Cashing in on ATM Malware

A Comprehensive Look at Various Attack Types

Trend Micro Forward-Looking Threat Research (FTR) Team
and Europol's European Cybercrime Centre (EC3)

A **TrendLabs** Research Paper

Written by:
David Sancho and Numaan Huq of Trend Micro Forward-Looking Threat Research (FTR) Team, and Massimiliano Michenzi of Europol's European Cybercrime Centre (EC3)

Contents

6
From Physical Access to Network-based Attacks: How ATM Malware Has Evolved

8
ATM Infrastructure – How to Move Around an ATM

14
Physical ATM Malware Attacks

20
Network-based ATM Malware Attacks

27
Other Noteworthy ATM Malware Attacks

30
The Perpetrators of ATM Malware Attacks

36
Conclusion

Foreword

April 2016 saw the first joint industry – law enforcement report by Trend Micro and Europol highlighting the emerging threat of ATM malware. That report gave a detailed analysis of the developing threat as well as the actions required to tackle this type of crime. The forecasts of that report have unfortunately proved to be accurate, with a significant growth in this crime phenomenon having been observed both in complexity and in geographical distribution.

The 2017 updated report shows that the malware being used has evolved significantly and the scope and scale of the attacks have grown proportionately. While industry and law enforcement cooperation has developed strongly, with a significant number of major arrests being made, the crime continues to thrive due to the major financial rewards available to the organized crime groups involved.

This report assesses the developing nature of the threat. I hope that it serves as a blueprint for future industry and law enforcement cooperation.

Steven Wilson

Head of Europol's
European Cybercrime Centre (EC3)

Martin Roesler

Senior Director of Trend Micro Forward-Looking Threat Research (FTR) Team

ATM malware attacks in various parts of the world continue to make headlines and cause significant costs to the financial industry. In the bigger scale of things, their persistence demonstrates the concerns that are attached to digital ATM security. We can gather that the use of ATM malware is becoming more commonplace, with cybercriminals constantly improving their attack methods in hopes of remaining undetected and unapprehended. This poses a growing problem to financial institutions and law enforcement agencies. However, together we can raise the bar on security.

In this joint report covering the different ATM malware families and attacks currently in existence, both Europol's European Cybercrime Centre (EC3) and Trend Micro's Forward-Looking Threat Research (FTR) team aim to raise awareness across the financial industry and hopefully help authorities to dismantle cybercrime syndicates that cause hundreds of thousands of dollars in losses around the world.

As ATM malware attacks have progressed beyond mere physical access, concerned organizations need to be more vigilant than ever and adopt necessary protections. To that end, our report presents details on ATM malware developments, attack types we have seen over the years, and the techniques organized crime groups use to orchestrate their activities.

Together with our security expert partners at Europol's EC3, we at Trend Micro believe that threat intelligence is a vital component of the continued and overarching digital security and strategy. We hope that members of the financial industry and law enforcement find this comprehensive report informative and useful in implementing better cybersecurity efforts.

ATM malware is one of the digital threats that have been around for a while now, with the discovery of the first known variant dating back to 2009. It should not be a surprise that it has become a mainstay in many cybercriminals' arsenal because it can, plainly put, steal cold, hard cash.

We have seen time and again how cybercriminals plant skimming devices on automated teller machines (ATMs), even those exposed in public sight, and how they use other physical attacks for quick gains.

However, as cybercriminals continue to aim at siphoning off considerable profits, it only makes sense that they would progress to targeting ATMs via networks. After all, finding a way to bypass security and infiltrate the financial institutions' networks promises a bigger payout.

Couple that motivation with the fact that many ATMs run on outdated operating systems, and you get a compelling reason for the sustained cybercriminal use of ATM malware. Such operating systems are vulnerable since they have already reached end of support, meaning there will no longer be security updates and hotfixes provided for them. Consequently, machines that rely on obsolete operating systems are highly susceptible to attacks.

In this paper, we explore in detail the different known ATM malware families and attack types (physical and network-based) and how attackers operate their way to and around their target infrastructures.

From Physical Access to Network-based Attacks: How ATM Malware Has Evolved

In 2016, we published a non-public paper, in which we described in detail known malware families that were specifically targeting ATMs. In that paper, we focused on the way those families were able to subvert the ATM vendors' application programming interfaces (APIs) and the common eXtensions for Financial Services (XFS) API in order to communicate with the ATM-specific hardware: mainly the card reader and the money cassettes.

