

APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks

By GReAT

Published: 2016-02-08 · Archived: 2026-04-05 14:09:46 UTC



Introduction

In late 2014, Kaspersky Lab researchers [made a worrying prediction](#): financially-motivated cyber-criminals would adopt sophisticated tactics and techniques from APT groups for use in bank robberies.

Just a few months later, in February 2015, we [announced the discovery of Carbanak](#), a cyber-criminal gang that used custom malware and APT techniques to steal millions of dollars while infecting hundreds of financial institutions in at least 30 countries.

Since then, we have seen an increase in these covert, APT-style attacks that combine the use of reconnaissance, social engineering, specialized malware, lateral movement tools and long-term persistence to steal money from financial institutions (particularly ATMs and money transfer systems).

In summer 2015, a #bank in #Russia lost millions of rubles in a one night #bankingAPT #TheSAS2016

[Tweet](#)

Today at the Security Analyst Summit ([SAS 2016](#)), Kaspersky Lab is announcing the discovery of two new gangs engaged in APT-style bank robberies – Metel and GCMAN – and the reemergence of the Carbanak group with new targets in its sights.

In 2015, Kaspersky Lab researchers conducted Incident Response for 29 organizations located in Russia and infected by these three groups.

Due to the active nature of law enforcement investigations and non-disclosure agreements with victim organizations, Kaspersky Lab cannot provide extensive details of the attacks. Kaspersky Lab is releasing crucial Indicators of Compromise (IOCs) and other data to help organizations search for traces of these attack groups in their corporate networks (*see below*).

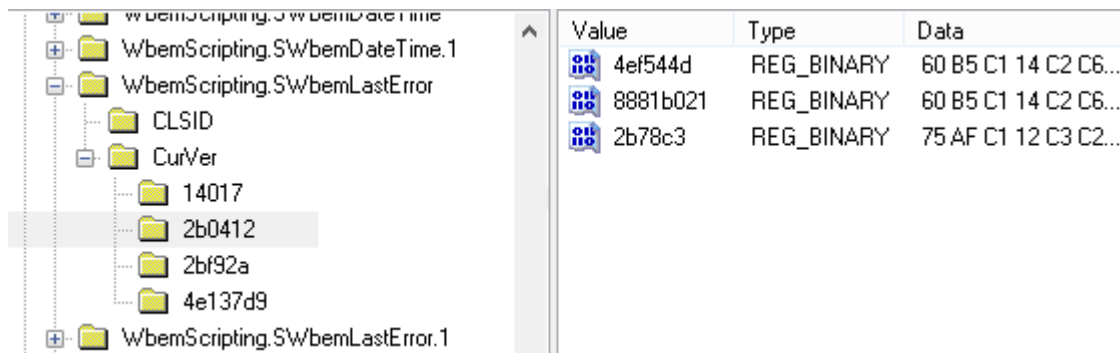
The story of Metel – ATM balance rollbacks

In summer 2015, a bank in Russia discovered it had lost millions of rubles in a single night through a series of strange financial transactions. The bank’s clients were making withdrawals from ATMs belonging to other banks and were able to cash out huge sums of money while their balances remained untouched. The victim bank didn’t realize this until it tried to recoup the money withdrawn from the other banks’ ATMs.

During our incident response, we discovered the solution to this puzzle: Metel, a modular malware program also known as Corkow.

The malware, used exclusively by the Metel group, infected the bank’s corporate network via e-mail and moved laterally to gain access to the computers within the bank’s IT systems.

Having gained access to the bank operator’s money-processing system, the gang pulled off a clever trick by automating the rollback of ATM transactions. This meant that money could be stolen from ATM machines via debit cards while the balance on the cards remained the same, allowing for multiple transactions at different ATM machines.



