Metel Bank Robbers Borrowing from APT Attacks

By Michael Mimoso

Published: 2016-02-08 · Archived: 2026-04-05 17:40:34 UTC

At the Security Analyst Summit, Kaspersky Lab researchers unveiled three cybercrime outfits—Metel, GCMAN, and Carbanak 2.0—targeting Russian banks with APT-style tactics.

TENERIFE, Spain— Many bank robbers long ago dropped the stick-up man persona in favor of a keyboard and a reliable password-stealing Trojan.

Banking malware, however, may soon not be good enough for the bad guys. More and more are copycatting the techniques deployed by advanced hackers to steal millions of dollars from banks and other financial institutions.

Today at the Security Analyst Summit, researchers from Kaspersky Lab Global Research & Analysis Team unveiled details on two new criminal operations that have borrowed heavily from targeted nation-state attacks, and also shared an update on a resurgent Carbanak gang, which last year, it was reported, had allegedly stolen upwards of $1 billion from more than 100 financial companies.

The heaviest hitter among the newly discovered gangs is an ongoing campaign, mostly confined to Russia, known as Metel. This gang targets machines that have access to money transactions, such as call center and support machines, and once they are compromised, the attackers use that access to automate the rollback of ATM transactions. As the attackers empty ATM after ATM—Metel was found inside 30 organizations—the balances on the stolen accounts remained untouched.

Kaspersky Lab said one Russian bank lost millions of rubles in a single night.

“The bank’s clients were withdrawing from ATMs belonging to other banks and were able to cash out huge sums of money while the balances remained untouched. It was a surprise for the victim bank to hear from other banks when they tried to recoup the money withdrawn from their ATMs.”

Kaspersky Lab added that it was not able to share specifics about the banks involved because of an ongoing law enforcement investigation. Indicators of compromise were released today on Securelist.com.

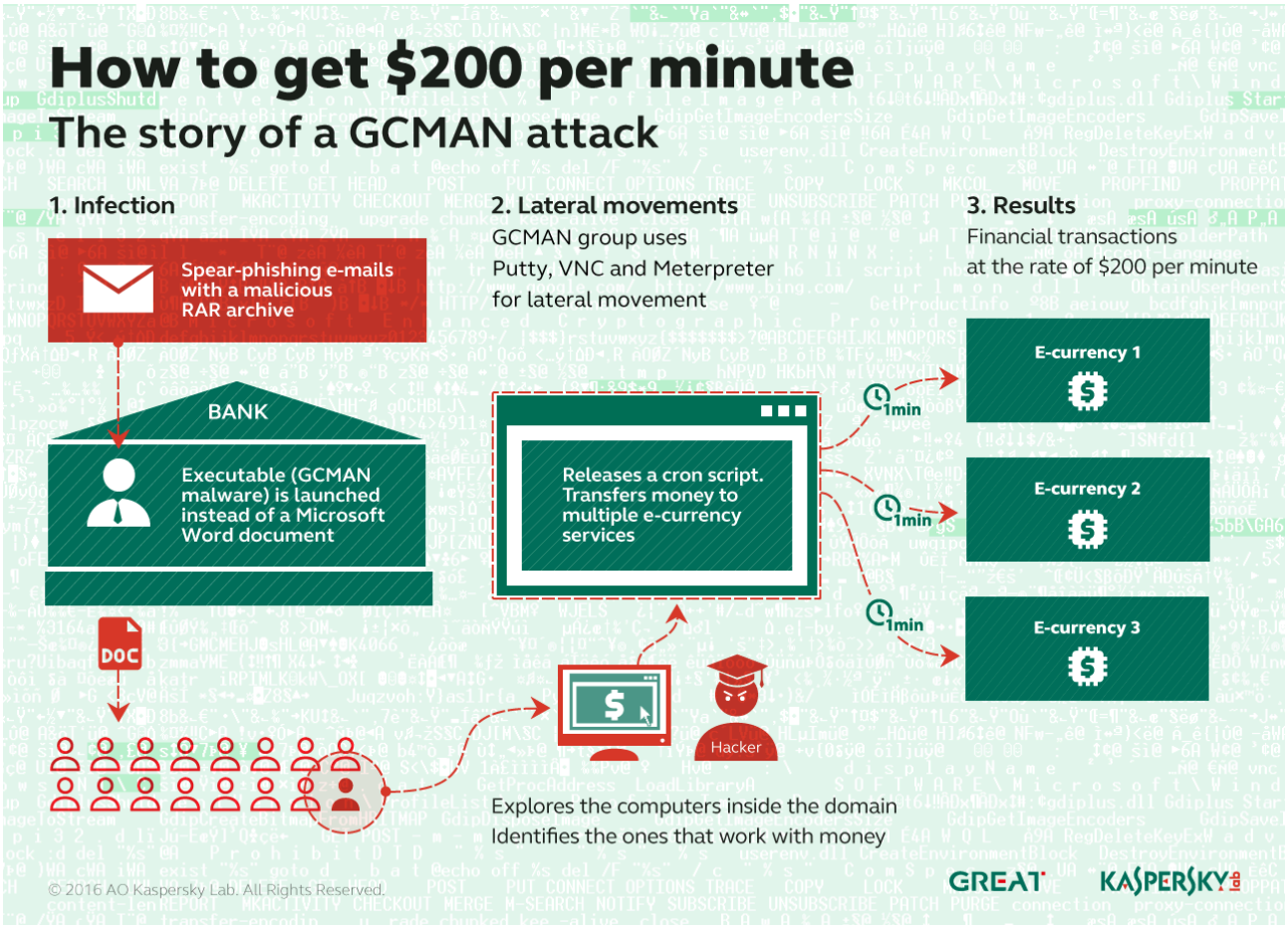
Metel, the Russian word for blizzard, burrows its way into a financial organization using cleverly crafted spear phishing emails laced with malware, or luring victims to sites hosting the Niteris exploit kit. The malware steals system information including process lists and screenshots, sending it to the attackers who evaluate whether the infected machine is interesting enough load the remainder of the Metel malware package.

