A TRUSTWAVE SPIDERLABS ADVANCED THREAT REPORT

Post-Soviet Bank Heists:

A Hybrid Cybercrime Study

Trustwave® SpiderLabs®

Post-Soviet Bank Heists:
A Hybrid Cybercrime Study

Authors Thanassis Diogos
EMEA Managing Consultant, Incident Response, Trustwave

Sachin Deodhar
EMEA Incident Response Consultant, Trustwave

Research and Publication Rodel Mendrez and Gerald Carsula
Malware Research Team, Trustwave

Table of Contents

Introduction **1**
A Closer look **2**
Detailed walkthrough 3
Malicious Code 5
Recommendations **7**
Indicators of Compromise **8**
Files 8
IPs/Domains 8

Introduction

Earlier this year, the SpiderLabs team at Trustwave investigated a series of bank breaches originating from post-Soviet states. These investigations took place during mid-to-late 2017, and each bank compromise resulted in a significant amount of stolen funds. The actual amount of money stolen was different in each case, with the average amount around USD$5 million (in cash), ranging from USD$3 to USD$10 million. The investigations showed that the attacks shared a number of common features, such as involving large amount of monetary loss originating from what initially appeared to be legitimate bank customer accounts. Additionally, in all cases, the theft took place using normal cash withdrawals from various ATM terminal locations outside the bank's originating country.

In some cases, the victim banks didn't even realize that a breach had taken place and a significant amount of money was stolen until well after the attack was completed. In a few cases, the malicious activity was reported to the banks by third-party processors responsible for processing the bank's debit and credit card transactions. The common feature between these cases is that money was stolen using legitimate ATM cards provided by each bank.

Criminals used (or hired) people to personally visit the various branches and request new accounts with minimum or zero initial deposit amounts. Beyond opening their "personal' accounts, they also demanded to receive a debit card with their new account. Initially this might not appear to be an issue since debit card usage is directly related to the account's balance. However, in the banking world, a service called "Overdraft" exists; simply put it means that under very specific circumstances a debit card can be converted into a credit card. This means that the bank allows their customer to withdraw cash even though they do not have the appropriate balance in their account. Of course, this is supposed to happen only for specific account types, also referred to as risk levels.

After the debit cards were delivered to the customers, they were distributed outside the originating country to a group of international conspirators. When all the cards had been relocated to their destination countries, a cyber-criminal, who had already breached the victim bank network, accessed the bank's internal systems and manipulated the debit cards' features to enable a high overdraft level and removed anti-fraud controls that had been placed for the specific accounts. Minutes later the operation continued in the countries where the debit cards had travelled. The debit cards were used to perform cash withdrawals from several different ATMs. Within the next few hours the operation concluded, removing up to USD$10 million from each bank.

We believe that the attack described in this report represents a clear and imminent threat to financial institutions in European, North American, Asian and Australian regions within the next year. Currently the attacks are localized to the Eastern European and Russian regions. However, in cybercrime, this area is often the canary in the mineshaft for upcoming threats to other parts of the world. Our investigations have revealed victim losses currently around approximately USD$40 million. However, when taking into account the undiscovered or uninvestigated attacks along with investigations undertaken by internal groups or third parties, we estimate losses to be in the hundreds of millions in USD. All global financial institutions should consider this threat seriously and take steps to mitigate it.

A Closer Look

To drill into the details of these criminal operations we will take a closer look at one of the cases. On a winter evening in February 2017, a credit/debit card processor's fraud management system picked up a series of suspicious ATM withdrawal transactions originating from the victim bank's customer accounts during the late-night hours until the early morning. The withdrawals occurred at ATM terminals located across the region, including Europe and the Russian Federation. Notably, no ATM transactions occurred in countries where the affected bank had a presence.

