ATTACKS AGAINST ATMS USING GREENDISPENSER: ORGANIZATION AND TECHNIQUES

POSITIVE TECHNOLOGIES

Hacking-related bank losses in selected countries (2016)

Bangladesh	81,000,000 $
Russia	30,000,000 $
Japan	13,000,000 $
Ukraine	10,000,000 $
Taiwan	2,200,000 $
Vietnam	1,100,000 $
Thailand	350,000 $
India	194,000 $

ARE BANKS LOSING THE FIGHT AGAINST ATM HACKERS? ANATOMY OF GREENDISPENSER THEFTS

Whatever the good guys have, the bad guys eventually get too. Any technology that makes banking more accessible to customers has the side effect of making life easier for criminals. Information sharing at security conferences for financial companies, regulators, telecom companies, and software developers is great for developing strategies and exchanging experience—but also for hackers trying to stay one step ahead of their targets.

Judging by the scale of damage and sophistication of attacks, banks are having a hard time keeping up with today's digital bank robbers. In this report, Positive Technologies experts draw upon the company's investigations of incidents at several Eastern European banks to show the inner workings of ATM logic attacks performed using GreenDispenser malware.

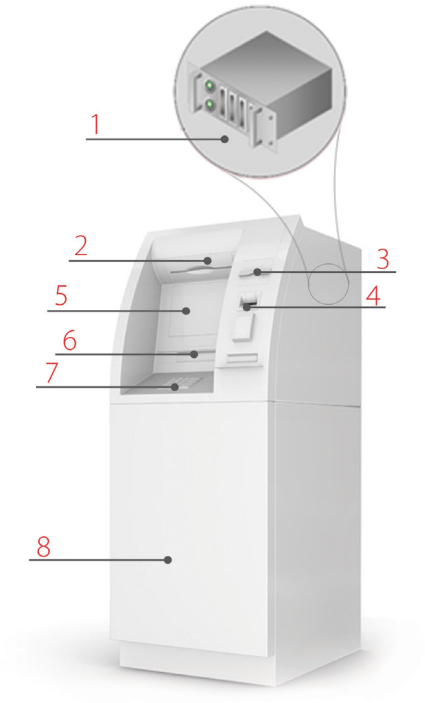
ATTACKS ON BANKS IN 2016

Digital-enabled bank robberies fall into four main categories:

+ Attacks on bank digital infrastructure in order to access the funds transfer system[1]
+ Attacks on bank digital infrastructure in order to access the ATM management system[2,3]
+ Attacks requiring direct physical access to an ATM[4,5]
+ Attacks on e-banking systems on the client side[6,7,8]

ATM-related attacks can be grouped under:

+ Fraud[9]
+ Physical attacks[10]
+ Logic attacks[11]



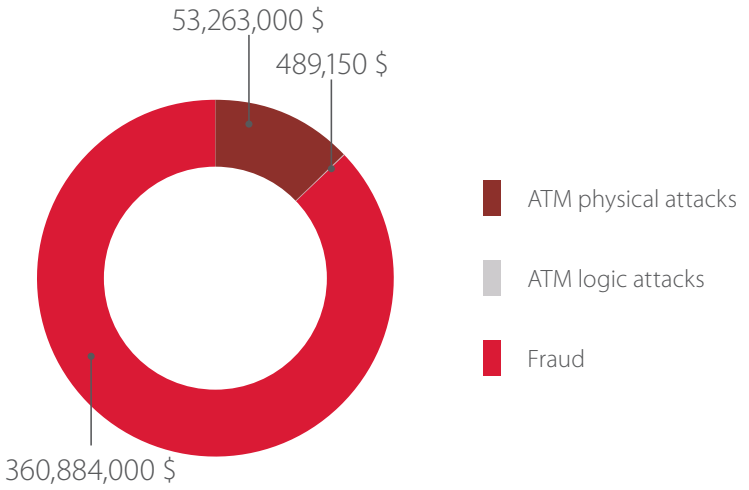
1. ATM computer
2. Security camera
3. Receipt printer
4. Card reader
5. Screen
6. Dispenser
7. PIN pad
8. Safe