The malware contains more than 30 modules—some homemade, some taken from publicly available sources. The attackers also use legitimate pen-testing tools such as mimikatz, which is freely available and used by analysts to extract plaintext passwords, hashes, PIN codes and Kerberos tickets from the memory of Windows machines.

Using this stolen data, the attackers are available to pivot internally, stealing credentials until they landed on a domain controller. With the reins of a domain controller, the attackers could extend their reach onto any machine.

“Our investigations revealed that the attackers drove around in cars in several cities in Russia, stealing money from ATMs belonging to different banks,” Kaspersky Lab said in a report published today. “With the automated rollback the money was instantly returned to the account, when the cash has already been dispensed from the ATM. The group worked exclusive at nights, emptying ATM cassettes at several locations.”

The second group unveiled today is known as GCMAN, so-called because the malware is based on code compiled on the GCC compiler. It too has adopted some APT-style techniques to pull off stealthy attacks, some without the use of malware, just with legitimate pen-testing tools, including VNC, Putty and Meterpreter. These tools were used to pivot inside the compromised network—initial compromises were carried out via spear-phishing and a malicious RAR archive disguised as a Word document—until they had access to computers used to transfer money to e-currency services without alerting other detection systems inside the bank.



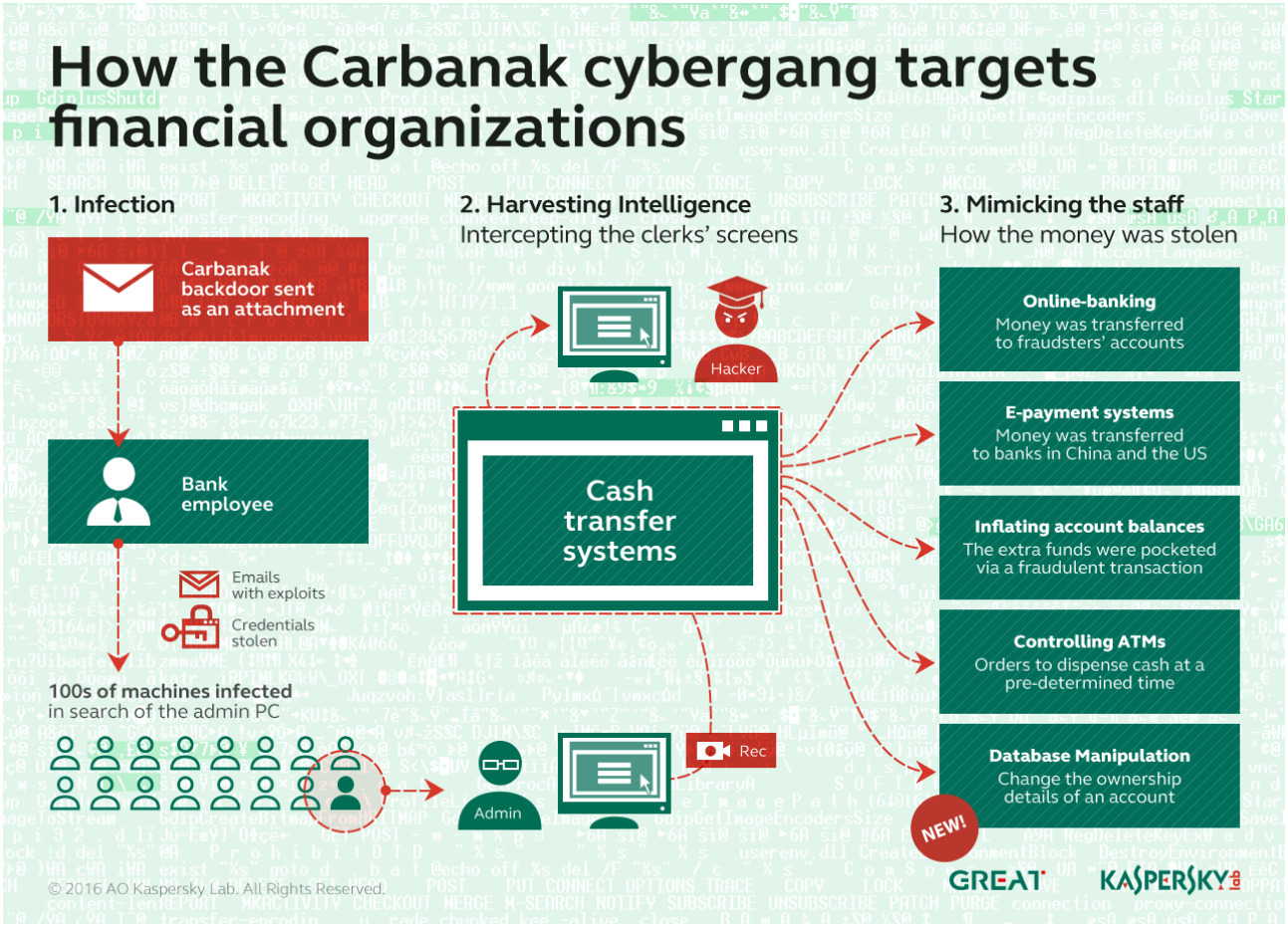
Researchers at Kaspersky said that in one attack, the criminals had access to the network for 18 months before stealing any money. Once they did, they were transferring $200 payments per minute using the CRON scheduler to execute malicious scripts and move money to a money-mule account. Those transaction orders were sent to an upstream payment gateway, Kaspersky Lab said, and were never logged by the bank’s internal systems.

