⬡ Lookout®

Alien Banking Trojan

Overview

The FBI recently released a FLASH report focusing on the Alien mobile malware, which is a variant of the widely used Cerberus mobile banking trojan. Alien joins the likes of Eventbot, Cerberus, and Anubis as well-known and highly customizable banking malware that cybercriminals can purchase through a Malware-as-a-Service (MaaS) model.

Alien is primarily delivered through phishing and smishing, which is common for this type of malware. Attackers can socially engineer their targets across mobile platforms including SMS, third-party messaging apps, social media, gaming and even dating apps to trick them into downloading the malware. Alien's capabilities align with what's commonly seen in banking trojans including but not limited to displaying phishing pages for legitimate applications, stealing login credentials, sending SMS messages from the device to spread to the victim's contacts, and exfiltrating authentication tokens.

Lookout Coverage and Recommendation for Admins

Lookout customers are currently protected from all variants of Cerberus including Alien. If the malware is delivered via a malicious link, Lookout Phishing and Content Protection (PCP) will block the device's connection to that link. Admins can require activation of Lookout PCP across the mobile fleet to ensure their users are protected from this attack vector.

If the user mistakenly downloads an app infected with the malware to their device, Lookout will alert the user and provide them instructions on how to remove the app and malware from the device. Admins can also create policies that block the device's access to corporate resources until it is clear of all malware.

Lookout Analysis

Lookout data shows that in 2021, most mobile phishing attacks intended to deliver malware like Alien. This exemplifies how problematic Malware-as-a-Service (MaaS) like Alien can be. Another well-known banking trojan that sold in the MaaS market is BancamarStealer. Upon initial discovery, researchers observed 7,700 samples of the malware in 2018. As of October 2021, Lookout researchers have observed over 130,000 samples, which exemplifies how explosive malware delivered as a service can be.

Lookout Phishing and Content Protection

As part of the broader endpoint-to-cloud security solution, Lookout provides comprehensive mobile phishing protection on both Android and iOS devices. This gives admins powerful tools for monitoring, managing and protecting mobile devices, and enables organizations to confidently embrace the use of smartphones within their organization.

Click here to learn more about Phishing and Content Protection