MoneyTaker Hacker Group Steals Millions from US and Russian Banks

bleepingcomputer.com/news/security/moneytaker-hacker-group-steals-millions-from-us-and-russian-banks/

Catalin Cimpanu

By
Catalin Cimpanu

- December 12, 2017
- 08:18 AM
- 0

A cyber-criminal group believed to be operating out of Russian-speaking territories has hit at least 20 banks and financial companies and stolen millions of US dollars in the process.

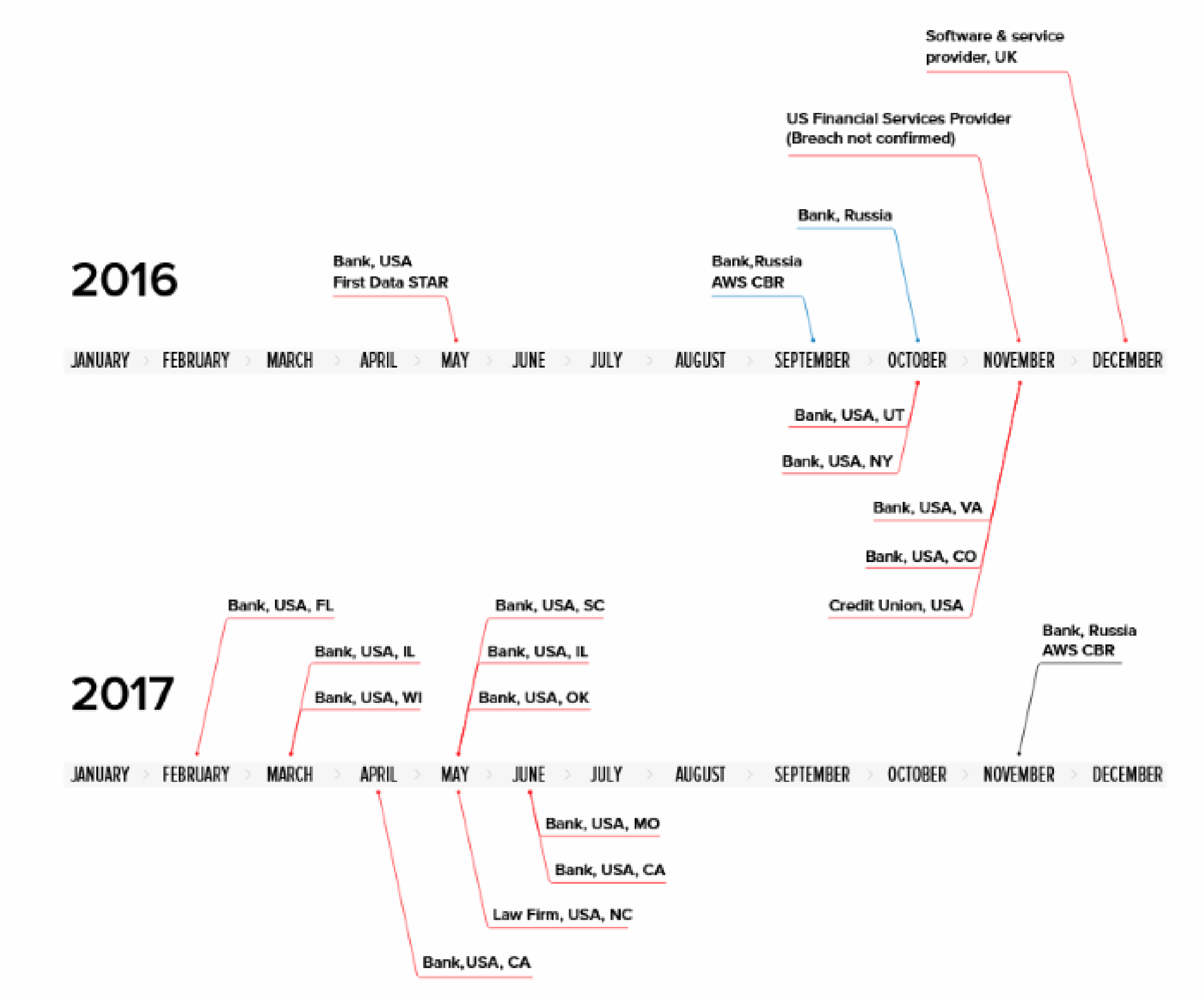
Details of these attacks were first made public in a report published yesterday by Russian cyber-security firm Group-IB. The company believes this is a new group, different from other advanced criminal organizations that have hit the financial sector in the past, like the Carbanak, Cobalt, and Lazarus Group operations.

Researchers named this new group MoneyTaker, based on the name attackers gave to one of their hacking utilities.

MoneyTaker group began operations in 2016

According to Group-IB, MoneyTaker has started operations sometimes in 2016, hitting its first target —a Florida bank— in May 2016.

Since then, the group has hit 14 US banks, a US services provider, a UK company, 3 Russian banks, and one Russian law firm.



The attacks that hit banks have focused on infiltrating inter-banking money transfer and card processing systems such as the First Data STAR Network and the Russian Central Bank's AWS CBR system.

