Warning As Devious New Android Malware Hides In Fake Adobe Flash Player Installations (Updated)

forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/

Zak Doffman August 16, 2019

Cybersecurity
Zak Doffman
Contributor
Opinions expressed by Forbes Contributors are their own.

I cover security and surveillance and co-host 'Straight Talking Cyber'

Aug 16, 2019,01:59am EDT|

This article is more than 2 years old.

Getty

Millions of Android users are being warned about a devious new banking trojan, dubbed Cerberus, that infects devices by masquerading as an Adobe Flash Player installation. Once installed, the fake download requests accessibility permissions that allow an attack to take

place. The malware overlays login screens for banking apps, stealing credentials for its operators. Cerberus also has a crafty evasion technique—using the accelerometer on an infected device to ensure the target is real and not a desk-based security analyst.

The developers behind Cerberus are reportedly renting the trojan out on the dark web and have taken the unusual step of advertising their capabilities on Twitter. The threat actors even use their Twitter account to mock the security community tasked with trying to stop them—and they are so confident, they even tried to sell the bot to a well known malware analyst so he could examine their work.

Cerberus infects users when they access a fake website which immediately requests a download of Adobe Flash Player. The download is fake, and carries the malware payload.

A video of the infection process can be seen here.

Android banking trojans are nothing new, and Cerberus is just the latest in a long line of such malware to hit the headlines. Even the fact that Cerberus is being "rented out" on underground forums is not unique. Malware "for hire" has become a theme.

Cerberus has been designed to steal banking credentials. It does this—again not unusually—by creating overlays on top of banking apps that capture usernames and passwords as they are being entered. Such overlays are designed around specific apps, and Cerberus has developed more than 30 of these thus far. Of note, the target banks are in the U.S., France and Japan—a fairly specific list of countries.

ESET security researcher Lukas Stefanko told me he "found Cerberus in June, a couple of days after it was published on an underground forum." Stefanko used Twitter to ask the research community if anyone had come across it before, "and that is when I noticed their twitter handle joined the debate under my tweet."

"Even though they know I am android malware analyst," Stefanko told me, "they tried to sell me their Cerberus bot. They created a profile where the only thing I needed to do is buy it. However my goal was to obtain working sample and C&C address to properly analyze it." The developers sent Stefanko a sample of Cerberus, but used his Twitter handle "instead of a real C&C server," and so he was unable to test it.

Two days later, Stefanko and colleagues "detected an active campaign using this new banking Trojan with thousands of website visits that contained the payload. Cerberus was spread via a fake website that asked users to install Adobe Flash Player."

Lukas Stefanko

Stefanko explained to me that the Cerberus developers used "a web framework where anyone can check website visit statistics—because of that I found out which countries are targeted with actual number of site visits."

Over a fourteen day period, Stefanko tracked more than 13,000 visits to the fake Cerberus website, most of which were from users in the U.S. and Japan.

At about the same time, Cerberus was seen being rented out in underground forums by the team at ThreatFabric. The malware's developers claimed it had been used privately for two years beforehand, and that it was "written from scratch" and does not "borrow" code from existing malware, making it harder to detect. There is certainly none of the leaked Anubis source code within Cerberus.

"Rental of banking Trojans is not new," the researchers explain. "It was an existing business model when computer-based banking malware was the only form of banking malware and has shifted to the Android equivalent a few years later."

Cerberus often comes as a social media attachment, so the usual caution on thinking before clicking applies. The malware uses its Flash Player application to trick user into granting accessibility rights. The malware can then grant itself additional rights to control the device, send messages, make calls, communicate back to its handlers. It can even disable Google Play Protect to avoid automatic detection.

None of which its unusual. And so the clever stuff—Cerberus has been designed to avoid detection from desk-based malware analysts by delaying activation until it can confirm the device belongs to a genuine victim. It uses the device's accelerometer to measure steps. "The Trojan uses this counter to activate the bot," ThreatFabric explains. And when the step counter hits a target, "it considers running on the device to be safe." This counter-measure "prevents the Trojan from running and being analyzed in dynamic analysis environments (sandboxes) and on test devices."

But the real standout for Cerberus is that its developers have even taken to Twitter to "post promotional content (even videos) about the malware" and to "make fun of the antivirus community—sharing detection screenshots from VirusTotal (thus leaking IoC) and even engaging in discussions with malware researchers directly."

Cerberus is not seen as "moving the needle" for trojan capabilities, but it's dangerous nonetheless. "Cerberus should not be taken lightly," ThreatFabric warns. It can harvest contacts, send messages, steal credentials. And its overlays are not limited to banking apps —it can attack messaging or other accounts using the same techniques.

The rental model is interesting—it ensures the malware can evolve and spread quickly, and it increases the likely damage during its lifespan. There is also the question of the apps coverage thus far—U.S., France and Japan. If those were created to order, then the rental model will quickly add more.

But the most interesting element to Cerberus is the cat and mouse game playing out in the open as its developers taunt the catcher community. And as entertaining as those Twitter exchanges might be, it's important to remember there are many thousands of victims of

Cerberus whose lives will be badly impacted.

And so, as ever, the usual advice applies. Take care what you download and install—avoid gimmicks and untrusted sources, use common sense. Our smartphones are the keys to our digital worlds, and malware like Cerberus is designed to steal those keys while avoiding detection in ever more clever ways.

Zak Doffman