BancaMarStealer

Customizable Malware-as-a-Service banking trojan delivered through any app with messaging capabilities.

Background and Discovery Timeline

The Lookout Threat Intelligence team discovered BancaMarStealer, a mobile trojan malware family designed to phish the victim's login credentials for banking and other services. Since initially being announced by Lookout in 2018, the number of observed samples of BancaMarStealer has grown from 7,700 to over 74,000 as of April 2021.

Key Findings

1. This banking trojan can be very effective when combined with social engineering and mobile phishing.
2. As a highly customizable piece of malware, it can be used to target employees or customers of any organization.
3. The total number of samples has grown almost 10 times in three years.

Capabilities and Affected Parties

BancaMarStealer is a mobile-specific banking trojan that serves as a perfect example of malware-as-a-service (MaaS). Out of the box, it can be configured to target specific banks, or any online service, communicate with specific command and control servers, and support a wide range of remote commands. It is delivered to the victim via SMS in a message that prompts the user to download a custom app. This makes it highly effective in social engineering campaigns.

Since it's a highly customizable piece of malware, BancaMarStealer continuously evolves and has become one of the most robust banking trojans seen to date. In addition to being able to steal login credentials through screen overlays, it also has the following capabilities:

- Grant significant control over the device
- Silently call attacker-specified numbers
- Send spam to contacts
- Reset the device
- Retrieve and intercept all SMS messages
- Change the command-and-control IPs
- Target the device with additional malware

How Lookout Detects and Protects Against Banking Trojan and Malware Campaigns

Lookout Security Intelligence teams are continuously discovering and researching new threats to protect and advise our customers. We do this by combining static and dynamic analysis with our machine learning engine. Devices with Lookout installed can detect and be alerted when BancaMarStealer is present. Lookout admins can create policies that block access to corporate resources until the malware is removed from the infected device.

Lookout Threat Advisory Service

In the fast-changing world of cybersecurity, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest threats and risks.

Click here to learn more about Threat Advisory