Attackers infiltrated one computer, then spread laterally, gathering any files and credentials they could, hoping to compromise a PC with access to the STAR or CBR networks.

Attackers studied bank networks by stealing documentation files

Evidence collected by Group-IB suggests attackers intentionally searched and stole internal documentation files to learn about bank operations in preparation for future attacks.

In some cases, attackers also stole documents on SWIFT, another inter-banking money transfer system, and files on OceanSystems’ FedLink, a card processing system widely deployed across Latin America.

Now, experts believe Latin America banks and banks utilizing the SWIFT system are in MoneyTaker's crosshairs. The SWIFT team issued a report last month with recommendations on how banks could improve their security.

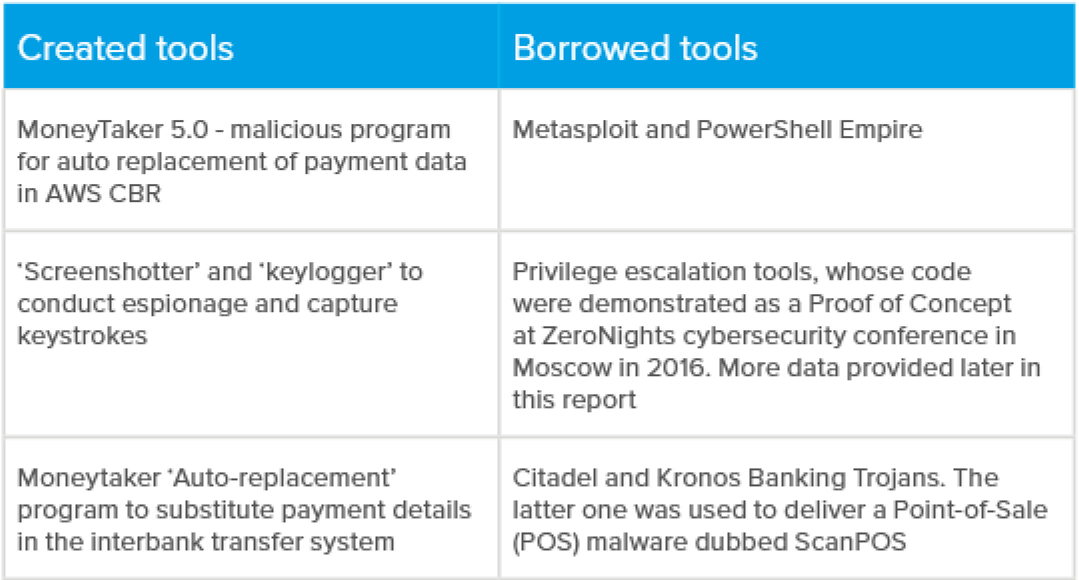
Attackers used fileless malware, legitimate apps

As for the "hacking" part of the MoneyTaker attacks, Group-IB said the hackers' activity was very hard to investigate.

Attackers used common and legitimate apps to carry out malicious operations and used a wide arsenal of malware families. Each hack was different, showing that the group studied each target in fine detail and deployed only tools appropriate for those targets.

The hackers never focused on one bank system alone, and stole money from card processing systems, from ATM networks, and even installed POS (Point-of-Sale) trojans when the hacked organizations weren't financial institutions and had no connection to a large inter-banking network.

According to Group-IB, the group used the MoneyTaker malware framework to hijack inter-banking and card processing operations, the ScanPOS malware for POS systems, custom screenshoting and keylogging tools and the Citadel and Kronos banking trojans to move laterally inside networks. The table below shows tools used by MoneyTaker during their attacks.



Created tools	Borrowed tools
MoneyTaker 5.0 - malicious program for auto replacement of payment data in AWS CBR	Metasploit and PowerShell Empire
'Screenshotter' and 'keylogger' to conduct espionage and capture keystrokes	Privilege escalation tools, whose code were demonstrated as a Proof of Concept at ZeroNights cybersecurity conference in Moscow in 2016. More data provided later in this report
Moneytaker 'Auto-replacement' program to substitute payment details in the interbank transfer system	Citadel and Kronos Banking Trojans. The latter one was used to deliver a Point-of-Sale (POS) malware dubbed ScanPOS

In addition, MoneyTaker also used SSL certificates generated in the name of big brands to sign their malware, used one-time Yandex and Mail.ru email accounts, and employed the overdraft technique for cashing stolen funds with the help of money mules.

Further, the hackers also took the time to delete their entry points, as Group-IB was not able to find the initial infection vector, and used a unique command-and-control server infrastructure that did not deploy any malware unless the download request came from a targeted bank's IP address range.

Group-IB investigators said they forwarded all the data they gather on this group to Europol and Interpol, as they suspect this will not be the last time we hear about MoneyTaker's operations.

Bleeping Computer readers can get their hands on the Group-IB MoneyTaker report from here.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

New RansomHouse group sets up extortion market, adds first victims

U.S. DOJ will no longer prosecute ethical hackers under CFAA

National bank hit by ransomware trolls hackers with dick pics

Chinese ‘Space Pirates’ are hacking Russian aerospace firms

- APT
- Bank
- Cybercrime
- Hack

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: