Cron has fallen

blog.group-ib.com/cron

Group-IB supports operations to arrest gang
for infecting 1 million smartphones

A black police vehicle, UAZ Patriot, is accelerating, chasing a cherry Renault Logan and forcing it to the roadside. The taxi driver in the Logan seems agitated, frightened even, accelerates quickly while shifting into higher gears. It has gotten dark; both cars speed close to the side of the road sweeping bushes. "Be ready to run," one of the officers warns his colleagues. "He's going to brake and flee over the fence." When the Logan finally stops, the officers act faster: with the entry team jumping out, pulling the passenger from the back seat and laying him face down in the snow.

This taxi passenger is a member of Cron, a hacker group that stole money from bank accounts of Android smartphone users. The hackers infected 3,500 mobile devices per day during the height of their operations. In total, infecting over 1 million devices!
ARREST VIDEO

Androids under attack

Group-IB first learnt about Cron in March 2015: Group-IB's Intelligence system tracked the activity of a new criminal group that was distributing malicious programs named "viber.apk", "Google-Play.apk", "Google_Play.apk" for Android OS on underground forums. The hackers

called this malware "Cron", hence the logic for our naming convention of the group. Cron targeted users of large Russian banks in the Top 50 standing – all of their SMS banking services were under siege during cron's operations.

According to statistics from the Russian Central Bank, 20% of the adult population in the country used mobile banking in Russia. Smartphones have become the new mobile wallet – this trend was capitalized on by cyber criminals. In 2015, 10 new hacker groups started stealing money using mobile Trojans, and the number of incidents tripled!
Trojans for mobile phones and tablets have finally replaced PC Trojans. According to 2015 year-end results, losses of online banking users from attacks employing Android Trojans amounted to over $1 million (61 million rubles).

Why are hackers choosing Android users as a key attack target? Easy. Almost 85% of smartphones run Android OS worldwide making them an attractive target for cyber criminal groups.

It is no longer necessary to be a virus writer to steal money from users of Internet banks – ready-to-use malware can be easily purchased or rented on hacker forums. The Cron organizers had already been convicted of various crimes before their hacker attacks. It comes as no surprise that experienced criminals become hackers. Once Group-IB investigated activity of a hacker who earned up to $20 million per month through thefts in online banking.

Cron's attack scheme

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.

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.
Every day Cron malware attempted to steal money from 50-60 clients of different banks. An average theft was about 8,000 rubles ($100). According to crime investigators, the total damage from Cron's activity amounted to approximately $800 000 (50 million rubles).

The gang applied several infection vectors:

1

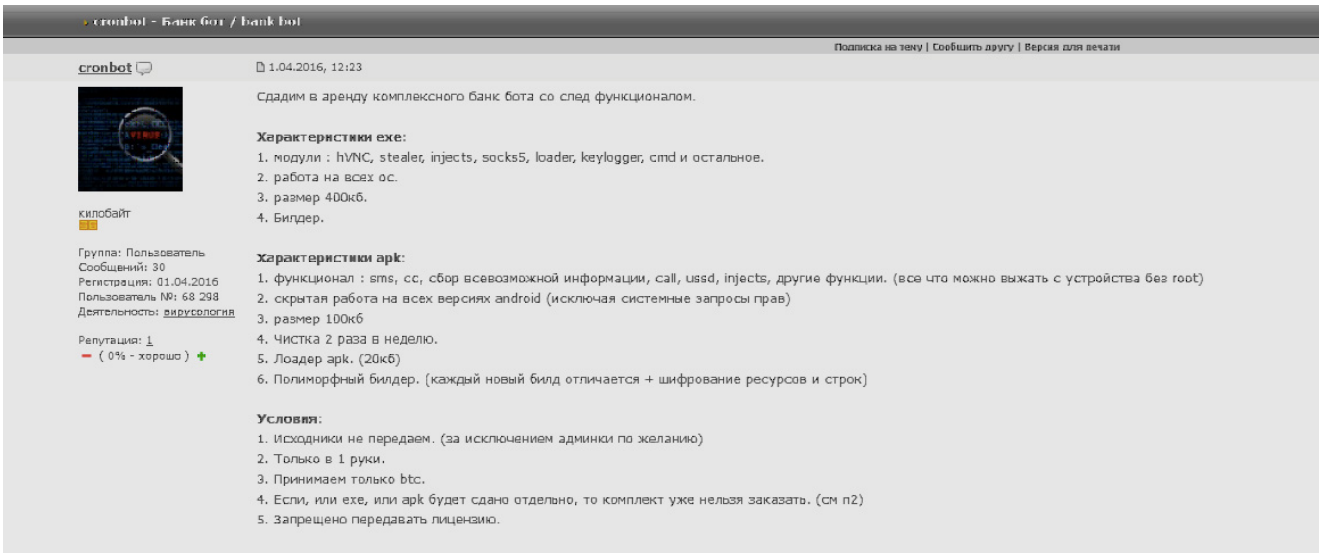
Spam SMS messages with a link to a website infected with the banking Trojan. The message was of the following form: "Your ad is posted on the website ....", or "your photos are posted here." After the user visits the compromised website, the malware will be downloaded on the device, tricking the victim to install it.