Back then, we observed that the main infection vector was purely physical: The criminal had to physically open the casing of the ATM and access the machine's internals to boot up from an external USB or CD. While this strategy is certainly still in use today, we have recently started to see the use of a new access point that we already alluded to in our previous paper: the network.

Although we speculated that this could happen, we could not foresee how close we were from it becoming a reality. As banks are starting to realize how much at risk they are from physical ATM attacks and therefore take steps to protect their machines accordingly, the attackers are catching up with alternative infection vectors. Enter network-based ATM attacks.

Network infections require more work and planning on the side of the attacker, with the difficulty lying in the challenge of accessing the ATM network from the main bank's network. In a well-planned network architecture, these two should be separated and accessing one from the other should involve bypassing firewalls and possibly other security elements. Sadly, some banks do not have this network separation. Even if the two are segregated, in some known incidents, the criminals have managed to attain such a tight foothold on the bank's network that they were able to install software on the ATMs from the main network.

For the purpose of giving the reader an overview, we will be describing all known attacks in two broad categories:

1. Those attacks whose way of entry into the ATM is by physical means. In these incidents, criminals usually open the machine's case with a generic key or by force; and

2. Those attacks that manage to access the ATMs via the network. These attacks normally involve hacking into the bank's corporate network first.

After those two sections, in a third part, we will describe two more attack types that are more ad hoc and not quite as common. We believe these two, though rarer, are worth knowing about because if they have happened in the past, chances are they might still pose some risk to ATM installations in the future. For the sake of completeness, we also describe here a criminal tool that was discovered and seemed to have been part of the testing elements while developing some of the attacks described above. Although it was never part of an incident, this illustrates how criminals test their capabilities before launching the real attacks against their targets.

In the last part of the paper, we talk about the perpetrators of these attacks. Although attribution is a thorny issue, our discussion is more about the overall landscape and a brief analysis of the business models that lead criminal outfits to mount these kinds of attacks.

As a reminder with regard to the attacker's objectives, all of the known ATM malware attacks provide the attackers a way to install arbitrary programs on the cash machines in order to empty their cash cassettes (i.e., jackpotting the machine), log all customer card transactions (i.e., virtual skimming), or both.

ATM Infrastructure – How to Move Around an ATM

The primary goal of ATM malware is to connect to and control peripheral devices inside the ATM in order to withdraw stored cash and/or collect information from bank customers. It is therefore important to understand the physical design of an ATM in order to understand how ATM malware attacks work.

An overly simplistic yet accurate description of an ATM is this: a computer system connected to a secure vault encased inside a housing unit. ATMs are complex devices with interconnected peripherals that provide bank customers with a range of banking services such as cash withdrawal and deposit, money transfers, and bill payments. ATMs come in all shapes and sizes, but their internals have a similar architectural layout. The following diagram illustrates some of the basic elements of an ATM:

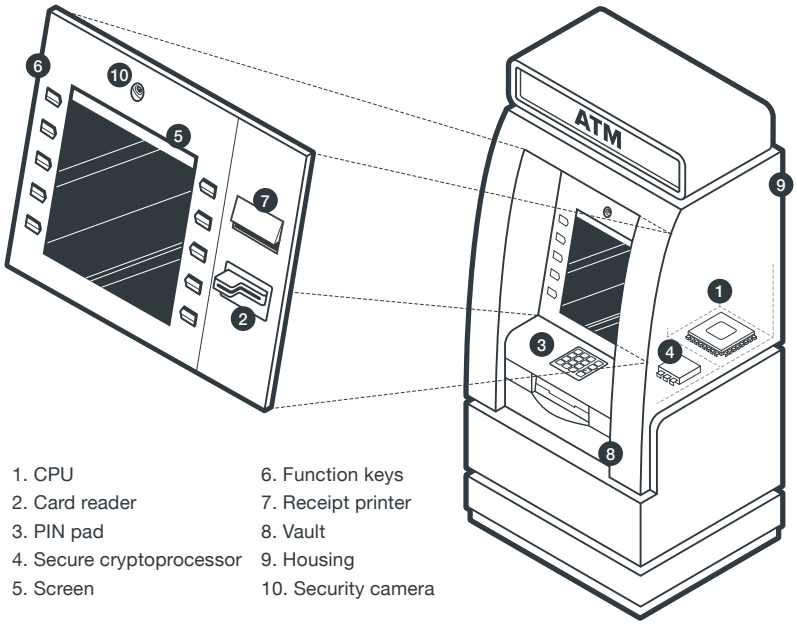

Figure 1. Components of an ATM

ATMs have the following components:

1. **Central processing unit (CPU):** Controls the user interface, handles communications, manages peripheral devices, and processes transactions.