“The group used an MS SQL injection in commercial software running on one of bank’s public web services, and about a year and a half later, they came back to cash out. During that time they poked 70 internal hosts,

compromised 56 accounts, making their way from 139 attack sources (TOR and compromised home routers)," Kaspersky Lab said in its report today. "We discovered that about two months before the incident, someone was trying different passwords for an admin account on a banking server. They were really persistent. They were doing it only on Saturdays, only three tries per week, all in an effort to stay under the radar."

After Carbanak had been outed a year ago, researchers believed the criminals had closed up shop. But last September, researchers at CSIS in Denmark spotted new Carbanak samples. Four months later, Kaspersky said it found Carbanak samples inside a telecommunications company and a financial organization, confirming the gang was still in business.

"One interesting new characteristic of Carbanak 2.0 is a different victim profile," Kaspersky Lab said in its report. "The group has moved beyond banks and is now targeting budgeting and accounting departments in any organization interesting to them with the same APT-style tools and techniques."



The criminals behind Carbanak used the access they had to computers inside one organization to change ownership data from the rightful owners to a money mule under their control.

Carbanak, too, covets domain controllers in order to move money and data off networks to money mule accounts.

"The information was modified to display the passport info and name of a money mule as a shareholder of the company, and subsequent attempts were made to prove that the hacking group's accomplice was co-owner of a major corporate entity," Kaspersky Lab said in its report.
