

## **Wroba mobile banking trojan targets US smartphones**



Kaspersky's threat monitoring system has detected a new wave of Wroba trojan activity targeting smartphone users in the United States.

Until Friday, attacks by the Wroba mobile banking trojan were limited mostly to Asia.

According to details Kaspersky released to the media, the new wave in the U.S. was detected Oct. 29 and targeted users in a variety of U.S. states, including Connecticut, Louisiana and Wisconsin. The attacks hit both iOS and Android devices.

The cybercriminals tried to attract users by notifying them of a parcel arrival and a text that said: "Your parcel has been sent out. Please check and accept it." Next, it took them to a malicious site that shows an alert saying that the user's browser is out of date and needs updating. Once a user clicks "OK" the malicious app downloads.

After the malicious app installs on the user's mobile device, Wroba can send SMS messages, open web pages, get files from folders related to financial transactions, steal contact lists, call specified numbers and show fake phishing pages to steal the victim's credentials. Kaspersky products detect the threat as Trojan-Dropper.AndroidOS.Wroba.g.

***AFP Vision 2028: A World-class Armed Forces, Source of National Pride***

Kaspersky researchers say more than 1,000 users faced Trojan-Dropper.AndroidOS.Wroba.g since the start of the year. The countries hit the hardest include Russia, Japan and China. While the U.S. does not sit at the top of the attack list, Kaspersky researchers believe cybercriminals are heading to North America and the number of Wroba infections will increase.

Hank Schless, senior manager, security solutions at Lookout, said malware delivery attacks like the one Kaspersky reported have become much more common than credential harvesting. He added that according to Lookout data, 88 percent of U.S., consumer phishing attacks so far in 2020 were attempts to deliver malware to a mobile device.

“Trojans like Wroba pose a significant threat to both consumer and enterprise users,” Schless said. “A mobile trojan can be built to access everything on your device and will not discriminate between personal and corporate data.”

Kaspersky recommends following these rules to protect mobile devices:

- Download applications only from official resources.
- If possible, disable the installation of applications from third-party sources in smartphone settings.
- Do not click on suspicious links from unknown senders.
- Install a reliable mobile security solution to protect your device.

References:

- <https://www.scmagazine.com/home/security-news/wroba-mobile-banking-trojan-targets-us-smartphones/>
- <https://threatpost.com/wroba-mobile-banking-trojan-spreads-us/160785/>
- <https://cisomag.eccouncil.org/wroba-trojan/>