Cyber Crime Gang Arrested for Infecting Over 1 Million Phones with Banking Trojan

By The Hacker News

Published: 2017-05-23 · Archived: 2026-04-05 19:37:42 UTC

The Russian Interior Ministry announced on Monday the arrest of 20 individuals from a major cybercriminal gang that had stolen nearly $900,000 from bank accounts after infecting over one million Android smartphones with a mobile Trojan called "CronBot."

Russian Interior Ministry representative Rina Wolf said the arrests were part of a joint effort with Russian IT security firm Group-IB that assisted the massive investigation.

The collaboration resulted in the arrest of 16 members of the Cron group in November 2016, while the last active members were apprehended in April 2017, all living in the Russian regions of Ivanovo, Moscow, Rostov, Chelyabinsk, and Yaroslavl and the Republic of Mari El.

Targeted Over 1 Million Phones — How They Did It?

Group-IB first learned of the Cron malware gang in March 2015, when the criminal gang was distributing the Cron Bot malware disguised as Viber and Google Play apps.

The Cron malware gang abused the popularity of SMS-banking services and distributed the malware onto victims' Android devices by setting up apps designed to mimic banks' official apps.

The gang even inserted the malware into fake mobile apps for popular pornography websites, such as PornHub.

Once victims downloaded and installed these fake apps on their devices, the apps added itself to the auto-start and the malware hidden inside them granted the hackers the ability to phish victims' banking credentials and intercept SMS messages containing confirmation codes sent by the bank to verify the transactions.

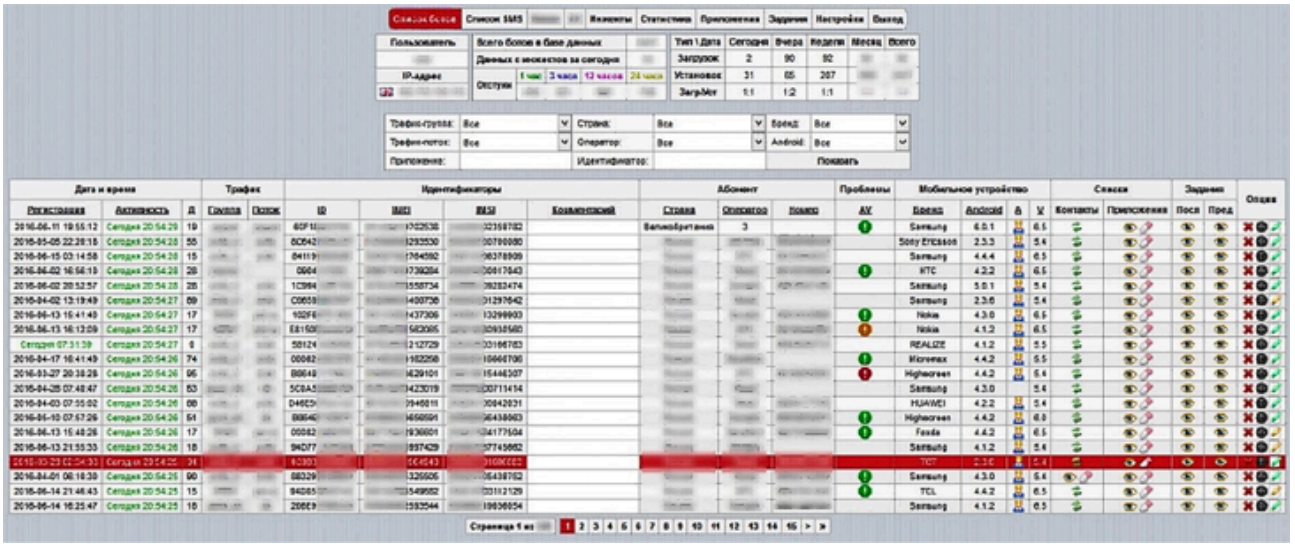
> "After installation, the program added itself to the auto-start and could send SMS messages to the phone numbers indicated by the criminals, upload SMS messages received by the victim to C&C servers, and hide SMS messages coming from the bank," writes Group-IB.

> "The approach was rather simple: after a victim's phone got infected, the Trojan could automatically transfer money from the user's bank account to accounts controlled by the intruders. To successfully withdraw stolen money, the hackers opened more than 6 thousand bank accounts."

The gang usually sent text messages to the banks initiating a transfer of up to $120 to one of their 6,000 bank accounts the group set up to receive the fraudulent payments.

The malware would then intercept the two-step verification codes sent by the bank to confirm the transaction and block the victims from receiving a message notifying them about the transaction.

Cyberthieves Stole $900,000 in the Russia Alone



On April 1, 2016, the gang advertised its Android banking Trojan, dubbed "Cron Bot," on a Russian-speaking forum, giving the Group-IB researchers and Russian authorities a clue to their investigation into the group's operation.

According to the security firm, the group stole approximately 8,000 Rubles (nearly $100) from a victim on an average, fetching a total amount of 50 Million Rubles (almost $900,000) from more than one million victims, with 3,500 unique Android devices infected per day.

After targeting customers of the Bank in Russia, where they were living in, the Cron gang planned to expand its operation by targeting customers of banks in various countries, including the US, the UK, Germany, France, Turkey, Singapore, and Australia.

In June 2016, the gang rented a piece of malware called "Tiny.z" for $2,000 per month, designed to attack customers of Russian banks as well as international banks in Britain, Germany, France, the United States and Turkey, among other countries.

Despite operating only in Russia before their arrest, the gang members had already developed web injections for several of French banks including Credit Agricole, Assurance Banque, BNP Paribas, Banque Populaire, Boursorama, Caisse d'Epargne, Societe Generale and LCL, Group-IB said.

However, before the gang could launch attacks on French banks, the authorities managed to disrupt their operations by making several arrests, including the gang's founder, a 30-year-old resident of Ivanovo, Moscow.

During the raids, the authorities seized computer equipments, bank cards, and SIM cards associated with the criminal gang.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