1 group-ib.com/blog/lazarus
2 ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf
3 group-ib.com/resources/threat-research/cobalt.html
4 itv.com/news/london/2017-02-03/exploding-cash-machine-gang-jailed-following-flying-squad-investigation
5 association-secure-transactions.eu/atm-explosive-attacks-surge-in-europe
6 onestore.nokia.com/asset/201094/Nokia_Threat_Intelligence_2H2016_Report_EN.pdf
7 group-ib.com/blog/cron
8 symantec.com/security_response/writeup.jsp?docid=2011-082216-3542-99
9 bankinfosecurity.com/euro-cops-cuff-suspected-payment-card-fraudsters-a-9994
10 association-secure-transactions.eu/tag/atm-physical-attacks
11 association-secure-transactions.eu/tag/atm-malware

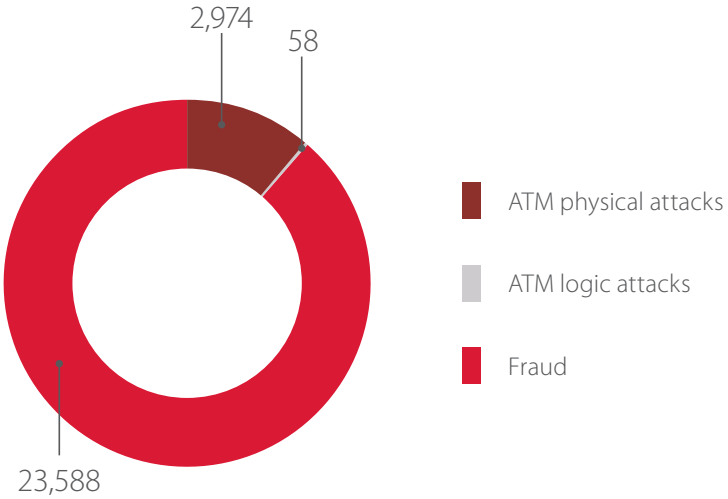
The most well-known ATM fraud method involves using a skimmer to steal card information and clone cards, with which criminals can withdraw money from the cardholder's account. A skimmer is a device that is disguised as a card reader. When a client inserts a card into the ATM, the skimmer reads the data from a card's magnetic stripe or chip.[12] Some skimmers can even read data from a card EMV chip at a distance.[13]

According to European ATM Security Team[14] fraud accounted for 89 percent of all attacks on ATMs in 2016. In terms of financial losses, fraud caused 87 percent of the total.

Physical attacks on European ATMs increased in 2016, making up 11 percent of all ATM incidents. This 12-percent year-over-year boom was caused primarily by a large jump (47%) in the number of explosions targeting ATMs.



Total damage from ATM attacks (Europe, 2016)



Number of ATM incidents (Europe, 2016)

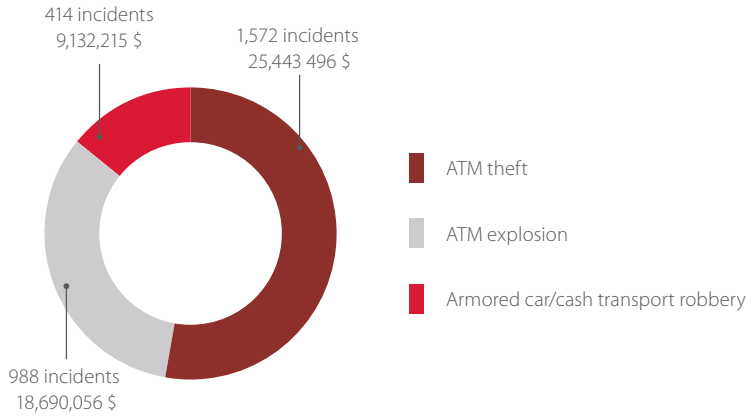
12 blackhat.com/us-16/briefings.html#hacking-next-gen-atms-from-capture-to-cashout
13 youtube.com/watch?v=6VaG1mwoukQ
14 association-secure-transactions.eu/atm-black-box-attacks-increase