2. **Card reader:** A magnetic stripe card or chip card reader – accepts as input both debit and credit cards.

3. **PIN pad:** An encrypting PIN pad (EPP) that encrypts identifiers such as the PIN entered on the keypad.

4. **Secure cryptoprocessor:** Encrypts and decrypts secure communications. Transactions are encrypted using AES or 3DES encryption algorithms.

5. **Screen:** Displays the graphical user interface (GUI) the customer uses to interact with the ATM. Some newer ATMs have touchscreen displays with virtual function keys.

6. **Function keys:** Mounted beside the display or touchscreen, they provide access to menu items, navigation, and commonly used functionality.

7. **Receipt printer:** Prints records of transactions. Some ATMs also support passbook printing.

8. **Vault:** The most important component of an ATM, it is constructed from high-tensile strength steel. It has a cash-dispensing mechanism, a deposit mechanism with check processor and bulk note acceptor, journaling system for tracking cash in/outflows, cash cartridges/cassettes for storing cash, and a locking mechanism that secures it.

9. **Inner housing:** A customized machine steel case. The outer housing is made of very hard thermoformed acrylonitrile butadiene styrene (ABS) plastic and is decorated with the bank's logo.

10. **Security equipment:** The ATM might also have a surveillance camera, security sensors (magnetic, thermal, seismic, and gas), speakers, and indicator lights.

ATMs have moved from using custom hardware to off-the-shelf PC hardware, such as USB, Ethernet and IP communications, and Windows® operating system (OS). The decision to switch architectures is most often motivated by a lower cost of ownership: from cheaper components to better support and interoperability with commercial software.

A majority of ATMs installed worldwide still run either Windows XP or Windows XP Embedded. Some of the older ATMs run Windows NT®, Windows CE®, or Windows 2000. Microsoft® support for Windows XP ended on April 8, 2014. Extended support for Windows XP Embedded ended on Jan. 12, 2016, and extended support for Windows Embedded Standard 2009 is scheduled to end on Jan. 8, 2019. This means that there are at least hundreds of thousands of ATMs running an OS that no longer receive

software patches for new vulnerabilities or will soon have security patch updates discontinued.

Application programs running on ATMs use XFS, middleware for communications with the peripheral devices. XFS and the impact of middleware will be discussed in greater detail later.

ATMs are connected to the network via ADSL or dial-up modem over a telephone line or direct leased line. Low-level network communication protocols used by ATMs include SNA over SDLC, TC500 over Async, X.25, and TCP/ IP over Ethernet.[1] ATMs are connected to the interbank networks (NYCE, PULSE, PLUS, Cirrus, AFFN, Interac, STAR, LINK, MegaLink, and BancNet) and communicate via ISO 8583: Financial transaction card originated messages – Interchange message specifications.[2, 3] ISO 8583 has no routing information and is used together with a TPDU header.[4] Transactions are encrypted using either AES or 3DES encryption. All communications between the ATM and the interbank network may also be encrypted via SSL for additional security.

Parallels Between a PC and an ATM

If we think of a modern ATM as a Microsoft Windows PC with a safe box full of money attached to it and controlled by software, we can see how it becomes a lucrative target for malware creators. Nevertheless, there are important differences between a normal desktop PC and an ATM, with the two main ones being the following:

1. The first and most important divergence between a PC and an ATM is that the latter cannot be accessed by normal means. Other than a magnetic card reader and a keypad, there is no easy way to interact with the machine's internal hardware. This implies that any infection would need to use either the card reader or a way to access the internal mainboard to connect an external device.

   Even though there have been successful attempts in using the magnetic card reader to infect ATMs,[5] this is so unusual that it does not even bear further mentioning. The most common infection method requires the criminal to open the physical metal casing and access internal hardware ports. The USB port is the most utilized, but older machines that have a CD/DVD reader have been abused in the same way.