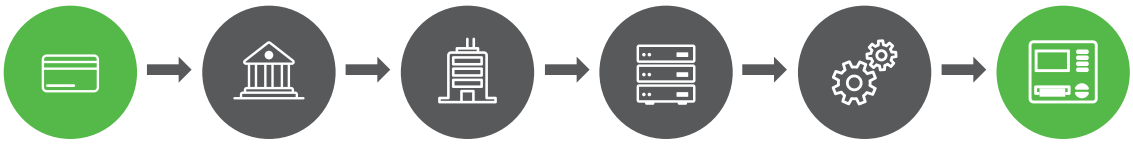
In addition to requesting the Trustwave SpiderLabs team to perform a thorough investigation, the bank also reported this incident to local law enforcement agencies. Undoubtedly this incident appeared to be multifaceted; it appeared that the bank's network was breached, and it also seemed likely that the processor's network may have also been compromised. Moreover, it was also likely that there was a physical facet to this breach, in which an organized cybercriminal network was involved. The Trustwave team's objective was to investigate the incident based purely on available factual evidence and its unbiased interpretation.

The third-party processor engaged an independent team from Trustwave SpiderLabs to investigate the impact of the incident on its network and its overall business. This way Trustwave could see the whole picture from the perspectives of both the affected bank and the third-party processor, whose services the bank used for its card processing functions.

The Trustwave team commenced both sides of the investigation immediately and was able to successfully uncover what we believe to be a very interesting, if not entirely unique, modus operandi behind the successful breaches of both the bank and processor networks. The objective of such an operation is the successful withdrawal of funds from the rogue accounts created earlier, as described in this report.

The attackers used innovative attack tactics, techniques and procedures to successfully execute a long duration "hybrid" attack campaign comprising two physical stages and multiple cyber-attack stages as depicted below:

STAGES OF THE ATTACK



Physical Stage I
Recruit mules to open bank accounts and issue new debit cards

Cyber Stage I
Obtain unauthorized privigeged access to the bank's network

Cyber Stage II
Compromise third party processor's network

Cyber Stage III
Obtain privileged access to Card Management System

Cyber Stage IV
Activate overdraft on specific bank accounts

Physical Stage I
Cash-out from ATMs in multiple cities and countries

Detailed Walkthrough

Our findings suggest that motivation for the attack was purely financial gain. Our analysis shows that the cyber attackers and their physical counterparts worked in close and very effective coordination to execute this malicious operation:

- The cybercriminal network behind this attack recruited so-called "mules", (non-technical conspirators whose job is to transfer money for cybercriminals), to open dozens of new bank accounts by physically visiting various branches of this bank in different cities in the country. These individuals used counterfeit documents to request bank accounts, most likely supplied by the organized cybercriminal network. Once these people had new bank accounts approved, they then requested debit/ATM card companions to their new bank accounts. After they obtained these debit cards, they probably handed these debit cards over to a member of the cybercriminal network for distribution outside the country for later use.

PHYSICAL PART OF THE ATTACK

- While the physical activities involving application for accounts and debit cards were taking place at the bank's various branches in the country, the cyber attackers gained initial entry, moved laterally and compromised multiple systems inside the bank's network.

GAINING INITIAL FOOTHOLD IN THE BANK NETWORK

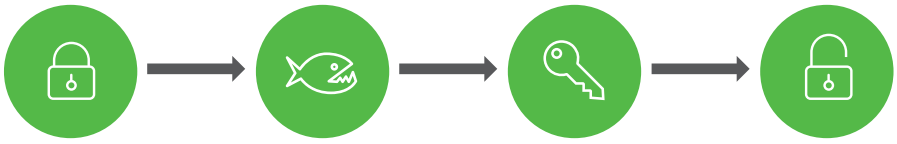
Opportunistic Phishing
Emails to employees with malicious attachments opened – 'backdoor' is created

Social Engineering
Attackers successfully obtain 'backdoor' access through compromised computers

Exploit Windows Computers
Set up multiple 'backdoors' and RDP access to compromised systems

