# Tyupkin: manipulating ATM machines with malware

By GReAT

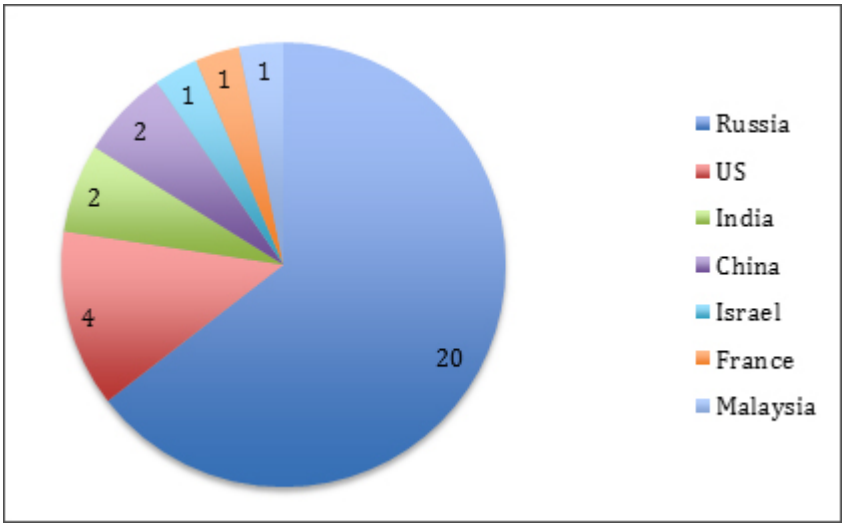
Published: 2014-10-07 · Archived: 2026-04-05 21:07:30 UTC

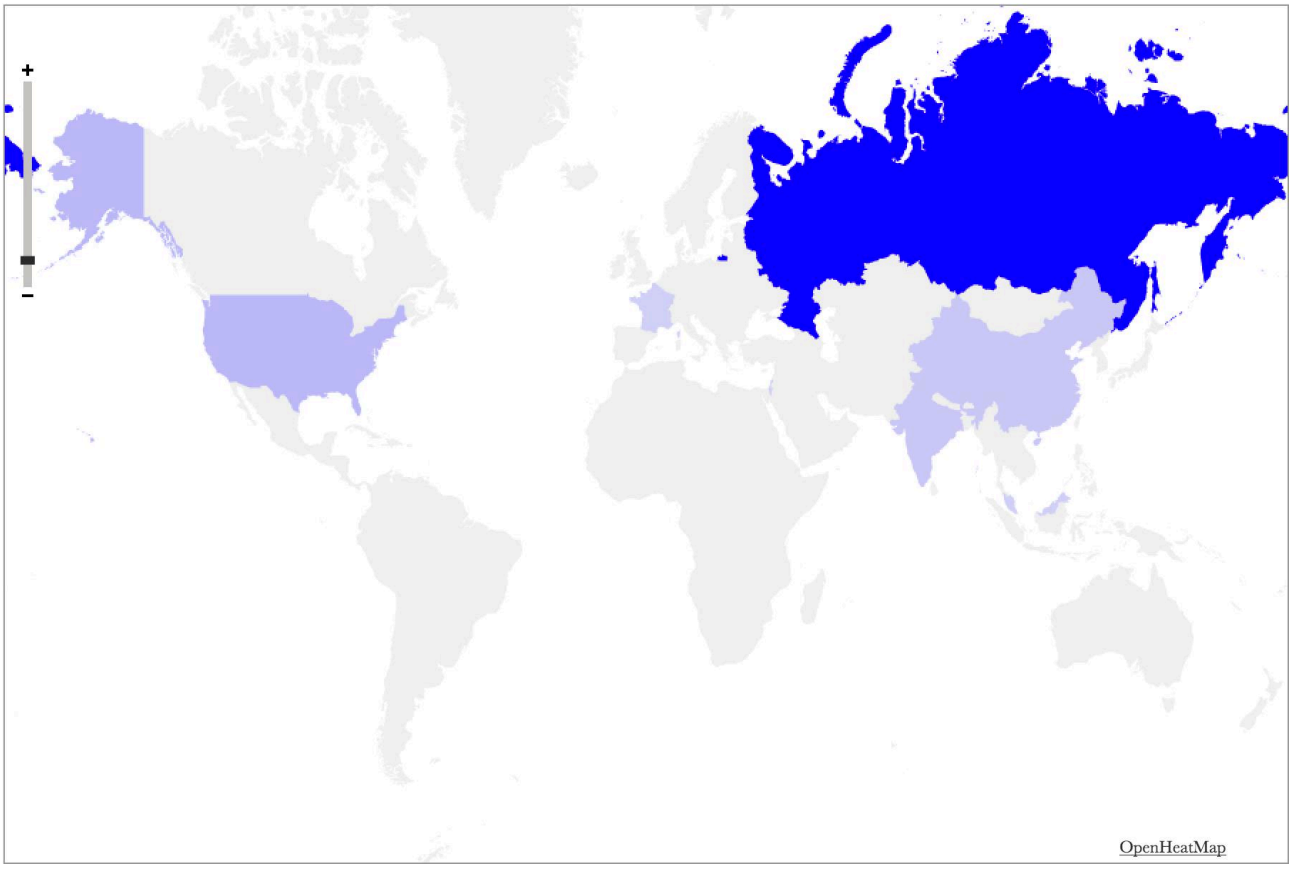
Earlier this year, at the request of a financial institution, Kaspersky Lab's Global Research and Analysis Team performed a forensics investigation into a cyber-criminal attack targeting multiple ATMs in Eastern Europe.