Encrypted configuration for Metel malware plugins

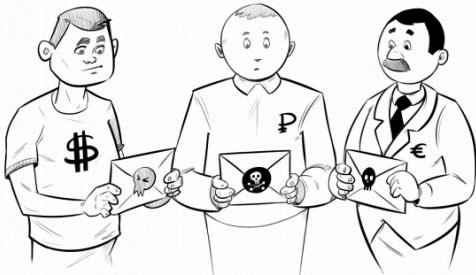
METEL GROUP - ATTACK STAGES

THE ATTACK BEGINS



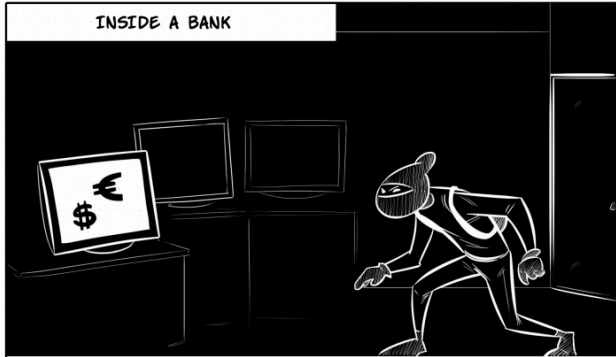
THE CYBERCRIMINAL SPREADS SPEAR-PHISHING E-MAILS AND A NITERIS EXPLOIT PACK. HE ATTACKS A LARGE GROUP OF VICTIMS AND GATHERS INFORMATION ABOUT THEM.

CHOOSE INTERESTING TARGETS



BANKS, FINANCIAL INSTITUTIONS

INSIDE A BANK



HE SEARCHES FOR THE MACHINES THAT CONTROL FINANCES



NOW HE CAN CONTROL AND MANAGE MONEY TRANSACTIONS IN AAA BANK

*ALL NAMES APPEARING IN THIS CHART ARE FICTITIOUS. ANY RESEMBLANCE IS PURELY COINCIDENTAL.

Our investigations revealed that the attackers drove around several cities in Russia, stealing money from ATMs belonging to different banks. With the automated rollback in place the money was instantly returned to the account after the cash had been dispensed from the ATM. The group worked exclusively at night, emptying ATM cassettes at several locations.