ATM logic attacks involving malware started in earnest in 2009, with the Skimer[15] Trojan. Since then, security researchers have identified several families of Trojans: Skimer, Ploutus,[16] NeoPocket,[17] Padpin[18] (Tyupkin[19]), Suceful,[20] GreenDispenser,[21] Ripper,[22] and Alice.[23]

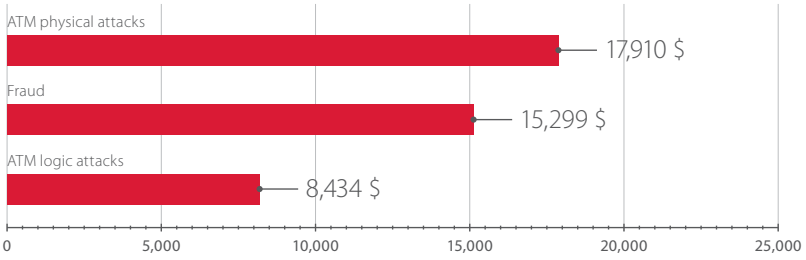
Fewer than one percent of attacks on European ATMs in 2016 saw the use of malware. While this number may pale in comparison to the flood of fraud, malware infections tend to grab media attention and deal a harsher blow to the reputation of the victim bank and its supposedly hapless security.

With that in mind, this report will present an in-depth look at GreenDispenser, which was found during incident investigation by Positive Technologies at multiple banks in Eastern Europe.

We estimate that losses caused by GreenDispenser in 2015 and 2016 were around $180,000. Belying the relatively low total are two facts: this method is relatively recent and therefore being actively improved, and that with the expected strengthening of ATM safes to withstand explosions, logic-based methods will likely become more attractive to criminals. Such incidents have already increased in popularity in Europe, growing by 287 percent from 2015 to 2016. Positive Technologies experts predict that 2017 will see 30 percent growth in overall cyberattacks against banks, including at the ATM level.



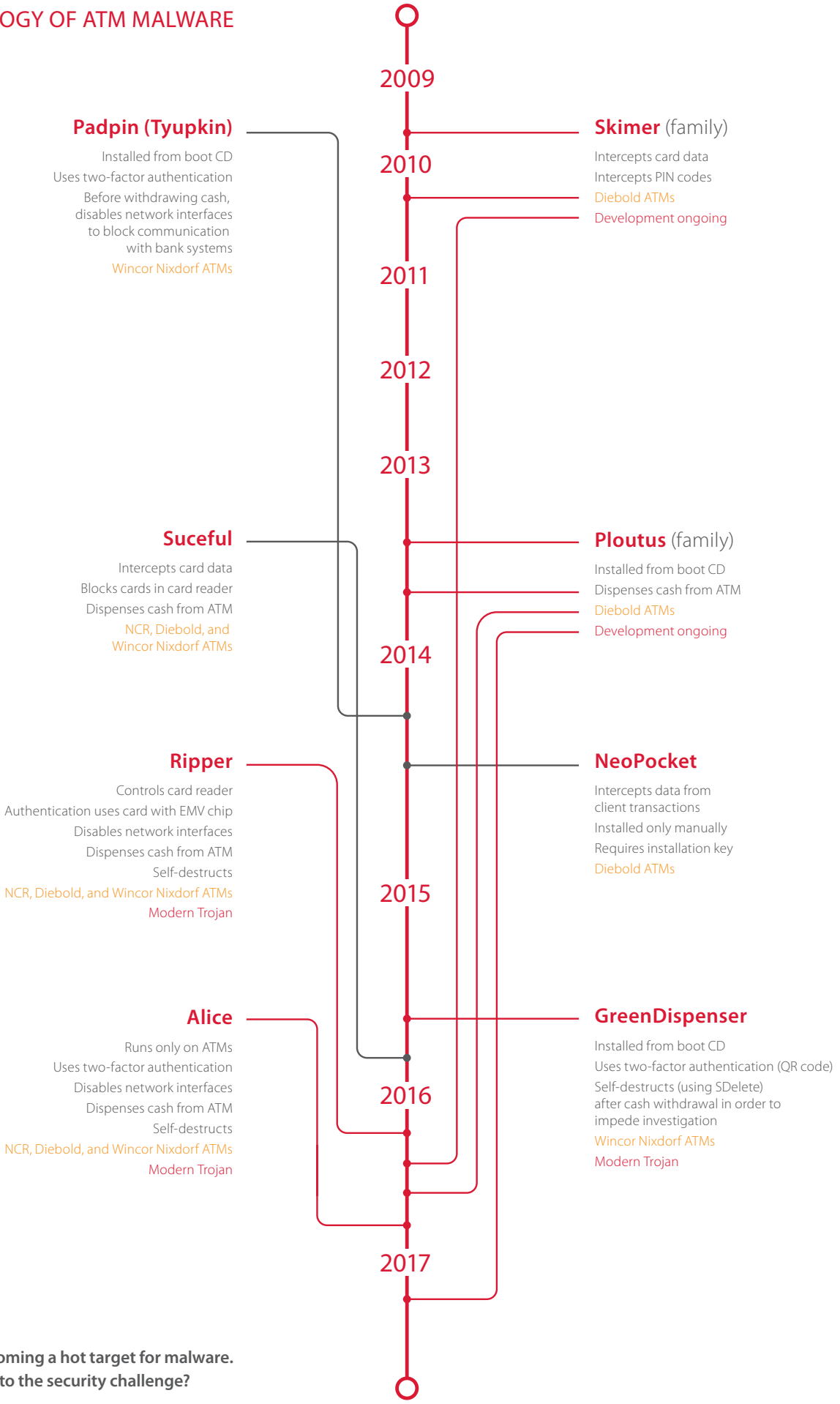
Total damage from ATM physical attacks (Europe, 2016)