During the course of this investigation, we discovered a piece of malware that allowed attackers to empty the ATM cash cassettes via direct manipulation.

At the time of the investigation, the malware was active on more than 50 ATMs at banking institutions in Eastern Europe.  Based on submissions to VirusTotal, we believe that the malware has spread to several other countries, including the U.S., India and China.

Due to the nature of the devices where this malware is run, we do not have KSN data to determine the extent of the infections. However, based on statistics culled from VirusTotal, we have seen malware submissions from the following countries:




This new malware, detected by Kaspersky Lab as **Backdoor.MSIL.Tyupkin**, affects ATMs from a major ATM manufacturer running Microsoft Windows 32-bit.

The malware uses several sneaky techniques to avoid detection. First of all, it is only active at a specific time at night. It also uses a key based on a random seed for every session. Without this key, nobody can interact with the infected ATM.

When the key is entered correctly, the malware displays information on how much money is available in every cassette and allows an attacker with physical access to the ATM to withdraw 40 notes from the selected cassette.

Most of the analyzed samples were compiled around March 2014. However this malware has evolved over time. In its last variant (version .d) the malware implements anti debug and anti emulation techniques, and also disables McAfee Solidcore from the infected system.

## Analysis

According to footage from security cameras at the location of the infected ATMs, the attackers were able to manipulate the device and install the malware via a bootable CD.

The attackers copied the following files into the ATM:

C:\Windows\system32\ulssm.exe
%ALLUSERSPROFILE%\Start Menu\Programs\Startup\AptraDebug.lnk

After some checks of the environment, the malware removes the .lnk file and create a key in the registry:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
“AptraDebug” = “C:\Windows\system32\ulssm.exe”

The malware is then able to interact with ATM through the standard library MSXFS.dll – Extension for Financial Services (XFS).

The malware runs in an infinite loop waiting for user input. In order to make it more difficult to detect, Tyupkin accepts (by default) commands only on Sunday and Monday nights.

It accepts the following commands:

- XXXXXX – Shows the main window.
- XXXXXX – Self deletes with a batch file.
- XXXXXX – Increases the malware activity period.
- XXXXXX – Hides the main window.

After every command the operator must press “Enter” on the ATM’s pin pad.