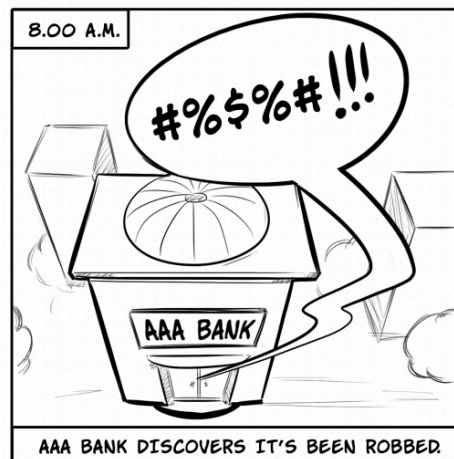
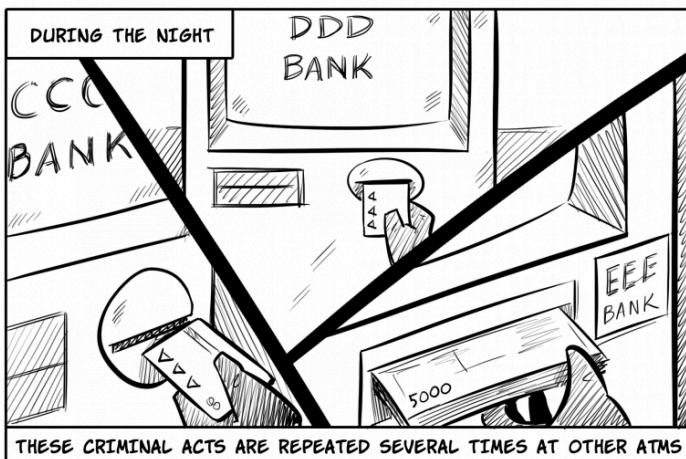
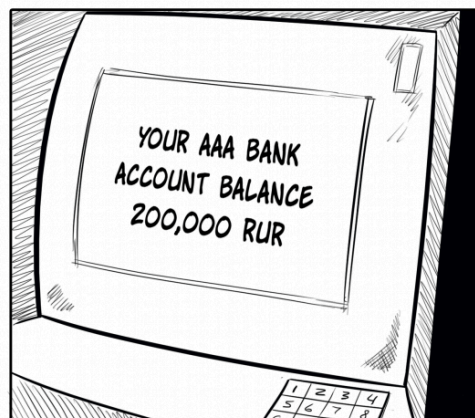
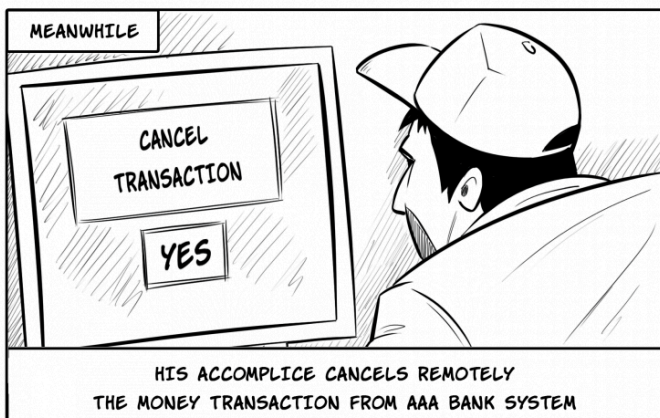
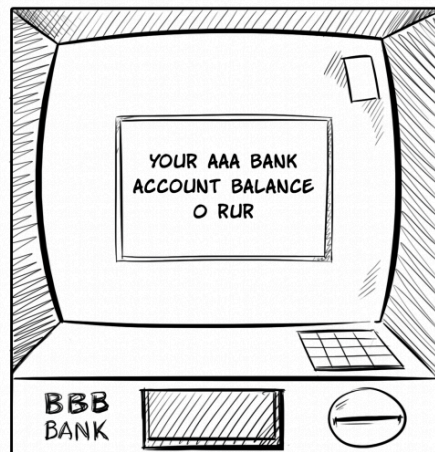
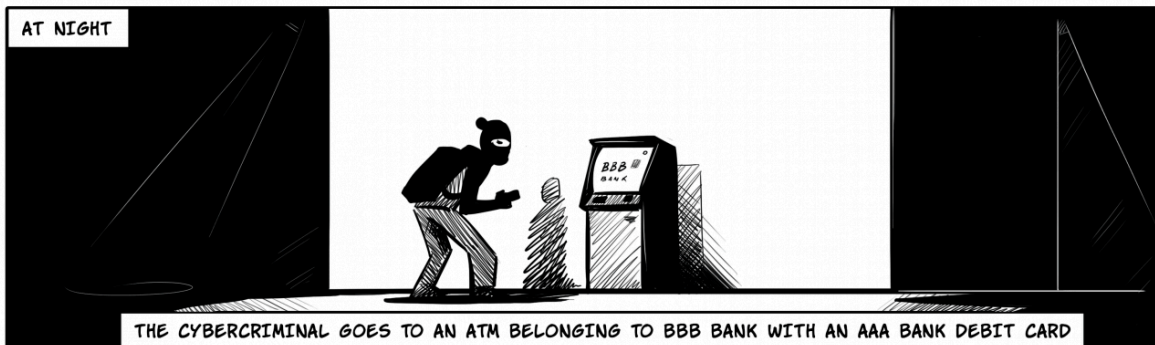
GCMAN group planted cron script into #bank server, stealing \$200/min #bankingAPT #TheSAS2016

[Tweet](#)

In all, we discovered Metel in more than 30 financial institutions, but Kaspersky Lab's incident responders were able to clean the networks before any major damage could be done. It is highly likely that this threat is far more widespread and we urge financial institutions around the world to scan their networks for signs of the Metel malware.

The Metel criminal group is still active. At the moment, we don't have any information about any victims outside Russia.