2. The second major difference between ATMs and desktop machines is with respect to network connectivity. ATMs are not usually connected directly to the bank's network and certainly not to the internet. The most common setup is to join the ATM's network with the bank's branch through a virtual private network (VPN). Some standalone ATMs in remote locations are instead attached to the bank's network by means of a satellite connection. This can be a problem if the criminals manage to take over the network infrastructure or if it is not configured securely.

Middleware – The Key to the Safe

The XFS middleware provides a client-server architecture for financial applications on the Microsoft Windows platform, especially peripheral devices such as ATMs, which are unique to the financial industry.[6] XFS is commonly installed in ATMs and widely supported by ATM vendors and financial service providers. The XFS specification defines a software interface that consists of:

- A set of application programming interfaces (APIs)
- A corresponding set of service provider interfaces (SPIs)
- Supporting services for the handling/processing of APIs and SPIs

XFS provides user applications an access interface to the connected peripheral devices and financial services running inside the ATM. Since these devices (PIN pads, magnetic card readers, receipt printers, and cash delivery mechanisms) are complex, proprietary, and difficult to manage, the use of XFS offers a number of benefits for financial institutions and their service providers.

An application that uses the XFS APIs to communicate with a particular service provider — interface for peripherals (e.g., PIN pad, cash dispenser, receipt printer) or interface for services (e.g., interbank network) — can work with a service provider of another XFS-conforming vendor without requiring code modifications. This is the same principle that allows a programmer to use the Windows API to open a file without worrying about what hard disk it uses. This is also the main reason ATM malware writers use the XFS APIs to compromise ATMs: They can easily communicate with the connected peripheral devices, and the malware code becomes portable, i.e., it will run on ATMs manufactured by different vendors with minor code modifications.

The following diagram illustrates the XFS system architecture:

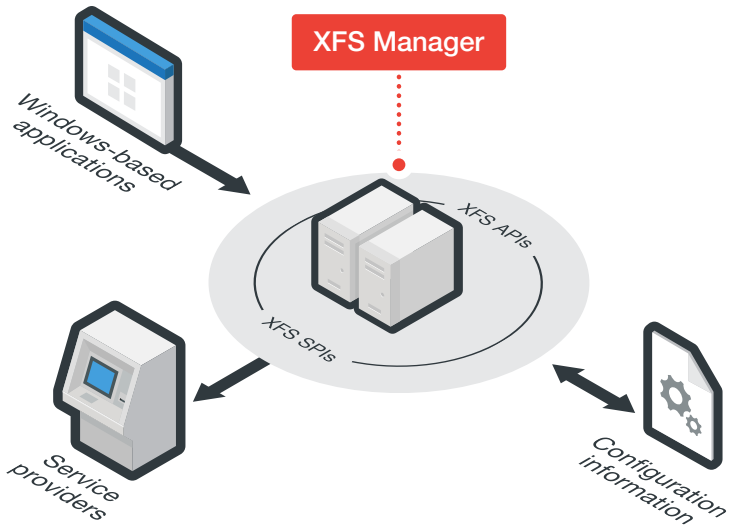

Figure 2. XFS system architecture

Applications communicate with service providers via the XFS Manager using a set of APIs. The XFS Manager maps the specified API to its corresponding SPI. The SPI talks to the peripheral device, and then the user indirectly invokes the SPIs using the vendor-neutral APIs via the XFS Manager. The vendor-neutral API abstracts the user application from device-specific implementations and calls. This is what enables the user application to run on ATMs from different manufacturers with little or no code modification.

The XFS API has the following general set of functions:[7]

- **Basic functions –** such as StartUp/CleanUp, Open/Close, Lock/Unlock, and Execute, that are common to all XFS device/service classes.
- **Administration functions –** such as device initialization, reset, suspend, and resume. They are also used for managing devices and services.
- **Specific commands –** used to request information about a service/device and to initiate service/device specific functions. These are sent to devices and services as parameters for the GetInfo and Execute basic functions.

The SPI is kept as similar as possible to the API. Some commands are processed exclusively by the XFS Manager, and so are not in the SPI.