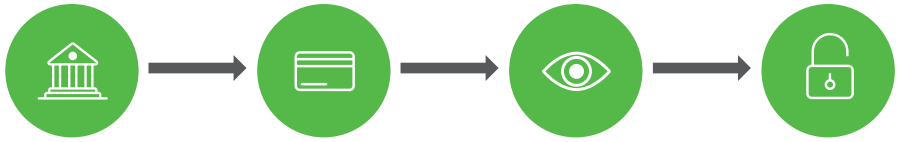
- After successfully compromising the bank's network the cyber attackers then proceeded to launch an attack on the third-party processor's network and eventually (after numerous attempts) they succeeded. The bank, due to their established cooperation with the processor, already maintained connectivity with the processor. This made it easier for the criminals because they had already gained access to the bank's infrastructure and had captured the credentials used to connect to the processor. After gaining foothold into the processor's network, the attackers compromised the Enterprise Admin account which eventually gave them full access into the infrastructure. Their next step was to execute reconnaissance of the card processing service.

LATERAL MOVEMENT AND SUCCESSFUL COMPROMISE OF BANK NETWORK



- Next, the attackers executed several malicious payloads on the processor's network, key amongst them was a legitimate monitoring tool installed on the processor's Terminal Server (that allowed users to access the card management application via a browser). This software called "Mipko" (advertised as "Employee Monitor") captures full information, including screen captures, keystrokes and several other types of information for all users who logged into the system and/or accessed the card management application using their respective credentials. In this way the software attackers captured almost 4GB of data within a month. The information captured included keystroke logging and countless screenshots.

INSTALLATION OF KEYLOGGER AND COMPROMISE OF THE PROCESSOR NETWORK



- The attackers then identified the accounts on the card management application used by the bank employees who had authorization to "request" changes to the properties of a customer's debit card, and "approve" or "commit" such a change. They were looking for such privileges to manipulate each of the cards associated with the rogue accounts created during the preceding months.
- During the day of the final stage attackers used these credentials to:
  - Change risk ratings on the rogue accounts from high to low allowing the attackers to activate further credit permission, known as Overdraft (or simply OD).
  - Activate the OD credit function on the accounts.
  - Manipulate or remove any anti-fraud control in place for these accounts.
  - Change the OD Limit on the accounts from the default value of USD$0 to ranges of USD$25,000 - USD$35,000.

- The physical counterparts stationed at various locations in Europe and the Russian Federation then cashed out substantial amounts of money for each of these cards from ATM terminals. Cash withdrawals across the region began within minutes of the first OD property change made to the debit cards on the card management application.

COORDINATED ATM CASH WITHDRAWALS ~ MILLIONS OF USD

Command & Control with Physical Mules for Coordinated Cash Outs

Coordinated ATM Withdrawals

Direct $ Value of Loss: Millions of USD

As in the preceding phases of the attack, careful planning went into the choice of ATM locations to be used for cash withdrawals, based on the following criteria:

1. Location: those in solitary locations took precedence over those in locations with higher foot traffic.
2. Degree of physical security: ATMs with no security cameras (or those with defective security cameras) were chosen as well as terminals that were not protected by security guards.
3. The ability to dispense substantial amounts of cash. ATMs (mis) configured to allow withdrawal of substantial amounts of money were chosen. (Specifically, either very high or no daily withdrawal limits were selected).
4. ATM locations were chosen in cities across Europe, (including former Soviet Union countries), and the Russian Federation. No selected ATM was located in the victim bank's actual country.

The final stage of this hybrid operation took almost five hours to complete. This was the time required for each rogue account to be carefully manipulated and for simultaneous debit card withdrawals across the geographic region to occur. As in the first phase of the operation where the mules played an active role in requesting the new accounts and debit cards, in the final phase the mules were employed to perform the cash withdrawals. Only a small number of the ATMs were equipped with security cameras, so a few mules were caught in action. Law enforcement requested video footage from surrounding buildings' cameras and this revealed that the mules met with other suspects (probably direct members in the cybercrime gang) shortly after cashing out the debit cards. These meetings were most likely to deliver the stolen cash, after keeping their fee.