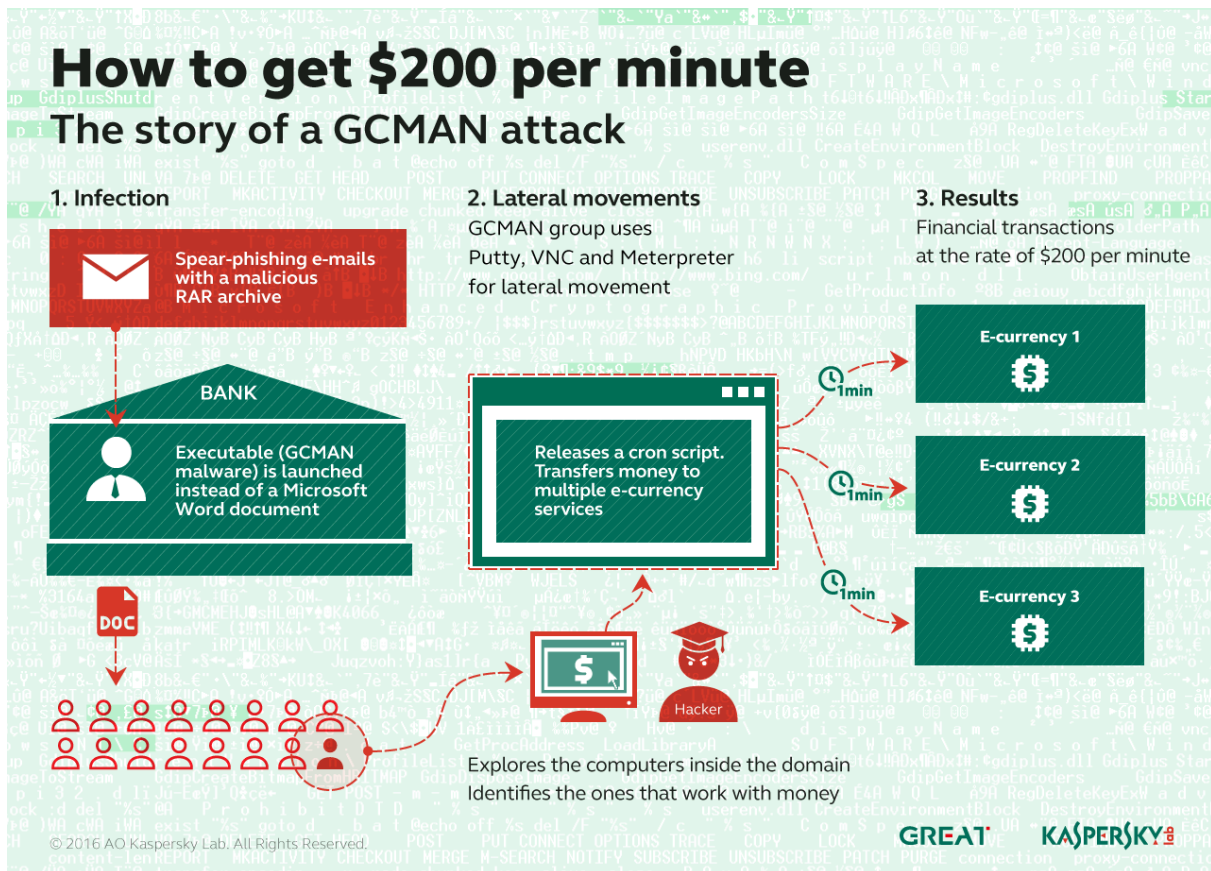
METEL: KEEP CALM AND ROLL BACK THE TRANSACTIONS



*ALL NAMES APPEARING IN THIS CHART ARE FICTITIOUS. ANY RESEMBLANCE IS PURELY COINCIDENTAL.

A second group, which we call GCMAN because the malware is based on code compiled on the GCC compiler, emerged recently using similar techniques to the Metel Group to infect banking institutions and attempt to transfer money to e-currency services.

The initial infection mechanism is handled by spear-phishing financial institution targets with e-mails carrying a malicious RAR archive to. Upon opening the RAR archive, an executable is started instead of a Microsoft Word document, resulting in infection.