The Master Plan – Infect and Conquer

There are two main objectives that a malware writer may try to achieve by infecting an ATM box:

- The first objective is emptying the safe of cash. This is colloquially known as "jackpotting" the machine and is the most obvious goal of ATM malware.
- The second objective is logging payment card data while the machine is being used by clients to withdraw funds. To this end, the malware acts like a virtual skimming device.

These two objectives are compatible and there are pieces of malware that can do both. As mentioned above, a successful attack would require either physical access to the ATM's mainboard or a way to access the bank's internal network. In case of infection through the network, the attacker might need additional network access, such as to the VPN or to the particular segment where the ATM network might be located.

Either way, there are two possibilities:

- The attacker has insider knowledge or help (to find out how to access the network or to open the machine's hardware protection).
- In the case of physical hardware access, the machine's internals are accessible by means of commonly available generic physical keys. This is not unheard of; there are plenty of hardware parts in public

places that use generic protection locks merely to deter easy access by passersby. These kinds of locks are usually found "protecting" those devices that are not critical enough to warrant the use of real customized security. Obviously, in the ATM's case, the deployment of generic security locks is a gross underestimation of the risks of allowing easy access to the machine's internal hardware to determined individuals.

Once the criminals have physical access to the USB port or CD/DVD drive, they can insert the device carrying the malware, restart the computer, and boot from it. At that point, the attackers have full control of the machine. The next step usually involves mounting the ATM's internal operating system file structure, copying the malware into it, and modifying the OS so that it executes the malware on a regular boot. The infection is effective after the machine reboots, giving the installed malware access to the special hardware, such as the keypad, the card reader, and the different cassettes that hold the banknotes of each of the denominations. The whole process should take no more than 10 minutes.

The malware attacks we describe in this paper are different from "black box" attacks. In black box attacks, the crooks detach the physical cash dispenser from the ATM, connect it to an external computer, and issue dispensing commands. In both attacks, the criminal accesses the ATM's hardware and physically manipulates it. The big difference is that there is no malware involved in black box attacks and therefore the defense strategies are also markedly different.

Figure 3. Old-school skimming attacks through physical means[8]

Physical ATM Malware Attacks

The first category includes the old-style ATM malware that is typically reported, although the criminals have certainly improved these malicious programs over the years. Also included in this category is a new malware family that has surfaced, which we shall be covering accordingly.

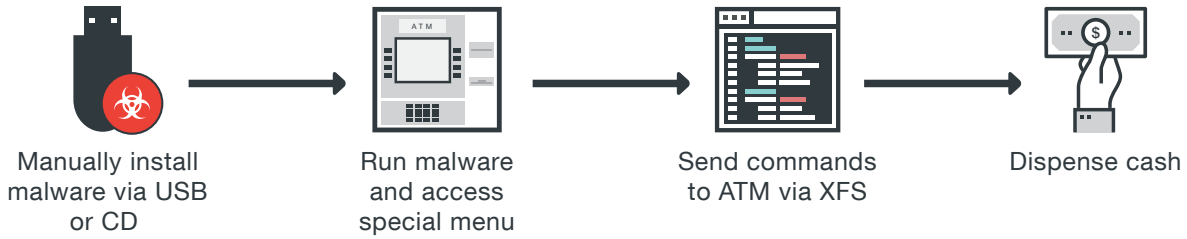

Figure 4. How a typical physical ATM malware attack is carried out

Skimer: The First Known ATM Malware

Skimer was the first known piece of malware to target ATMs. It was first discussed in a SophosLabs blog post in March 2009 and was initially thought to be a credit card skimming malware targeting ATMs.[9] Skimer might have existed as early as July 2007 and was originally found targeting ATMs in Russia and Ukraine.[10] It exclusively targets ATMs manufactured by Diebold®, which confirmed that there was no network-level security compromise in Skimer infection cases. This meant that the malware was manually installed on the ATMs.[11]

Recent ATM malware families directly or indirectly use the XFS middleware to access ATM peripheral devices such as the cash dispenser, PIN pad, and receipt printer. Skimer, on the other hand, uses a Diebold custom middleware, similar in functionality to XFS, to access the ATM's peripherals. It is unclear whether all Diebold ATMs or only older ones run the custom middleware. Also, it is unclear whether or not the Diebold custom middleware interfaces with XFS at all.