Malicious Code

Throughout the distinct phases of the cyber-attack, we noted that attackers adopted the emerging tactic sometimes called "living off the land" which involves very limited use of actual malware in the form of malicious files and easily detected protocols associated with Command & Control and data exfiltration traffic. Instead, the attackers used legitimate Windows and PowerShell commands in combination with tools such as PSExec for lateral movement. Notably they also used plink.exe (Windows SSH client) to access RDP over an already established SSH tunnel. Other software components used in this operation were split among commercial monitoring application (Mipko Employee Monitor) and the well-known suspect "Cobalt Strike Beacon" mainly used to maintain backdoor connection with an endpoint geolocated in the United States of America.

It should be noted that after the attackers penetrated the bank's network, they continually used a specific system to perform their activities. We focused our investigation on this system after backtracking malicious activities in the processor's network to it. Remote Desktop activity on the processor network was identified to have originated from the bank system. Eventually we asked the bank to provide this system for investigation. At that point, the bank's IT staff responded that this system became unbootable shortly after the massive cash out occurred.

When we obtained a copy of the system for analysis we found it was unbootable and the file system was corrupt. However, the Trustwave team was able to reconstruct the partition table and analyze the file system enabling collection and analysis of significant evidence from this key system. One of them was called dropper.exe and upon execution its main function was to wipe the Master Boot Record on the hard disk, effectively destroying the system for any future use. This was the last recorded action taken by the attackers before leaving the network. They appeared to truly care about clearing any remaining tracks of their activity that may have been left behind.

Our investigation did not reveal any signs of data exfiltration from the bank itself. The bank's network appears to have been breached for two primary reasons:

1. The bank had an established mechanism to connect to the processor's network from several terminals inside the bank network by first establishing a VPN session between the two networks and then using Remote Desktop Protocol (RDP) to connect from a system inside the bank network to the Windows Terminal Server in the processor's network. By attacking the bank's network, the attackers could piggy back on this connection to get a foothold on the processor's network (and subsequently obtain access to the card management application in the processor's network)
2. To withdraw funds from the newly issued debit cards for the "rogue" bank accounts, the attackers needed to obtain credentials of the bank employees that used the card management application on the processor's network. Using these credentials, they could change the necessary properties of the debit cards to cash out from ATM terminals in the final stage of the attack.

Based entirely on the precision with which the attack was carried out, we believe that the attackers had previously obtained deep inside knowledge of the bank's network and systems. Similarly, they obtained an understanding of the processor's environment, and of the card management software and how these systems could be used to manipulate a debit card's sensitive properties such as its overdraft (OD) limit and its Risk Rating. These two parameters are needed to determine the account's OD limit and therefore how much money the account holder can withdraw.

It should also be noted that the attacker's tradecraft suggests involvement of organized cybercrime groups; for example, the attackers successfully wiped the Master Boot Record (MBR) of the hard disk attached to the main Windows system used in this attack. They used specialized malware intending to thwart any future forensic examination of the system.

It goes without saying that the adverse negative impact of this incident was felt by both the bank and the processor:

- The direct dollar value of the loss incurred by the bank pales in comparison with the harder to quantify intangible losses suffered because of loss of trust and goodwill with its customers, partners and regulators. Also, the bank customers' money remained intact as the debit cards that were used for ATM withdrawals were issued against the newly created rogue accounts, none of which had any balance since they were set up.
- In the case of the processor, while no direct monetary loss was incurred, the processor likely lost much more in terms of erosion of trust in their services both with the regulators and their clients (other banks).