Once inside the network, the GCMAN group uses legitimate and penetration testing tools such as Putty, VNC, and Meterpreter for lateral movement. Our investigation revealed an attack where the group then planted a cron script into bank’s server, sending financial transactions at the rate of \$200 per minute. A time-based scheduler was invoking the script every minute to post new transactions directly to upstream payment processing system. This allowed the group to transfer money to multiple e-currency services without these transactions being reported to any system inside the bank.

```
● 528         mc({(int)&text, "none\n", 5u);
529     }
● 530     pass = "p4ssw0rd";
● 531     fflush(&iob[1]);
● 532     text_1 = text;
● 533     char_text = (char *)text;
● 534     bb = *(_BYTE *)text;
● 535     if ( *(_BYTE *)text )
536     {
537         do
538         {
● 539             v81 = *pass;
● 540             if ( !*pass )
541             {
● 542                 v81 = aP4ssw0rd[0];
● 543                 pass = "p4ssw0rd";
544             }
● 545             ++pass;
● 546             *char_text++ = (v81 + -128) ^ bb;
● 547             bb = *char_text;
```

Decompiled code of GCMAN malware that is responsible for connecting to CnC

In a stroke of luck, the financial institutions discovered the suspicious activity on their network in time to neutralize the threat and cancel the transactions.

One interesting observation is that the real attack happened approximately 18 months before it was discovered. 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).

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 but doing it only three times a week and then only on Saturdays, in an effort to stay under the radar.

Kaspersky Lab’s research team responded to three financial institutions in Russia that were infected with the GCMAN malware. It is likely that this threat is far more widespread and we urge banks to sweep their networks for signs of this cyber-criminal group.

Carbanak 2.0: new targets beyond banks

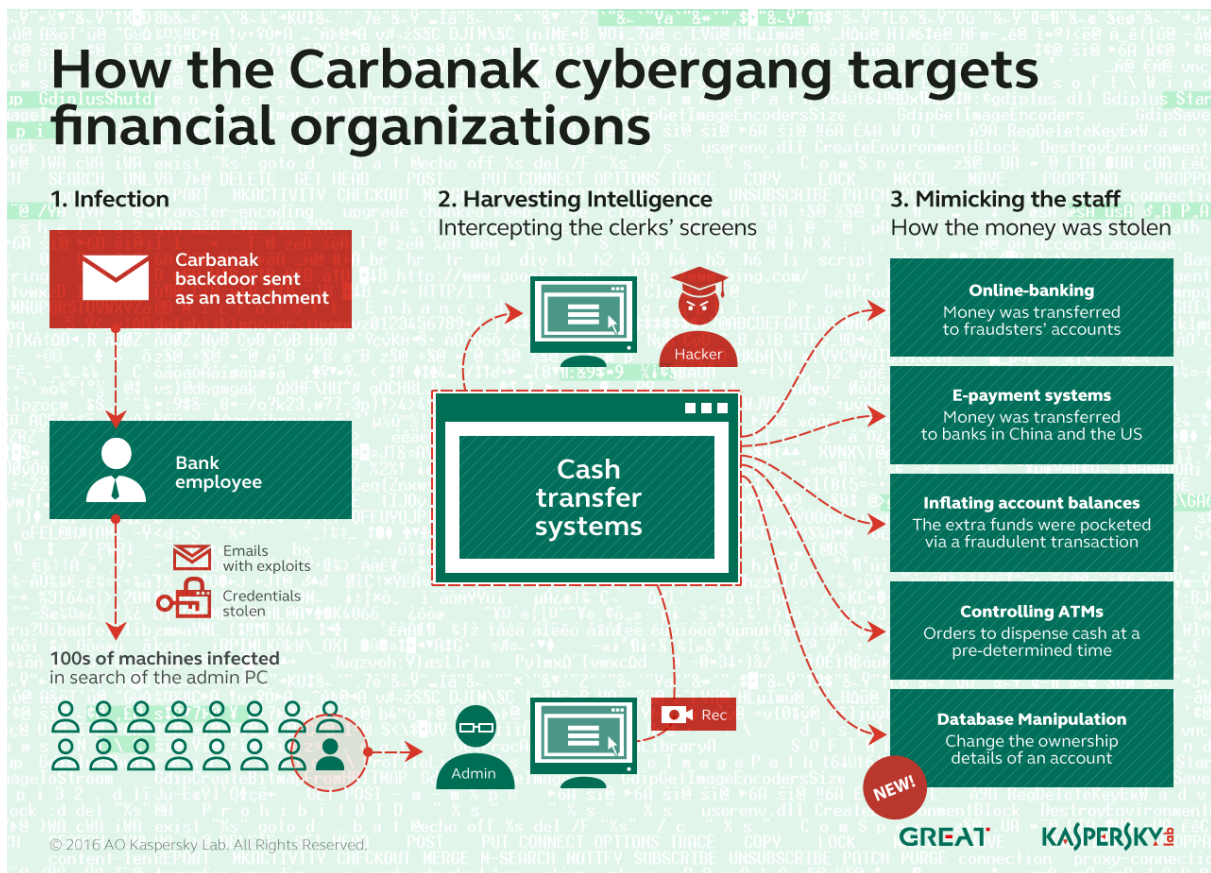
After [our exposure of the Carbanak group](#) exactly a year ago, the group disappeared for about five months, leading us to believe that the operation was disbanded. However, in September last year, our friends at [CSIS published a blog detailing a new Carbanak variant](#) affecting one of its customers.