Average damage per ATM attack (Europe, 2016)

15 vms.drweb.com/virus/?i=426550&lng=en
16 symantec.com/connect/blogs/criminals-hit-atm-jackpot
17 communicationstoday.co.in/images/reports/20170301-TrendLabs-2016-annual-security-roundup-report.pdf
18 symantec.com/security_response/writeup.jsp?docid=2014-051213-0525-99
19 securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988
20 fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html
21 proofpoint.com/us/threat-insight/post/Meet-GreenDispenser
22 fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html
23 blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware

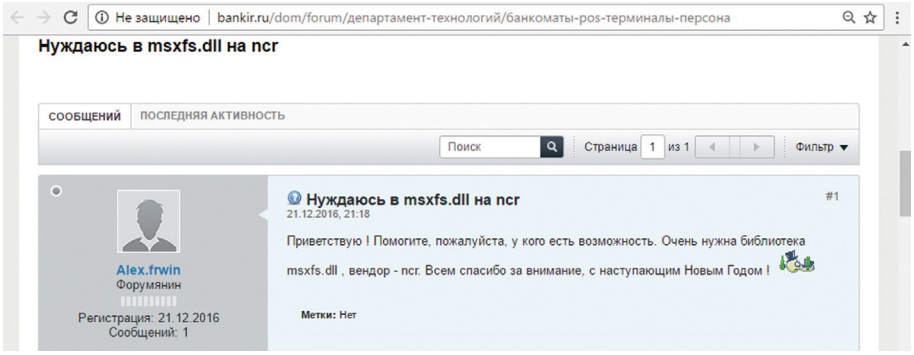
CHRONOLOGY OF ATM MALWARE



ATMs are becoming a hot target for malware. Are banks up to the security challenge?

GREENDISPENSER: ROLE BY ROLE

Financial applications on Microsoft Windows use the Extension for Financial Services (XFS), a special standard that ensures compatibility between ATMs and hardware components. GreenDispenser, like other malware such as Tyupkin and Padpin, uses the XFS API from the msxfs.dll library in order to communicate with the ATM PIN pad, dispenser, and other components.

