Metel – ATM balance rollbacks

By Kaspersky

Published: 2017-09-13 · Archived: 2026-04-05 23:44:20 UTC

VIRUS DEFINITION

Virus Type: Advanced Persistent Threat, Trojan, Malware.

What is Metel?

Metel is a banking Trojan (also known as Corkow) discovered in 2011 when it was used to attack users of online banking services. In 2015, the Metel gang began to target banks and financial institutions directly.

What it can do?

After the infection stage, criminals move laterally with the help of legitimate and pentesting tools, stealing passwords from their initial victims (entry point) to gain access to the computers within the organization that have access to money transactions. With this level of access, the gang has been able to pull off a clever trick by automating the rollback of ATM transactions. This means that money can be stolen from ATM machines via debit cards while the balance on the cards remains the same, allowing for multiple transactions at different ATM machines.

Who are the victims of its attacks?

The victims we observed are limited to banks and financial institutions.

Their major targets inside these organizations are:

- In banks – the online banking database: criminals can play with the balance on cards.
- In companies - a computer in the accounting department with a Client-Bank system that has access to money transactions. Criminals can replace the banking details of a real transaction or manually process fraudulent transactions.
- Servers of Payment APIs: there is software that indicates how much money should be transferred to a specific phone number. Criminals can play with this API making it think that a client is transferring 10,000 rubles (around $120) to a large number of phone numbers.

Am I at risk?

So far Kaspersky Lab researchers have identified attacks only in Russia. Still, there are grounds to suspect that the infection is much more widespread, and banks around the world are advised to proactively check for infection.

How do I know if I’m infected?

Kaspersky Lab products successfully detect and block the malware used by Metel with the following detection names:

Trojan-Dropper.Win32.Metel; Backdoor.Win32.Metel; Trojan-Banker.Win32.Metel

Also Indicators of Compromise can be found in a blogpost on Securelist.

How can I protect myself?

To raise the level of protection, it is recommended that organizations use System Watcher that includes the BSS (Behavior Stream Signatures) module. This is included in all modern products and solutions.

To be on the safe side make sure you are using advanced anti-malware solutions such as Kaspersky Next EDR Optimum. Also pay attention to your cybersecurity awareness to make sure that you can identify phishing emails in your email box.

Of course, just offering a multitude of powerful endpoint security layers is not enough. Spear-phishing, one of the most popular techniques for initial infection, makes reliable mail security a must. Kaspersky Security for Mail Server scans incoming emails for both malicious attachments and URLs, significantly reducing the chances of malware reaching its victims.