2

Infected applications. The victim could install the malicious program on the phone by downloading fake applications masked as legitimate ones. The Trojan is distributed under the guise of such applications as **Navitel; Framaroot; Pornhub; Avito.**

Thus, Cron managed to infect over 1 million mobile devices. The gang infected 3,500 devices on average daily.

In April 2016, an announcement about the lease of a mobile Trojan called **cronbot** appeared on a hacker forum. According to its description, the Trojan had the functionality to intercept SMS messages and calls, send USSD requests, and perform web injections. We assumed that the criminal group decided to recruit a new member to the team, because according to the author of the announcement, they were ready to provide the Trojan to one person only. At the time, the group consisted of the organizers, operators, "cryptors", "traffickers" and money mules.


cronbot - Банк бот / bank bot

Подписка на тему | Сообщить другу | Версия для печати

cronbot

1.04.2016, 12:23

Сдадим в аренду комплексного банк бота со след функционалом.

Характеристики exe:
1. модули : hVNC, stealer, injects, socks5, loader, keylogger, cmd и остальное.
2. работа на всех ос.
3. размер 400кб.
4. Билдер.

Характеристики apk:
1. функционал : sms, cc, сбор всевозможной информации, call, ussd, injects, другие функции. (все что можно выжать с устройства без root)
2. скрытая работа на всех версиях android (исключая системные запросы прав)
3. размер 100кб
4. Чистка 2 раза в неделю.
5. Лоадер apk. (20кб)
6. Полиморфный билдер. (каждый новый билд отличается + шифрование ресурсов и строк)

Условия:
1. Исходники не передаем. (за исключением админки по желанию)
2. Только в 1 руки.
3. Принимаем только btc.
4. Если, или exe, или apk будет сдано отдельно, то комплект уже нельзя заказать. (см п2)
5. Запрещено передавать лицензию.

Килобайт

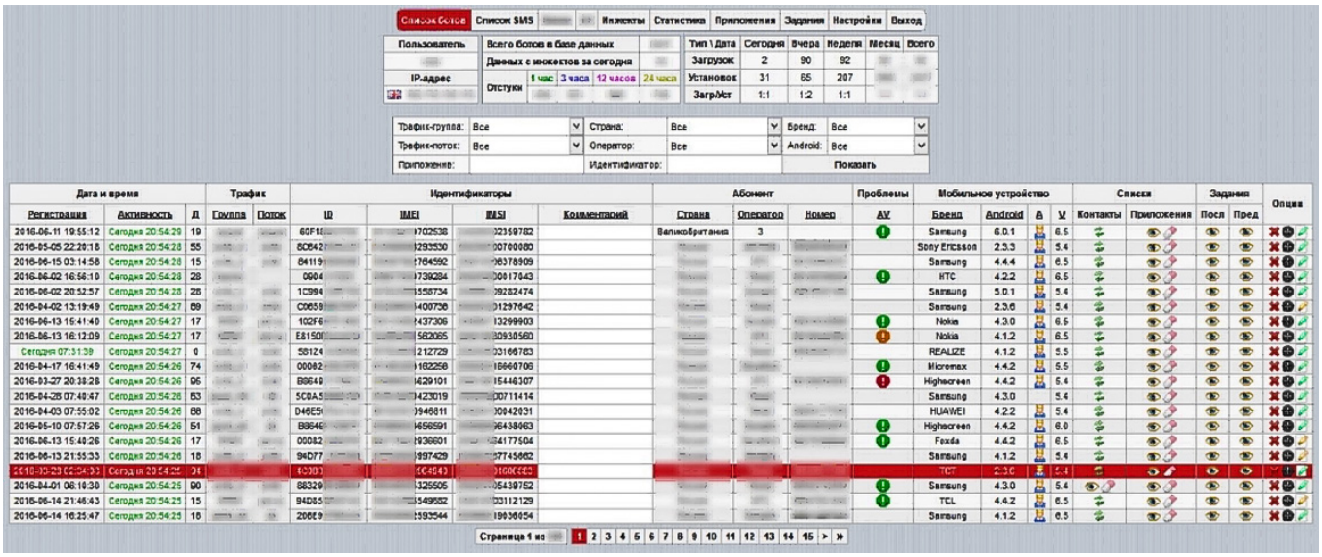
Группа: Пользователь
Сообщений: 30
Регистрация: 01.04.2016
Пользователь №: 68 298
Деятельность: вирусология

