers safe and free from the worries of the digital world.

Cleafy S.p.a.
VAT: 02340370226
email: info@cleafy.com
pec: cleafy@legalmail.it
cleafy.com

Headquarters
Via Simone Schiaffino n. 11
20158 Milano, ITALY
Tel: +39 02 49517001
Fax: +39 02 70059905