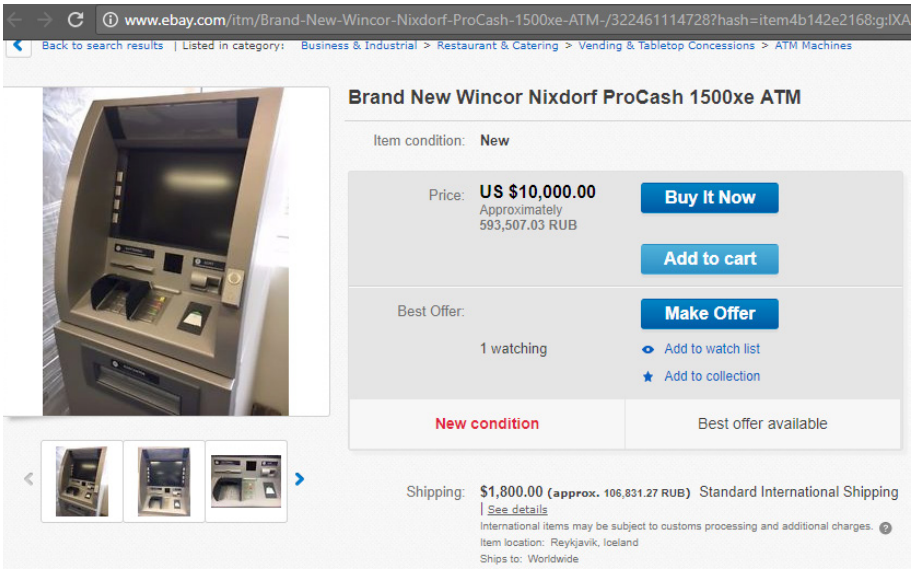


A forum user looking for technical assistance (specifically, a .dll file specific to NCR ATMs)

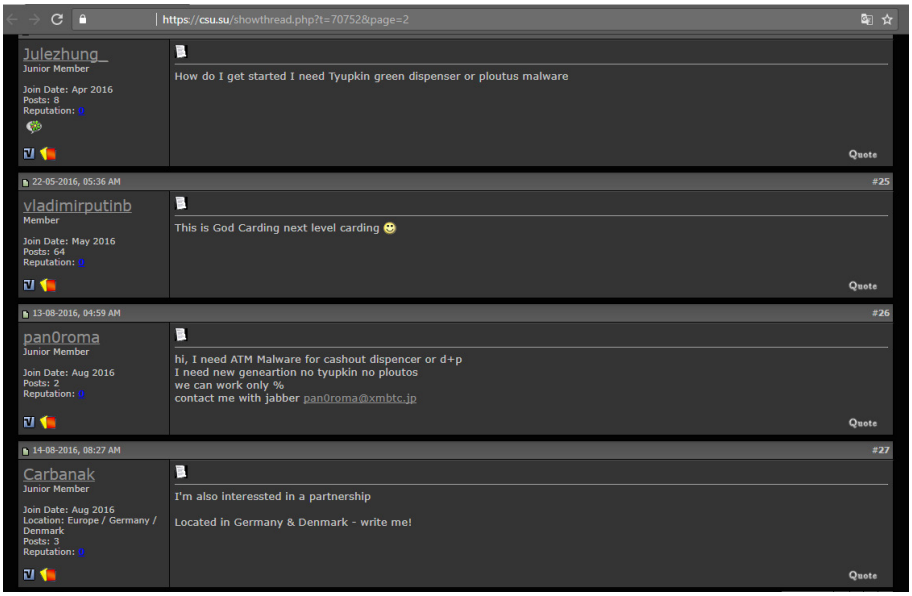
Since XFS is widely used by almost all ATM manufacturers, criminals can use XFS to create malware that is compatible with (in other words, can attack) any ATM regardless of type or manufacturer. This is shown by Ripper and Alice, two Trojans discovered in 2016 that indicate a trend for malware to target multiple ATM manufacturers simultaneously.

msxfs.dll is a library included in a special version of Microsoft Windows for ATMs. So an essential step for a criminal developing and testing a Trojan is to get a copy of this library. There are different ways of doing so, including:

+ Buying an old or discarded ATM for testing and research
+ Bribing a bank employee to copy the library and, later, install the Trojan on an ATM
+ Simply asking for the necessary files on internet forums



ATMs are available on eBay



A forum user looking for criminals willing to install malware on Wincor ATMs

The term "reenDispenser" came into use after 2015 attacks on ATMs in Mexico. Later, thefts with GreenDispenser were discovered in Eastern European countries in 2016. Most likely the creator of GreenDispenser sold the malware to criminals in another country, who intended to rob banks without having to physically modify ATMs or hack bank networks via the internet.

