

Android bank app users targeted in sophisticated malware attack - blueAPACHE

Canonical: <https://www.blueapache.com/blog/android-bank-app-users-targeted-in-sophisticated-malware-attack>

Details:

Summary

This blog post, "Android bank app users targeted in sophisticated malware attack", is a blueAPACHE article from 2016 covering security. Hot on the tail of our recent article on new Android malware discovered by Palo Alto Networks (and the scary numbers released by Bitdefender), ESET has identified that a new trojan named Android/Spy.Agent.SI is mimicking banking and other financial applications on Android devices. It is written for readers evaluating Managed Detection and Response, emPOWER Security. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Topic	Android bank app users targeted in sophisticated malware attack
Services referenced	Managed Detection and Response, emPOWER Security, emPOWER Core Network & DC Interconnect
Named products or vendors	Palo Alto Networks, Google

Article

Hot on the tail of our recent article on new Android malware discovered by Palo Alto Networks (and the scary numbers released by Bitdefender), ESET has identified that a new trojan named Android/Spy.Agent.SI is mimicking banking and other financial applications on Android devices. According to media releases, millions of customers of Australia and New Zealand's largest banks may be targeted. Discovered January 29 2016, the trojan is also known as HEUR:Trojan-Banker.AndroidOS.Agent.au (Kaspersky) and Android.SmsBot.539.origin (Dr.Web). The malware presents victims with a fake version of the login screen of their banking application and locks the screen until they enter their username and password. Using the stolen credentials, the thieves can then log in to the victim's account remotely and transfer money out. They can even get the malware to send them all of the SMS text messages received by the infected device, and remove these. "This allows SMS-based two-factor authentication of fraudulent transactions to be bypassed, without raising the suspicions of the device's owner," explains Lukáš Štefanko, ESET Malware Researcher who specialises in Android malware. In its current state, the Trojan spreads as an imitation of Flash Player

application. After being downloaded and installed, the app requests administrator rights to protect itself from being easily uninstalled from the device. It then checks if any target banking applications are installed on the device, and if they do, it downloads fake login screens for each banking app from its command and control server. When the victim launches a banking app, a fake login screen appears over the top of the legitimate app, leaving the screen locked until the victim submits their banking credentials. It currently targets major banks in Australia, New Zealand and Turkey. In fact, the 20 financial institutions currently targeted by the app include the largest retail banks in each of the three countries. Examples of the fake overlays are: The full list of targeted banks include: ANZ Bank, Commonwealth Bank, National Australia Bank, Westpac, St. George Bank, Bendigo Bank, Bankwest, Me Bank, ASB Bank, Bank of New Zealand, Kiwibank, Wells Fargo, Finansbank, Halkbank, VakfBank, Garanti Bank, Yap Kredi Bank, Akbank, Türkiye Bankas and Ziraat Bankas.

“The attack has been massive and it can be easily re-focused to any another set of target banks,” warns Lukáš Štefanko. Hackers can make millions if they get the malware model right, as we saw with cryptolocker . Successes like cryptolocker mean there will always be people and organised groups trying to develop new ways to exploit devices and systems. Fortunately, there are things you can do to protect yourself.

If you see anything masquerading as Adobe Flash Player on Android, you can be sure it's fake. Flash Player hasn't created a client for Android since 2012, so it is highly unlikely anything legitimate is still making the rounds on the mobile platform.

Only install mobile apps from the official Google Play Store rather than third-party sites.

Add antivirus to your devices. This will only detect known threats, but may pick up something you miss.

Last but not least, if you do become infected with Android/Spy.Agent.SI, you can remove the malware by disabling the fake Flash Player's administrator privileges in Settings or by removing it while in Safe Mode. As always, we encourage all clients to add employee training on spotting potential security threats to their training programs. While this trojan targets banking applications, it could easily be modified to target business applications or services, presenting an entirely different array of issues for organisations. For more information on security, or educating your staff on how to identify malware before it becomes an issue, contact the blueAPACHE account team .

Related

Managed Detection and Response

emPOWER Security (pillar hub)

emPOWER Security

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

Lovisa (case study)

Frequently asked questions

What trojan does the article name, and what does it disguise itself as?

The article names the trojan Android/Spy.Agent.SI, identified by ESET and also known as HEUR:Trojan-Banker.AndroidOS.Agent.au (Kaspersky) and Android.SmsBot.539.origin (Dr.Web). It says the trojan spreads as an imitation of the Flash Player application and was discovered on 29 January 2016.

What does the article say the malware does with SMS text messages, and why does that matter?

The article says the malware can get infected devices to send all received SMS text messages to the attackers and then remove them from the device. ESET malware researcher Lukáš Štefanko is quoted saying this allows SMS-based two-factor authentication of fraudulent transactions to be bypassed without raising the device owner's suspicions.

How many banks and which three countries does the article say were targeted?

The article says 20 financial institutions across Australia, New Zealand and Turkey were targeted, including the largest retail banks in each country. It names examples including ANZ Bank, Commonwealth Bank, Westpac, ASB Bank, Bank of New Zealand, and Turkey's Garanti Bank and Akbank.

What three protective steps does the article recommend to avoid infection?

The article recommends treating anything masquerading as Adobe Flash Player on Android as fake, since Flash Player has not had an Android client since 2012. It also recommends only installing apps from the official Google Play Store and adding antivirus software to devices, while noting antivirus only detects known threats.

Is this post still current?

No. This post describes a specific malware threat identified in January 2016 and a list of banks targeted at that time. For current security guidance, a reader should use the linked service pages rather than this post.

Source

origin post (2016)

Knowledge Base

What is the URL of this blueAPACHE article?

The article can be found at
<https://www.blueapache.com/blog/android-bank-app-users-targeted-in-sophisticated-malware-attack>.