Group-IB uncovers Android Trojan named «Gustuff» capable of targeting more than 100 global banking apps, cryptocurrency and marketplace applications

group-ib.com/media/gustuff/

Group-IB, an international company that specializes in preventing cyberattacks, has detected activity of Gustuff a mobile Android Trojan, which includes potential targets of customers in leading international banks, users of cryptocurrency services, popular ecommerce websites and marketplaces. Gustuff has previously never been reported. Gustuff is a new generation of malware complete with fully automated features designed to steal both fiat and crypto currency from user accounts en masse. The Trojan uses the Accessibility Service, intended to assist people with disabilities.

The analysis of Gustuff sample revealed that the Trojan is equipped with web fakes designed to potentially target users of Android apps of top international banks including Bank of America, Bank of Scotland, J.P.Morgan, Wells Fargo, Capital One, TD Bank, PNC Bank, and crypto services such as Bitcoin Wallet, BitPay, Cryptopay, Coinbase etc. Group-IB specialists discovered that Gustuff could potentially target users of more than 100 banking apps, including 27 in the US, 16 in Poland, 10 in Australia, 9 in Germany, and 8 in India and users of 32 cryptocurrency apps.

Initially designed as a classic banking Trojan, in its current version, Gustuff has significantly expanded the list of potential targets, which now includes, besides banking, crypto services and fintech companies' Android programs, users of apps of marketplaces, online stores,

payment systems and messengers, such as PayPal, Western Union, eBay, Walmart, Skype, WhatsApp, Gett Taxi, Revolut etc.

Weapon of mass infection

Gustuff infects Android smartphones through SMS with links to malicious Android Package (APK) file, the package file format used by the Android operating system for distribution and installation of applications. When an Android device is infected with a Gustuff, at the server's command Trojan spreads further through the infected device's contact list or the server database. Gustuff's features are aimed at mass infections and maximum profit for its operators — it has a unique feature — ATS (Automatic Transfer Systems), that autofills fields in legitimate mobile banking apps, cryptocurrency wallets and other apps, which both speeds and scales up thefts.

The analysis of the Trojan revealed that the ATS function is implemented with the help of the Accessibility Service, which is intended for people with disabilities. Gustuff is not the first Trojan to successfully bypass security measures against interactions with other apps' windows using Android Accessibility Service. That being said, the use of the Accessibility Service to perform ATS has so far been a relatively rare occurrence.

After being uploaded to the victim's phone, the Gustuff uses the Accessibility Service to interact with elements of other apps' windows including cryptocurrency wallets, online banking apps, messengers etc. The Trojan can perform a number of actions, for example, at the server's command, Gustuff is able to change the values of the text fields in banking apps. Using the Accessibility Service mechanism means that the Trojan is able to bypass security measures used by banks to protect against older generation of mobile Trojans and changes to Google's security policy introduced in new versions of the Android OS. Moreover, Gustuff knows how to turn off Google Protect; according to the Trojan's developer, this feature works in 70% of cases.

Gustuff is also able to display fake push notifications with legitimate icons of the apps mentioned above. Clicking on fake push notifications has two possible outcomes: either a web fake downloaded from the server pops up and the user enters the requested personal or payment (card/wallet) details; or the legitimate app that purportedly displayed the push notification opens — and Gustuff at the server's command and with the help of the Accessibility Service, can automatically fill payment fields for illicit transactions.

The malware is also capable of sending information about the infected device to the C&C server, reading/sending SMS messages, sending USSD requests, launching SOCKS5 Proxy, following links, transferring files (including document scans, screenshots, photos) to the C&C server, and resetting the device to factory settings.

In order to better protect their clients against mobile Trojans, the companies need to use complex solutions which allow to detect and prevent malicious activity without additional

software installation for end-user. Signature-based detection methods should be complemented with user and application behaviour analytics. Effective cyber defence should also incorporate a system of identification for customer devices (device fingerprinting) in order to be able to detect usage of stolen account credentials from unknown device. Another important element is cross-channel analytics that help to detect malicious activity in other channels.

Pavel Krylov

Head of Secure Bank / Secure Portal

Used mainly outside Russia

Although the Trojan was developed by a Russian-speaking cybercriminal, Gustuff operates exclusively on international markets.

All new Android Trojans offered on underground forums, including Gustuff, are designed to be used mainly outside Russia, and target customers of international companies.
In Russia, after the owners of the largest Android botnets were arrested, the number of daily thefts decreased threefold, Trojans' activity became significantly less widespread, and their developers focused to others markets. However some hackers „patch" (modify) the Trojan samples and reuse it in their attacks on users in Russia.

Rustam Mirkasymov

Group-IB Head of Dynamic Analysis of malware department and threat intelligence expert

Group-IB's Threat Intelligence system first discovered Gustuff on hacker forums in April 2018. According to its developer, nicknamed Bestoffer, Gustuff became the new, updated version of the AndyBot malware, which since November 2017 has been attacking Android phones and stealing money using web fakes disguised as mobile apps of prominent international banks and payment systems. Gustuff is a «serious product for individuals with skills and experience», as advertised by the Trojan's developer. The price for leasing the «Gustuff Bot» was $800 per month. Group-IB Threat Intelligence customers were notified about Gustuff upon discovery. A team of Group-IB analysts continue to research the Trojan.