GREENDISPENSER CREATOR

+ Develops the Trojan and sells it
+ Localizes and adapts the Trojan for use in different countries

Naturally, for an infected ATM to not arouse suspicion among clients or bank employees, the Trojan would need to be translated and adapted for the countries in which it would be used. The creator would handle localization as requested by the criminals. So we can say that the creator's development of the Trojan had sales of the Trojan as its goal. We can then assume that the creator of GreenDispenser and attack organizers are not related to each other.

THEFT ORGANIZER

+ Coordinates with the Trojan creator regarding purchase, localization, and configuration of GreenDispenser
+ Organizes search for other operation participants
+ Monitors and oversees participants during the operation

That said, a criminal who has just purchased the Trojan would need to answer two questions before starting to steal money from ATMs:

+ How does the Trojan get installed on ATMs?
+ How does the ATM money get collected?

The Positive Technologies investigation showed that criminals obtained physical access to ATMs in order to install GreenDispenser.

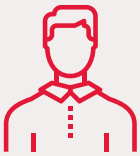
MALWARE INSTALLER

Gains physical access to an ATM and installs GreenDispenser on it

How does one install GreenDispenser (or a similar Trojan) on an ATM? Best of all is a person who has legitimate access to the ATM, such as a bank employee or contractor responsible for ATM maintenance. Otherwise, a person with special tools and lockpicking experience can perform this task. In either case, the attack organizer would need to train this person in how to install GreenDispenser.

Once the necessary ATMs have been infected, the criminals proceed to the cash withdrawal phase.

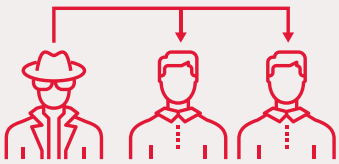
Although the malware is stealthy and relatively advanced, this phase is the riskiest and carries the greatest risk of discovery by the bank. After all, someone still has to physically come to the ATM and take the cash.



MULE

+ Relays Trojan-generated QR code to the mule herder
+ Withdraws money from ATM after entering PIN2
+ Reports to the mule herder

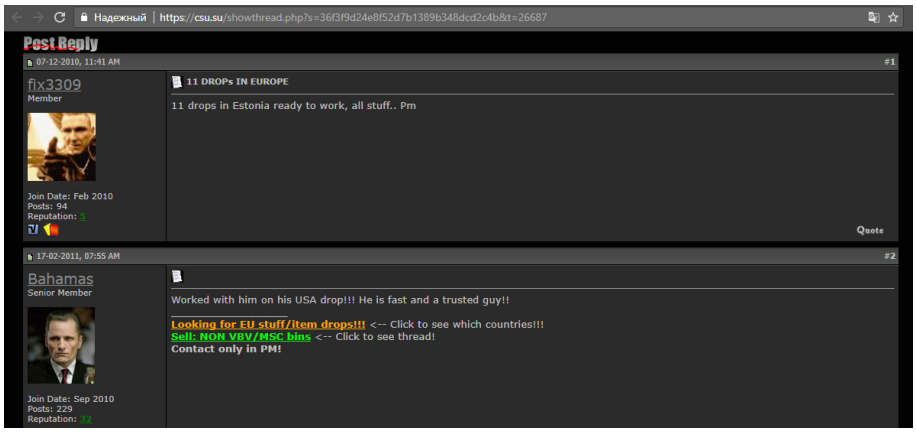
Instead of risking their own necks, cybercriminals prefer to hire special cutouts—"mules"—to perform this dirty work. A mule's work might include receiving money in their own name, using a card to withdraw money from an ATM, or receiving money when the criminals send a trigger to the ATM. The mule keeps a portion of the stolen money as payment for their work.



