

New Android threats appear, and they're worth noting - blueAPACHE

Canonical: <https://www.blueapache.com/blog/new-android-threats-appear-and-theyre-worth-noting>

Details:

Summary

This blog post, "New Android threats appear, and they're worth noting", is a blueAPACHE article from 2016 covering security. Ransomware and hijacking Trojans have been plaguing Windows for the past couple of years, but recently it seems to have developed platform-agnostic capabilities and has moved towards Android. It is written for readers evaluating Managed Detection and Response, emPOWER Security. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2016
Topic	New Android threats appear, and they're worth noting
Services referenced	Managed Detection and Response, emPOWER Security, emPOWER Core Network & DC Interconnect
Named products or vendors	Windows, Palo Alto Networks, Google
Cited statistic	These were ransomware that demanded \$500 to restore access to the device.

Article

Ransomware and hijacking Trojans have been plaguing Windows for the past couple of years, but recently it seems to have developed platform-agnostic capabilities and has moved towards Android. Palo Alto Network's research team, Unit 42, has recently announced the discovery of 22 Android applications that belong to a new Trojan family named "Xbot". Xbot attempts to steal victims' banking credentials and credit card information via phishing pages crafted to mimic Google Play's payment interface as well as the login pages of 7 different banks' apps. It can also remotely lock infected Android devices, encrypt the user's files in external storage (e.g., SD card), and then ask for a \$US100 PayPal cash card as ransom. In addition, Xbot will steal all SMS messages and contact information, intercept certain SMS messages, and parse SMS messages for mTANs (Mobile Transaction Authentication Number) from banks. Xbot has some additional capabilities. It will collect all contacts' names and phone numbers and upload them to its C2 server, as well as all new SMS messages. In some samples, Xbot will also intercept and parse specific SMS messages. It parses all SMS messages sent by a specific

premium rate SMS short number in an attempt to collect the victim's account and confirmation numbers from a bank in Russia, and then uploads the information to its C2 server. Xbot primarily uses a popular attack technique called "activity hijacking" by abusing some features in Android. The apps Xbot is mimicking are not themselves being exploited. Starting with Android 5.0, Google adopted a protection mechanism to mitigate this attack but other attack approaches used by Xbot are still affecting all versions of Android. Prior to the Palo Alto news, Bitdefender released data on Android and Linux ransomware. While not yet as advanced as its Windows counterpart, Android ransomware can still cause massive headaches, disruptions and financial losses. Bitdefender Android telemetry shows the Android.Trojan.Slocker ransomware family ranked first in UK, German and Australian charts, based on the number of devices that reported it. Almost twenty per cent of these threats are fake apps that install malware or highly aggressive adware through multiple mechanisms including pretending to be legitimate updates. Other delivery methods include spam messages that will hopefully be read by Android users on their devices. Bitdefender detected more than 15,000 spam emails with zipped files. These were ransomware that demanded \$500 to restore access to the device. Android ransomware could be considered more important than its PC counterpart because mobile devices have access to and store a lot of personal and even corporate data that's usually not backed up. Losing that data or simply being denied access to it could be irreversible and users would be far more inclined to pay to recover their contacts, conversations, pictures and documents. A Bitdefender study conducted in November 2015 revealed that ransomware victims would be willing to pay up to \$500 to recover their data. Regardless of whether it is Android ransomware, PC ransomware, or even Linux ransomware, malware-as-a-service has become a financially driven industry that's willing and able to supply malware to anyone who will pay for it. The Cryptolocker kit for PCs is being reportedly sold for as little as \$3,000 and with various business models that favor both the customer and the malware developers. As Android continues to dominate the mobile market, malware developers will continue to write code that fits their agenda. Whether it's stealing data or locking your device and asking for money to release it, Android malware is a lucrative business for malware coders and a gateway for other malicious actions. blueAPACHE customers of Palo Alto Networks are protected from Xbot through their optional WildFire, URL filtering, and IPS services. More information on Palo Alto's findings can be found in their Unit 42 blog . The Bitdefender report in PDF format is available here . For more information on improving your security profile, 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)

Frequently asked questions

How many Android applications did Palo Alto's Unit 42 discover belonging to the Xbot Trojan family, per this article?