Two variants of Skimer have been found in the wild. Skimer v2009 reads user input from the PIN pad, dispenses cash, and collects transaction data. Skimer v2011 is a scaled-down version of v2009 that only does data collection. Both Skimer variants are still actively being used by criminals today.

Key Points:

- Skimer is likely installed manually by accessing the ATM's internal hardware via USB or bootable CD.
- Two variants of Skimer have been discovered in the wild: v2009 and v2011.
- Skimer v2009 reads user input from the PIN pad, dispenses cash, and collects transaction data. It also requires an authorization code before dispensing cash. The operator has to obtain this code from the criminal group controlling Skimer.
- Skimer v2011 is a scaled-down version of Skimer v2009 that only collects data. It writes the collected data to log files and encrypts the files using RC4 encryption. The operators use a "master" card to authenticate the malware. They also use the same card to retrieve the stolen credit card information.
- Both variants of Skimer are still being used by criminals.

Ploutus: Exhibiting Expert Knowledge of ATMs

Ploutus exclusively targets ATMs manufactured by NCR®. The information security firm SafenSoft first disclosed news about Ploutus' existence back in September 2013, when the malware was discovered attacking ATMs in Mexico.[12]

A month after the malware was discovered, a more advanced variant of Ploutus with a modularized architecture[13] was found. The new variant, dubbed Ploutus.B, made it more difficult to discover the infection, as there were now three modules to identify and detect as opposed to only one. This redesign also extended the malware's functionality. In more recent reported cases of infections, a mobile phone had been physically installed inside the ATM's housing. This device received cash withdrawal commands via SMS and then forwarded them to Ploutus.B, thereby minimizing direct physical interaction between the malware operator and the ATM.

The criminals who wrote Ploutus seemed to have expert knowledge and experience in developing software for ATMs manufactured by NCR. However, in October 2016, a new variant, dubbed Ploutus.C, surfaced, adding support for subverting and controlling a specific software framework that managed ATMs regardless of vendor.

Another version of the malware, dubbed Ploutus.D, emerged in January 2017, adding a module to manage the ATM remotely. This new feature might look great in a news header, but it does not seem to make a lot of sense in practical terms. Features such as this (and the SMS receiving feature from Ploutus.B) only makes a second jackpotting operation easier for the criminals, but in reality, most of the banks we have

spoken to disable an affected ATM as soon as the first attack is discovered. Once this happens, the machine is taken offline and forensically analyzed. Unless the banks targeted by these criminals have different policies in place, adding hardware to enable a second attack will only serve to provide more clues to the investigators.

The revealing fact is that Ploutus is being actively developed with new versions coming out fairly often. The new features being implemented suggest that the criminals know the situation of the ATMs and the bank's particular configurations well and that their attacks are targeted operations.

Key Points:

- The Spanish-language strings found in the original Ploutus malware were translated into English in the second version. Some observers are suggesting that this is a strong indication that Ploutus.B is also used in other countries.
- The criminals who wrote Ploutus seemed to have expert knowledge and experience in developing software for ATMs manufactured by NCR.
- Ploutus' initial infection was supposedly done using a bootable CD-ROM. It is highly probable that the lock of the ATM housing was either picked or opened with a key to access the CPU and load a CD-ROM containing the Ploutus malware.
- The original Ploutus malware accepts an eight-digit activation code. This activation code is required to start interacting with Ploutus to withdraw cash. This is a control feature: The low-level operator withdrawing the cash from the ATM needs to call the criminal group to receive the activation ID and proceed with the cash withdrawal.
- Ploutus.B accepts a 16-digit code and when an incorrect activation code is entered, the malware will sleep for 500 minutes, rendering repeated attempts to activate the malware useless. This is yet another built-in security control.
- When the correct activation code is entered, Ploutus.B becomes active for 24 hours. The low-level operator can withdraw cash only during this 24-hour period before requiring a new activation code. Ploutus prints an error message and will not dispense cash after that period.
- Ploutus can read user input from both the ATM's PIN pad and a connected external keyboard. On the other hand, Ploutus.B can read user input only from the ATM's PIN pad.
- Ploutus.B does not have the option to specify the number of bills to dispense. The malware checks the number of bills in each cassette and dispenses all of the cash from the first cassette with 40 or more bills and repeats the process every time it receives a new dispense request.

