MoneyTaker: in pursuit of the invisible

By Dmitry Volkov, CEO of Group-IB

Archived: 2026-05-01 02:11:24 UTC

In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group. **Get the report**

Although the group has been successful at targeting a number of banks in different countries, to date, they have gone unreported. In addition to banks, the MoneyTaker group has attacked law firms and also financial software vendors. In total, Group-IB has confirmed 20 companies as MoneyTaker victims, with 16 attacks on US organizations, 3 attacks on Russian banks and 1 in the UK.

By constantly changing their tools and tactics to bypass antivirus and traditional security solutions and most importantly carefully eliminating their traces after completing their operations, the group has largely gone unnoticed.

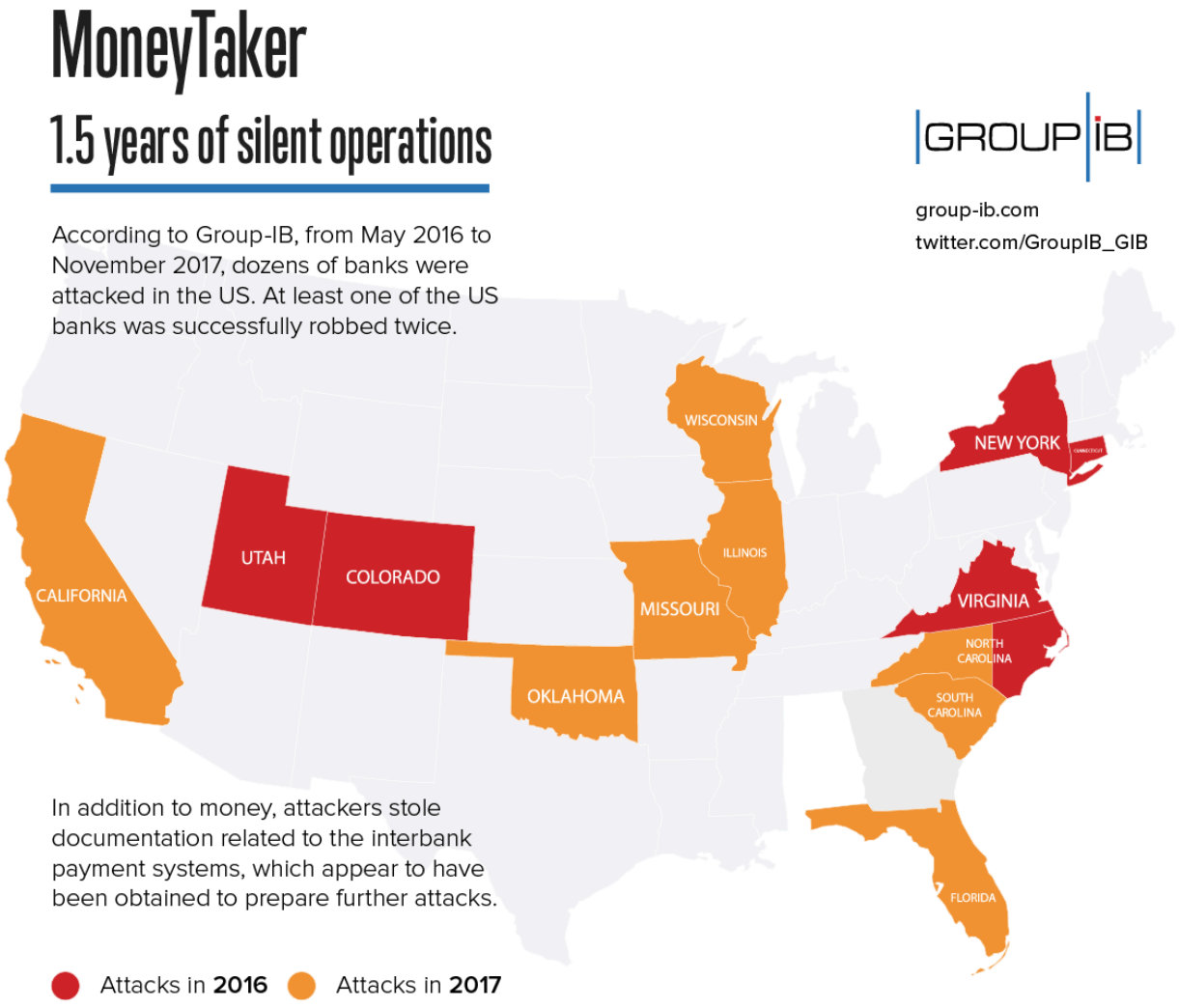
"MoneyTaker uses publicly available tools, which makes the attribution and investigation process a non-trivial exercise. In addition, incidents occur in different regions worldwide and at least one of the US Banks targeted had documents successfully exfiltrated from their networks, twice. Group-IB specialists expect new thefts in the near future and in order to reduce this risk, Group-IB would like to contribute our report identifying hacker tools, techniques as well as indicators of compromise we attribute to MoneyTaker operations".

MoneyTaker attacks: past and future

The first attack in the US that Group-IB attributes to this group was conducted in the spring of 2016: money was stolen from the bank by gaining access to First Data's "STAR" network operator portal. Since that time, the group attacked companies in California, Utah, Oklahoma, Colorado, Illinois, Missouri, South Carolina, North Carolina, Virginia and Florida.

In 2016, Group-IB identified 10 attacks conducted by **MoneyTaker**; 6 attacks on **banks in the US**, 1 attack on **a US service provider**, 1 attack on **a bank in the UK** and 2 **attacks on Russian banks**. Only one incident involving a Russian bank was promptly identified and prevented that is known to Group-IB.

