Mobile banking Trojan modifications reach all-time high

Mobile banking Trojans hit the list of cyber-headaches in Q2 2018. The number of installation packages for mobile banking - modifications which help attackers avoid detection by security solutions and to expand their arsenal - peaked at over 61,000.

Source: Yauhen Korabau © https://www.123rf.com/

This represents a historic high; more than a three-fold growth when compared with Q1 2018, and over double the installations than in Q1 2017. This is just one of the main findings from Kaspersky Lab's Q2 IT threat evolution report.Mobile banking Trojans are one of the most infamous types of malware, as they are designed to steal money directly from mobile users' bank accounts. This type of attack is attractive to cybercriminals from all over the world, looking for an easy profit. The malware is typically disguised as a legitimate app, to lure people into installing it.

Once the banking app is launched, the Trojan displays its own interface overlaying the banking app's interface. When the user inputs credentials, the malware steals the information.

The second quarter of 2018 experienced a massive influx of these types of trojan at 61,045, which is a historic high in all the time that Kaspersky Lab has been observing such threats. The greatest contribution to the number was made by the creators of Trojan Hqwar, with about half of the new modifications discovered relating to this malware. Trojan Agent took second place with around 5,000 packages.

A global trend for mobile malware growth

In Q2 2018, the top three countries with the biggest share of users attacked with mobile banking malware as a proportion of all users attacked with any kind of mobile malware were the following: USA (0.79%), Russia (0.7%), and Poland (0.28%). Russia and USA changed places compared with Q1 2018, while Poland jumped from 9th place to 3rd – mainly due to the active distribution of Trojans.AndroidOS.Agent.cw and Trojan-Banker.AndroidOS.Marcher.w modifications.

According to Kaspersky Lab experts, such high numbers could be part of a global trend for mobile malware growth, as the overall number of mobile malware installation packages also increased by over 421,000 compared to previous quarter.

Concern regarding mobile users' security

“The threat landscape in the second quarter of this year gives us lots of cause for concern regarding mobile users’ security. The overall growth in mobile malware installation packages – especially associated with banking – demonstrates that cybercriminals are constantly creating new modifications to their malicious software to make it more sophisticated and discreet for cybersecurity vendors to detect. User and the industry should be extremely cautious and vigilant in the coming months as the trend continues to grow,” notes Victor Chebyshev, a security expert at Kaspersky Lab.

In the second quarter, Kaspersky Lab solutions detected and repelled 962,947,023 malicious attacks from online resources located in 187 countries around the world – it means over 20% growth against previous period. Attempted infections by malware that aims to steal money via online access to bank accounts grew by over 5% in comparison with Q1 2018: such attacks were registered on 215,762 user computers.

Reduce the risks

To reduce the risk of infection, users are advised to:

- Install applications only from trusted sources, ideally – from the official app store;
- Check permissions requested by the app – if they do not correspond with the app’s task (e.g. a reader asks to access your messages and calls), this can be a sign of an unscrupulous app;
- Use a robust security solution to protect you from malicious software and its actions. The free version of Kaspersky Internet Security for Android can help you avoid such unpleasant situations;
- Do not click on links from spam emails;
- Do not perform the rooting procedure of the device that will provide cybercriminals with limitless capabilities.

Read the full version of the Kaspersky Lab’s IT threat evolution report.