- More recent Ploutus versions, named Ploutus.C and Ploutus.D, each add features that seem to be aimed at very specific situations or at certain bank installations. This indicates that the malware is being actively developed and the criminals study the targeted banks very carefully.

Padpin-Tyupkin: Stealth in the Dead of Night

Padpin was first discovered in May 2014 by Symantec. This malware family is responsible for the theft of millions of dollars from ATMs across parts of Europe and Southeast Asia.[14, 15] An updated version, dubbed Tyupkin, was discovered in October 2014 by Kaspersky Labs.[16] Padpin and Tyupkin are based on the same code base,[17] as confirmed through code analysis and also by the ATM manufacturer NCR.

Key Points:

- Padpin targets NCR-manufactured ATMs with McAfee® Solidcore installed on the machines.
- Padpin is installed on the target ATM using a bootable CD-ROM. The most probable scenario involves picking the ATM housing's lock and infecting the system through a bootable CD.
- Padpin hooks the ATM's PIN pad and allows control of the malware via the PIN pad.
- By default, Padpin is set to be active between 1 a.m. and 5 a.m. every Sunday and Monday. This indicates that the criminal group behind it operates at night to avoid raising suspicion.
- Padpin allows cash to be withdrawn from the ATMs. It uses session keys to ensure that low-level operators rely on the main criminal group to withdraw funds.

GreenDispenser: A Self-Deleting Malware

GreenDispenser is an ATM malware family discovered by Proofpoint in September 2015 and found to be victimizing ATMs in Mexico.[18] GreenDispenser malware samples were first uploaded to VirusTotal back in June 2015 from India and Mexico. Based on available evidence, there is no connection between these two countries and GreenDispenser. One could theorize that the criminals have outsourced the malware's development to Indian programmers but there is no further evidence pointing to it.

Key Points:

- GreenDispenser will run only if the date is between Jan. 1 and Aug. 31, 2015. The samples we analyzed were created for a time-limited campaign period.
- ATMs infected with GreenDispenser display an error screen with a message: "We regret this ATM is temporary out of service." The infection renders the ATM unusable to regular users.
- GreenDispenser does not restrict itself to targeting ATMs from a single manufacturer only. Instead, the malware is designed to be able to compromise any ATM that uses the XFS middleware.

- GreenDispenser employs a two-stage authentication process before the operator can access the cash dispenser menu.
- The first authentication key is used to disable the error screen. Once the error window is disabled, GreenDispenser displays a new screen with a QR code and menu options: "Enter second key. Press 9 to pause, 8 to permanently delete."
- The second authentication key is dynamically generated using Windows' built-in cryptographic functions. The QR code displays the encrypted second key.
- The operator scans the QR code and either uses a custom app to decrypt the key or contacts the main criminal group for help with decryption. The decrypted second key is entered on the PIN pad to access the cash dispenser menu.
- After each dispensing operation, an updated count shows how many bills remain inside the ATM. GreenDispenser assumes there is only a single type of currency stored in the ATM.
- GreenDispenser has an elaborate uninstall procedure to remove all traces of an infection. After GreenDispenser has been successfully removed from the system, the ATM returns to its regular operation.
- GreenDispenser is probably installed manually in the ATM either by an insider or by members of the criminal group.

Alice: Designed to Empty Safes

Trend Micro first discovered the Alice ATM malware family in November 2016 as a result of our joint research project on ATM malware with Europol's EC3. We collected a list of hashes and the files corresponding to those hashes were then retrieved from VirusTotal for further analysis.[19]

One of those binaries was initially thought to be a new variant of the Padpin ATM malware family. However, after reverse engineering the sample, we found it to be part of a brand new family, which we called Alice.

Several things stand out about Alice. It is extremely feature-lean and, unlike other ATM malware families we have dissected, it includes only the basic functionality required to successfully empty the money safe of the target ATM. Alice only connects to the currency dispenser peripheral and it never attempts to use the machine's PIN pad. The logical conclusion is that the criminals behind Alice need to physically open the ATM and infect the machine via USB or CD-ROM, and then connect a keyboard to the machine's mainboard to operate the malware through it.