Recommendations

- Banks are advised to prepare a well-documented and tested Incident Response Plan (IRP) so they are better prepared to deal with such incidents swiftly and effectively.
- In addition to implementing an effective (but inherently reactive) IR Plan, banks are also advised to consider setting up a proactive program for Managed Detection & Response (MDR), also known as threat hunting, which would allow banks to detect threats early on, and mitigate them before they have a chance to realize their full potential.
- The success of these cyber-attacks may be attributed to failures in both technical and non-technical controls, for example, the lack of coupling between the Core Banking System and the Third-Party Card Management System. Had these systems been integrated properly, it would have been much simpler for the changes to the debit card properties to be red-flagged and blocked by the bank prior to successful monetary theft. Another example of a non-technical control failure is that several accounts on the Card Management System were allowed to both "raise a request" for a change to be made, and to "approve" such a change. This is in clear violation of the very commonly used type of control in banks and banking applications called Maker-Checker control (or the 4-eye principle). Therefore, banks are advised to undertake not only a proactive cyber security risk assessment exercise, but also to undertake a holistic "business process" risk management exercise to detect and mitigate these types of control weaknesses.
- From a technical standpoint, success of these cyber-attacks may be attributed to the following reasons:
  - First, the attackers were able to successfully spear phish and socially engineer bank employees to get an initial foothold in their networks.
  - Second, the attackers took advantage of the common approach of setting the same password for "Local Administrator" accounts for all the systems in the Windows network, and the tendency of the systems administrators to use the "Domain Administrator" account (over the network) to perform routine tasks, to compromise other systems in the Windows network and eventually obtain the "Domain Admin" credentials.

For these reasons, we recommend:

- A different approach (e.g. Windows LAPS) to managing Local Administrator account credentials for the systems in their Windows networks.
- Restrict by policy the use of the Domain Admin account over the network unless absolutely necessary.

Indicators of Compromise

FILES

Table 1: *Indicators of Compromise (Files)*

File name	SHA256 Hash (malicious Files only)	Type
plink.exe	5A21A83DFB5822301896A696F3A1A3E8207BF541E11CD1F2BBB7BC666251D8C7	Legitimate tool but malicious usage
netscan.exe	5748BFB17E662FB6D197886A69DF47F1071052C3381EB1C609A2BC5DBA8C2992	Legitimate tool but malicious usage
crss.exe	D845AF9B15052D49CBE67960AF2A9E51EEAD4D1E21A0DE5C372D4925BA8E1B62	Malicious
adobeArm.exe	DAAB0E5CF3D968B4144B781793763CC6672B30FACC5AF061D0469D6DFFFDA967	Malicious
dropper.exe	DF8948696BB8759EDE500A6A27CE788F1438D1A57F114709D7239865C728B22C	Malicious
servicePS1.txt	589B49D72115A24A0F898E3A5165AFF13BE29EA4A6190977BD046B8657C0D994	Malicious
lor2.exe	97A34BCECF276F9B0E16770D43CEBB2AA3A2FACB47081507DF44A961E932220D	Malicious
java.exe	EED138E53A748EC82A99633BC19020AE6C1D0F609CE3D6555389FB34437EBC02	Malicious
sys64.dll	8A80CA46C0C18CC9B93D5130293A527AA8A925179FAA46597DDD087CD5B1A49F	Malicious
mpk.exe	1940C9C9BFBBD64BA7079178CB819E3253E7057EAA8BEA136A99C90C9436782E	Legitimate tool but malicious usage
mpkview.exe	8086C8836EBEDE1E7FCF3DEBDC009B0982193DF684A55047237C2112DD376AEA	Legitimate tool but malicious usage

IPS/DOMAINS

Table 2: *Indicators of Compromise (IPs/Domains)*

Host	Usage	Geo Location
192.52.167.228	C&C, Backdoor reverse connect IP	United States
192.52.167.28	C&C, Backdoor reverse connect IP	United States

Trustwave®

trustwave.com

PSBH_1017