Репутация: 1
(0% - хорошо)

Announcement about the cronbot Trojan offered for rent

Plans for France

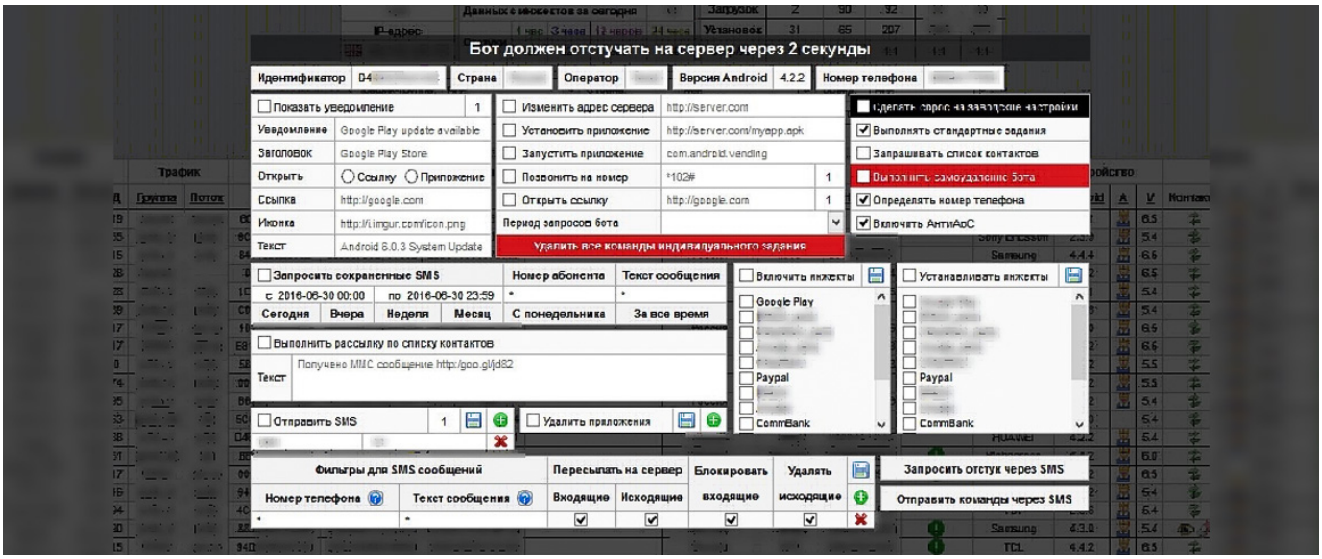
Having earned money in Russia, Cron decided to expand throughout the world. In June 2016 the criminals rented a mobile banking Trojan Tiny.z for $2000 per month. This universal tool has capabilities to attack Android devices of both Russian and international banks' customers.



*Control panel of the **Tiny.z** mobile Trojan*

Group-IB specialists detected Tiny.z in early 2016. According to analysis of the botnet control panel, this is the same panel that was used by the well-known "404" criminal group that actively attacked clients of both Russian and foreign banks. Purportedly, after the arrest of a "404" member named Foxxx in 2015, Cron modified the malicious program.

The malware authors adjusted this program for attacks on banks of Great Britain, Germany, France, the USA, Turkey, Singapore, Australia and other countries. The Trojan scanned the victim's phone for a banking application and displayed a universal window with the icon and name of the bank retrieved from Google Play that prompted the user to enter his personal data.



*Control panel of the **Tiny.z** mobile Trojan*

Cron planned to start their "international activity" with attacks targeting banks of France. They developed special web injections for the following French financial institutions: Credit Agricole, Assurance Banque, Banque Populaire, BNP Paribas, Boursorama, Caisse d'Epargne, Societe Generale and LCL.

However, by November 2016, Russian legal enforcement with support from Group-IB had managed to identify all members of the group and collect digital evidence of the crimes committed. On November 22, 2016, a large-scale operation was carried out in 6 Russian regions: 16 Cron members were detained. The last active member of the group was detained in early April in St. Petersburg.

How to avoid becoming a victim of an Android Trojan

1

Android users are particularly vulnerable to security threats and should be extremely cautious.

Do not click on URLs in emails or social media communications, even when coming from your friends or colleagues. They can be hacked. Only download mobile applications from the official website or app store directly.

2

Keep your smartphone up.

Experts strongly urge you not to root your Android device and to update the firmware in a timely manner, because updates usually contain security patches. Install a modern Internet security solution on your device - this minimizes the risks.

3

Do not hesitate to contact bank specialists for assistance.

In the event of any suspicious activity related your bank account, alleged theft or fraud, immediately contact your bank.