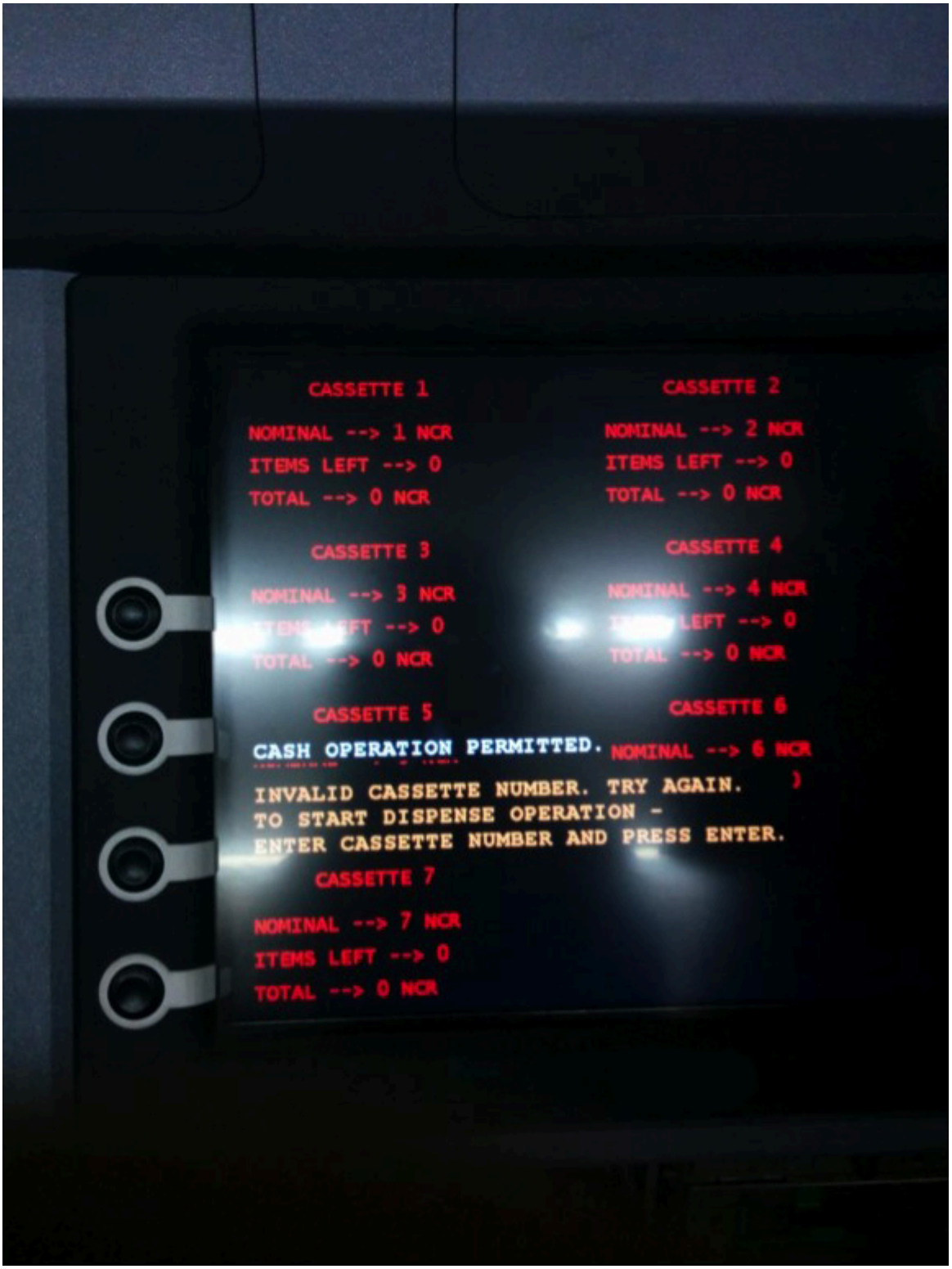
Tyupkin also uses session keys to prevent interaction with random users. After entering the “Show the main window” command, the malware shows the message “ENTER SESSION KEY TO PROCEED!” using a random seed for each session.

The malicious operator must know the algorithm to generate a session key based on the seed shown. Only when this key is successfully entered that it is possible to interact with the infected ATM.

After that, the malware shows the following message:

CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER.

When the operator chooses the cassette number, the ATM dispenses 40 banknotes from it.




When the session key entered is incorrect, the malware disables the local network and shows the message:

DISABLING LOCAL AREA NETWORK…
PLEASE WAIT…

It is not clear why the malware disables the local network. This is likely done to to delay or disrupt remote investigations.

Video with a demonstration in a real ATM is available:


## Conclusion

Over the last few years, we have observed a major uptick in ATM attacks using skimming devices and malicious software. Following major reports of skimmers hijacking financial data at banks around the world, we have seen a global law enforcement crackdown that led to arrests and prosecution of cyber-criminals.

The successful use of skimmers to secretly swipe credit and debit card data when customers slip their cards into ATMs at banks or gas stations is well known and has led to a greater awareness for the public to be on the lookout – and take precautions – when using public ATMs.

Now we are seeing the natural evolution of this threat with cyber-criminals moving up the chain and targeting financial institutions directly. This is done by infecting ATMs directly or direct APT-style attacks against the bank. The Tyupkin malware is one such example of attackers moving up the chain and finding weaknesses in the ATM infrastructure.

The fact that many ATMs run on operating systems with known security weaknesses and the absence of security solutions is another problem that needs to be addressed urgently.

Our recommendations for the banks is to review the physical security of their ATMs and consider investing in quality security solutions.

## Mitigation recommendations

We recommend that financial institutions and businesses that operate ATMs on premises consider the following mitigation guidance:

- Review the physical security of their ATMs and consider investing in quality security solutions.
- Change default upper pool lock and keys in all ATMs. Avoid using default master keys provided by the manufacturer.
- Install and make sure that ATM security alarm works. It was observed that the cyber-criminals behind Tyupkin infected only those ATMs that had no security alarm installed.
- For the instructions on how to verify that your ATMs are not currently infected in one step, please contact us at intelreports@kaspersky.com. For the full scan of the ATM's system and deleting the backdoor, please use free Kaspersky Virus Removal Tool (you may download it here).

## General advice for on-premise ATM operators

- Ensure the ATM is in an open, well-lit environment that is monitored by visible security cameras. The ATM should be securely fixed to the floor with an anti-lasso device that will deter criminals.
- Regularly check the ATM for signs of attached third-party devices (skimmers).
- Be on the lookout for social engineering attacks by criminals who may be masquerading as inspectors or security alarms, security cameras or other devices on premises.
- Treat intruder alarms seriously and act accordingly by notifying law enforcement authorities of any potential breach.
- Consider filling the ATM with just enough cash for a single day of activity.
- For more advices both for merchants and users please visit http://www.link.co.uk/AboutLINK/site-owners/Pages/Security-for-ATMs.aspx

---