In 2017, the number of attacks has remained the same with 8 US banks, 1 law firm and 1 bank in Russia being targeted. The geography, however, has narrowed to only the USA and Russia.



Connections between incidents

Using the Group-IB Threat Intelligence system, Group-IB researchers have discovered connections between all 20 incidents throughout 2016 and 2017. Connections were identified not only in the tools used, but also the distributed infrastructure, one-time-use components in the attack toolkit of the group and specific withdrawal schemes – using unique accounts for each transaction. Another distinct feature of this group is that they stick around after the event, continuing to spy on a number of impacted banks and sending corporate emails and other documents to Yandex and Mail.ru free email services in the first.last@yandex.com format.

Important findings that enabled Group-IB to discover the links between crimes include privilege escalation tools compiled based on codes presented at the Russian cybersecurity conference ZeroNights 2016. Also, in some incidents, hackers used the infamous Citadel and Kronos banking Trojans. The latter was used to deliver Point-of-Sale (POS) malware dubbed ScanPOS.

Group 1	Group 2	Group 3
17 incidents in US and UK organizations. In the majority of instances, hackers used the same C&C server to control the initial part of their attacks. In some cases, we saw a similar use of the infrastructure from which remote connections were performed using LogMeIn.	2 incidents occurred in Russia in the autumn of 2016. The two attacks occurred at the same time; in both cases Meterpreter was used to attack the same target – servers of the Russian interbank transfer system (AWS CBR).	1 incident in Russia in the autumn of 2017. The attack was conducted on the AWS CBR using Meterpreter.

Common features of Groups 1-3

- Metasploit used to infiltrate corporate networks
- SSL certificates generated using popular brands to protect traffic between Meterpreter and C&C
- Russian-speaking attackers
- Own developers who create unique tools
- Modification of the malicious code during attack
- Covering tracks of the initial infection vector
- Setting up forwarding corporate emails to Yandex and Mail.ru, free mail services.

Connections between incidents

MoneyTaker: arsenal for attacks

Group-IB reports that **MoneyTaker uses both borrowed and their own self-written tools**. For example, to spy on bank operators they developed an application with ‘screenshot’ and ‘keylogger’ capabilities. This program is designed to capture keystrokes, take screenshots of the user’s desktop and get contents from the clipboard. The application is compiled in Delphi and contains 5 timers: functions of the application (such as taking screenshots, capturing keystrokes, disabling itself) are executed once the timer triggers. To circumvent antivirus and automated sample analysis, hackers again used ‘security measures’: they implemented the anti-emulation function in the timer code.

In an attack on a Russian bank through the AWS CBR, hackers used a tool called MoneyTaker v5.0, which the group has been named after. Each component of this modular program performs a certain action: searches for payment orders and modifies them, replaces original payment details with fraudulent ones, and then erases traces. The success of replacement is due to the fact that at this stage the payment order has not yet been signed, which will occur after payment details are replaced. In addition to hiding the tracks, the concealment module again substitutes the fraudulent payment details in a debit advice after the transaction back with the original ones. This means that the payment order is sent and accepted for execution with the fraudulent payment details, and the responses come as if the payment details were the initial ones. This gives cybercriminals extra time to mule funds before the theft is detected.

Created tools	Borrowed tools
MoneyTaker 5.0 – malicious program for auto replacement of payment data in AWS CBR	Metasploit и 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

Leaving no trace behind

To conduct targeted attacks, **MoneyTaker use a distributed infrastructure that is difficult to track**. A unique feature of the infrastructure is a persistence server, which delivers payloads only to victims with an IP addresses in MoneyTaker’s whitelist.

To control the full operation, MoneyTaker uses a Pentest framework Server. On it, the hackers install a legitimate tool for penetration testing – **Metasploit**. After successfully infecting one of the computers and gaining initial access to the system, the attackers perform reconnaissance of the local network in order to gain domain administrator privileges and eventually consolidate control over the network. Hackers use Metasploit to conduct all these activities: network reconnaissance, search for vulnerable applications, exploit vulnerabilities, escalate systems privileges, and collect information.

The group uses ‘fileless’ malware only existing in RAM and is destroyed after reboot. To ensure persistence in the system MoneyTaker relies on PowerShell and VBS scripts – they are both difficult to detect by antivirus and easy to modify. In some cases, they have made changes to source code ‘on the fly’ – during the attack.

After successful infection, they carefully erase malware traces. However, when investigating an incident in Russia, we managed to discover the initial point of compromise: hackers penetrated the bank’s internal network by gaining access to the home computer of the bank’s system administrator.

In addition, **to protect C&C communications from being detected by security teams, MoneyTaker employs SSL certificates generated using names of well-known brands**: Bank of America, Federal Reserve Bank, Microsoft, Yahoo, etc.), instead of filling the fields out randomly. In the US, they used the LogMeIn Hamachi solution for remote access.

Attacks on card processing

The first attack on card processing that Group-IB specialists attribute to this group was conducted in May 2016. Having gained access to the bank network, the attackers compromised the workstation of First Data’s STAR

network portal operators, making the changes required and withdrawing the money. In January 2017, the attack was repeated in another bank.

The scheme is extremely simple. **After taking control over the bank's network, the attackers checked if they could connect to the card processing system.** Following this, they legally opened or bought cards of the bank whose IT system they had hacked. Money mules – criminals who withdraw money from ATMs – with previously activated cards went abroad and waited for the operation to begin. After getting into the card processing system, the attackers removed or increased cash withdrawal limits for the cards held by the mules. They removed overdraft limits, which made it possible to overdraw even with debit cards. Using these cards, the mules withdrew cash from ATMs, one by one. The average loss caused by one attack was about $500,000 USD.