In December 2015, we confirmed that the group was still active. Kaspersky Lab discovered signs of Carbanak in two institutions – a telecommunications company and a financial institution.

1	09/16/2015	20:27:40.231	81	c:\perflogs\146\svchost.exe
2	09/18/2015	08:34:16.189	187	c:\perflogs\226\svchost.exe
3	09/16/2015	18:48:05.415	189	c:\perflogs\239.exe
4	09/16/2015	17:17:13.979	191	c:\perflogs\netscan.exe
5	09/16/2015	10:38:44.625	82	c:\perflogs\procdump.exe
6	09/16/2015	10:39:52.917	209	c:\perflogs\procdump64.exe
7	09/16/2015	10:37:43.111	79	c:\perflogs\psexec.exe
8	09/18/2015	08:34:16.189	188	c:\perflogs\svchost.exe
9	09/16/2015	20:27:40.231	190	c:\perflogs\svchost.exe
10	09/16/2015	19:17:35.043	205	c:\perflogs\team.exe

Executable files founded in SHIM during Carbanak incident response

One interesting characteristic of Carbanak 2.0 is a different victim profile. The group has moved beyond banks and is now targeting the budgeting and accounting departments in any organization of interest to them, using the same APT-style tools and techniques.



In one remarkable case, the Carbanak 2.0 gang used its access to a financial institution that stores information about shareholders to change the ownership details of a large company. The information was modified to name a money mule as a shareholder of the company, displaying their IDs. It's unclear how they wanted to make use of this information in future.

#Carbanak gang is now targeting budgeting & accounting departments #bankingAPT #TheSAS2016

[Tweet](#)

Kaspersky Lab products successfully detect and block the malware used by the Carbanak 2.0, Metel and GCMAN threat actors with the following detection names:

- Trojan-Dropper.Win32.Metel
- Backdoor.Win32.Metel
- Trojan-Banker.Win32.Metel
- Backdoor.Win32.GCMan
- Backdoor.Win64.GCMan
- Trojan-Downloader.Win32.GCMan
- Trojan-Downloader.Win32.Carbanak
- Backdoor.Win32.Carbanak

Kaspersky Lab urges all organizations to carefully scan their networks for the presence of Carbanak, Metel and GCMAN and, if detected, to disinfect their systems/computers/networks and report the intrusion to law enforcement.

All this information has been made available to customers of our [APT intelligence reporting service](#) and they received the indicators of compromise and context information as soon as they became available.

Indicators of Compromise (IOC) are available here:

[Metel](#)

[GCMAN](#)

[Carbanak 2.0](#)

For more about the measures to be taken against these Bank Busters and similar offensives, read [this article](#) in the Kaspersky Business Blog.

SUBSCRIBE NOW FOR KASPERSKY LAB'S APT INTELLIGENCE REPORTS

Source: <https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/>