MULE HERDER

+ Recruits mules and instructs them
+ Arranges for exchange of QR and PIN2 codes between organizers and mules

The larger an operation, the more mules are needed. When the number of drops becomes large, criminals hire "mule herders" to streamline the process. These go-betweens hire, train, and coordinate mules, and also handle communication between the attack organizers and mules. So when a mule is standing by to withdraw money from an ATM infected with GreenDispenser, the organizer would give the mule herder the necessary confirmation code to pass on to the mule.

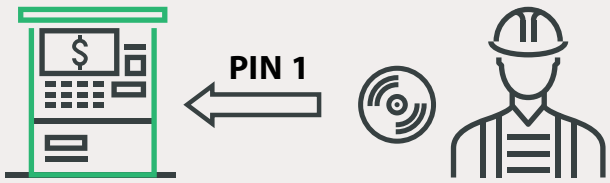


Mule herders aren't afraid to promote their services to potential clients on online forums

GREENDISPENSER: STEP BY STEP

Since GreenDispenser aims only to steal cash contained inside an ATM—instead of stealing card information—the criminals realized that legitimate cardholders might withdraw money from an infected ATM. That would leave less cash available in the ATM for the mule to steal. The solution? After the operating system is infected, a country-specific message (in the local language) states that the ATM is temporarily out of order. Ordinary clients think that the machine is not working and walk away. But despite the message, the ATM is actually working. GreenDispenser (via XFS) has seized control of the PIN pad and is waiting for a mule to enter the static PIN code that has been selected by the malware creators.

Step 1. Infecting an ATM



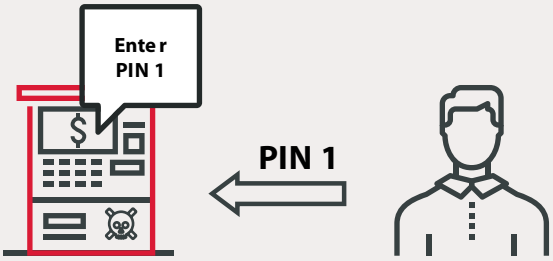
1.1 Getting access to the service area and installing the Trojan

1.2 Visual confirmation that the ATM is compromised

After the first PIN is entered correctly, the mule needs to enter a second PIN code. This code is needed to prove that access has been granted by the theft organizers—otherwise, the mule could rob the infected ATM on their own initiative. To get this second PIN code, the mule sends the QR code displayed on screen to the criminals.

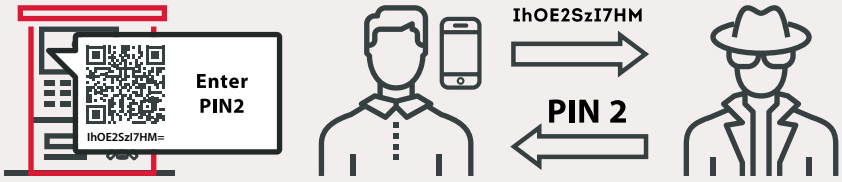
IhOE2SzI7HM=

To make sure that the second PIN code is unique, the malware generates a random value, which is encrypted by Microsoft CryptoAPI and then coded in Base64. The Base64-coded result is displayed on screen both as a QR code and string of characters (the string is useful if the mule does not have a smartphone or the mule's smartphone cannot read the QR code). It is also possible that the criminals developed a special smartphone app that could generate the second PIN code when standing next to an infected ATM.

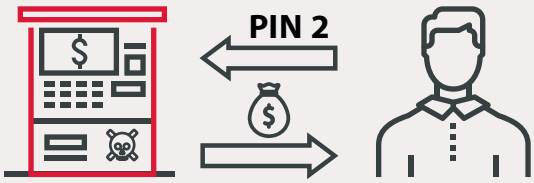


2.1 Authentification. Stage 1: the intruder enters PIN1 generated by the malware creators

Step 2.
ATM robbery



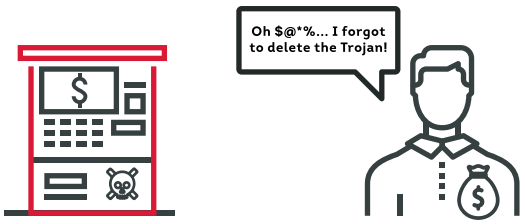
2.2 Authentification. Stage 2: the intruder scans the QR code displayed on the ATM screen, sends it to the mule herder, and gets PIN2