22 Android applications, discovered by Palo Alto Networks' research team, Unit 42.

What ransom does Xbot demand after encrypting a victim's external storage, according to the article?

A US\$100 PayPal cash card, after remotely locking the device and encrypting files on external storage such as an SD card.

How many different banks' login pages does Xbot mimic to steal credentials, per this article?

7 different banks' apps, alongside a phishing page crafted to mimic Google Play's payment interface.

Which ransomware family topped Bitdefender's Android telemetry charts in the UK, Germany and Australia, according to this article?

Android.Trojan.Slocker, ranked first in those markets based on the number of reporting devices.

How many spam emails with zipped ransomware files did Bitdefender detect, per this article, and what ransom did they demand?

More than 15,000 spam emails with zipped files, containing ransomware that demanded \$500 to restore device access.

What price does the article say the Cryptolocker kit for PCs was being sold for on the malware-as-a-service market?

As little as \$3,000, reflecting various business models favouring both malware developers and their customers.

What Android version introduced protection against Xbot's "activity hijacking" technique, according to the article?

Android 5.0, when Google adopted a protection mechanism to mitigate this specific attack, though the article notes other Xbot attack approaches still affect all Android versions.

How does the article say blueAPACHE customers using Palo Alto Networks are protected from Xbot? Through their optional WildFire, URL filtering, and IPS services.

Source

origin post (2016)

Knowledge Base

What is the Xbot Android Trojan and who discovered it?

Xbot is a new Trojan family discovered by Palo Alto Networks' research team, Unit 42, affecting 22 Android applications. It attempts to steal victims' banking credentials and credit card information via phishing pages that mimic Google Play's payment interface and the login pages of 7 different banks' apps.

What malicious actions can the Xbot Trojan perform on infected devices?

Xbot can remotely lock infected Android devices, encrypt the user's files in external storage (like an SD card) and demand a \$US100 PayPal cash card as ransom. It also steals all SMS messages and contact information, intercepts certain SMS messages, and parses SMS messages for mTANs (Mobile Transaction Authentication Numbers) from banks. Additionally, it collects contacts' names and phone numbers, uploads new SMS messages to its C2 server, and in some samples parses SMS messages from a specific premium rate SMS short number to collect account and confirmation numbers from a bank in Russia.

What attack technique does Xbot primarily use, and does it affect all Android versions?

Xbot primarily uses a popular attack technique called 'activity hijacking' by abusing certain Android features. The apps Xbot mimics are not themselves exploited. Starting with Android 5.0, Google adopted a protection mechanism to mitigate this specific attack, but other attack approaches used by

Xbot still affect all versions of Android.

What did Bitdefender's data reveal about Android and Linux ransomware?

Bitdefender released data showing that while Android ransomware is not yet as advanced as its Windows counterpart, it can still cause massive headaches, disruptions and financial losses. Bitdefender's Android telemetry showed the Android.Trojan.Slocker ransomware family ranked first in UK, German and Australian charts based on the number of devices that reported it.

How are Android ransomware threats typically delivered to devices?

Almost twenty per cent of these threats are fake apps that install malware or highly aggressive adware through multiple mechanisms, including pretending to be legitimate updates. Other delivery methods include spam messages read by Android users on their devices; Bitdefender detected more than 15,000 spam emails with zipped files containing ransomware that demanded \$500 to restore access to the device.

Why might Android ransomware be considered more significant than PC ransomware?

Android ransomware could be considered more important than its PC counterpart because mobile devices have access to and store a lot of personal and even corporate data that's usually not backed up. Losing that data or being denied access to it could be irreversible, making users far more inclined to pay to recover their contacts, conversations, pictures and documents.

How much are ransomware victims willing to pay to recover their data, according to Bitdefender?

A Bitdefender study conducted in November 2015 revealed that ransomware victims would be willing to pay up to \$500 to recover their data.

What is the Cryptolocker kit and what does it represent about the malware industry?

The Cryptolocker kit for PCs is reportedly sold for as little as \$3,000, with various business models that favor both the customer and the malware developers. This illustrates that malware-as-a-service has become a financially driven industry willing and able to supply malware (whether Android, PC, or Linux ransomware) to anyone who will pay for it.

How are your customers protected from the Xbot Trojan?

Our customers of Palo Alto Networks are protected from Xbot through their optional WildFire, URL filtering, and IPS services.