2.3 Cash withdrawal: the intruder enters PIN2, gets access to the control interface, and sends a command to the ATM to dispense cash

After entering both codes, the mule gains access to the control interface, which includes the cash dispensing function. After successfully retrieving the money, the mule follows the instructions of the mule herder. In the control interface, the mule tells GreenDispenser to erase itself from the ATM. This "self-destruct sequence" involves adding a task to the Windows Task Scheduler for creating and running the file del.bat. This file contains commands for deleting GreenDispenser with the help of SDelete, a Windows Sysinternals utility, which in this case has been renamed to del.exe. Currently SDelete is used by a number of digital criminals as an antiforensic tool—by irreversibly deleting files, it eliminates traces of the malware and makes investigation more difficult.

```
:start
tasklist /FI “IMAGENAME eq <malware.exe>” 2>NUL | find /I /N “<malware.exe>”>NUL
if “%ERRORLEVEL%”==”0” goto start
“<path>\del.exe” / accepteula –p 3 –q “<path>\<malware.exe>”
del ”<path>\del.exe”
del ”<path>\<malware.exe>”
shutdown –t 0 –r –f
del “%~f0”
```



3.1 The mule leaves without deleting the Trojan via the control interface

3.2 GreenDispenser launches a script that deletes its files and restarts the system

3.3 Security staff find the ATM empty and functioning normally

Step 3. Covering tracks

Any criminal mastermind knows that even the best-laid plans go awry. For example, if different people are performing infection and cash withdrawal, the criminals might not have enough mules to withdraw more cash. Or perhaps a mule can't find the right time to perform a withdrawal. In any case, since an ATM cannot stay out of service for long without arousing suspicion, GreenDispenser deletes itself from the ATM automatically one week after infection. If a mule is at an ATM and started to enter the PIN codes but cannot finish the process, the mule can force GreenDispenser to delete itself either before or after entry of the second PIN code.

FORECAST AND RECOMMENDATIONS

The information presented here, considering the increasing number of malware incidents overall, indicates that GreenDispenser may be only one of a larger number of logic attacks directed against ATMs. Based on interest observed on cybercriminal forums in ATM-related standards and system libraries, we can expect ongoing development of new malware involving either direct physical access to ATMs or targeted attacks on bank ATM management infrastructure.

Similarities among ATMs make it possible for criminals to reuse the same malware for crimes in multiple countries. GreenDispenser was used to attack ATMs in Mexico but was later found in Eastern Europe as well. Moreover, moving from country to country may even make things easier for criminals: while authorities in one country are investigating crimes and trying to develop countermeasures, the same malware (along with gained experience) can be used against ATMs in other, less prepared countries.

Besides securing network infrastructure against both insiders and internet hackers, banks need to pay attention to physical security of ATMs. Cash is stored in a robust safe but the computer that decides whether to dispense cash from that safe is much easier to access—such as with a special pick or key from another ATM. All an attacker needs to do is connect a microcomputer with special software or boot disk to the ATM computer. After that, it takes just minutes to empty out an ATM.[24] That is why it is important to keep an eye on physical security, placement zones, and personnel with ATM access. All communication equipment (modems, etc.) should be inside the ATM.

Special protection should be enforced for the computer that manages all ATM functions. First, banks should disable external input devices (keyboards, mice, etc.) and loading from external disks (USB drives, CDs, etc.), since these are major opportunities for hackers. A strong BIOS password is necessary to prevent attackers from changing ATM startup settings. Second, banks should install and properly configure application control software to monitor software integrity, allowing only whitelisted programs that have been checked for unauthorized modifications. Third, banks should regularly perform audits in order to have up-to-date information on ATM security and minimize the chances of intrusion.

By diligently implementing these security measures throughout their networks, banks can make themselves less attractive to attackers and prevent substantial risks to their reputation and bottom line.

24 banki.ru/news/daytheme/?id=8018520

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com