Another possibility would be to open a remote desktop and control the menu via the network, similar to the hacking attacks in Thailand and other recent incidents. However, we have not seen Alice being used this way. The existence of a PIN code prior to money dispensing suggests that Alice is used only for

in-person attacks; nor does Alice have an elaborate install or uninstall mechanism — it works by merely running the executable in the appropriate environment.

Alice's user authentication is similar to that of other ATM malware families. The money mules that carry out the attacks receive the needed PIN from the actual criminal gangs. The first command they enter drops the cleanup script, while entering the machine-specific PIN code lets them access the operator panel for money dispensing. This access code changes between samples to prevent mules from sharing the code and bypassing the criminal gangs, to keep track of individual money mules, or both. In our samples, the passcode is only four digits long, but this can be easily changed. Attempts to brute-force the passcode will eventually cause the malware to terminate itself once the PIN input limit is reached.

Given that Alice only looks for an XFS environment and does not perform any additional hardware-specific checks, we believe that it has been designed to run on any vendor's hardware configured to use Microsoft's XFS middleware.

Key Points:

- Alice is a very feature-lean piece of malware focused on emptying the cash from the target ATM.
- Alice does not need installation and can be simply run.
- Alice needs a keyboard to properly accept commands.
- Alice can run on ATMs from any manufacturer.

Network-based ATM Malware Attacks

The second category of ATM malware attacks encompasses those that use the network as their point of entry. In our observation of the different attacks that have been reported, the criminals hack into the bank's corporate network through ways as simple as phishing emails directed at the bank's employees. This is by no means the only way to accomplish such a hack but it is the easiest and therefore the most common one.

Once the criminals have established a solid foothold into the bank's network, they then go on to perform lateral movement to identify and access other sub-networks, including the ATMs. Normally, banks have a clear separation between their corporate network and that of the ATMs, with separate routing and firewalls or other defenses. Some banks do have a flat network, thus making the hackers' lives much easier, but these tend to be a lot rarer.

We will cover five distinct attacks that have been publicized in media outlets:

- The Taiwan attack from July 2016
- Cobalt Strike
- Anunak/Carbanak
- Ripper
- ATMitch

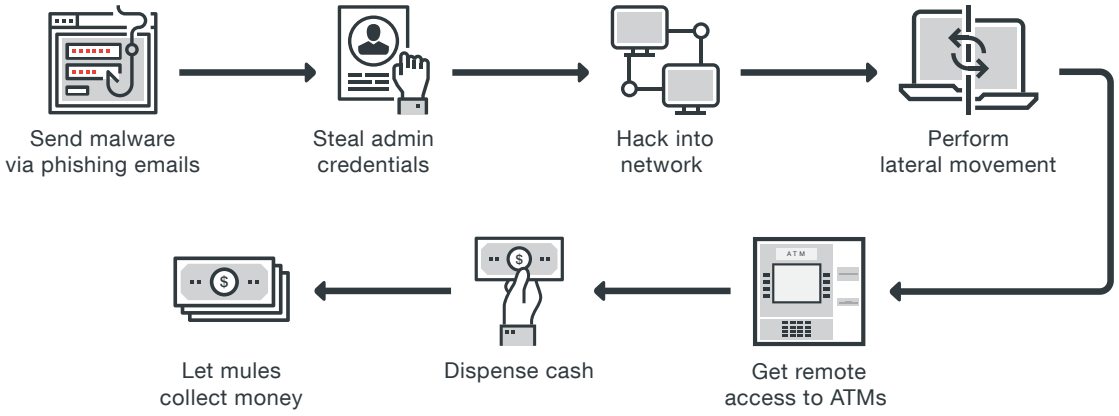

Figure 5. How a typical network-based ATM malware attack is carried out

Taiwan Network Attack: An Elaborate Intrusion

In early July 2016, 41 Wincor Nixdorf® ATMs in Taiwan were attacked and the criminals stole NT$80 million (US$2.5 million) from 22 branches of First Commercial Bank without using cash cards or even touching the PIN pads.[20] The ATM malware used was not initially disclosed, but the bank suspended withdrawals from 1,000 ATMs of the same kind until they could address the situation. Although the criminals were eventually caught and most of the money retrieved, by mid-September the Taiwan police and the Ministry of Justice's Investigation Bureau had revealed the results of their joint forensic investigation. The ATM thefts proved to have been a network attack that was quite sophisticated. The consultancy firm iThome described the attack as follows:

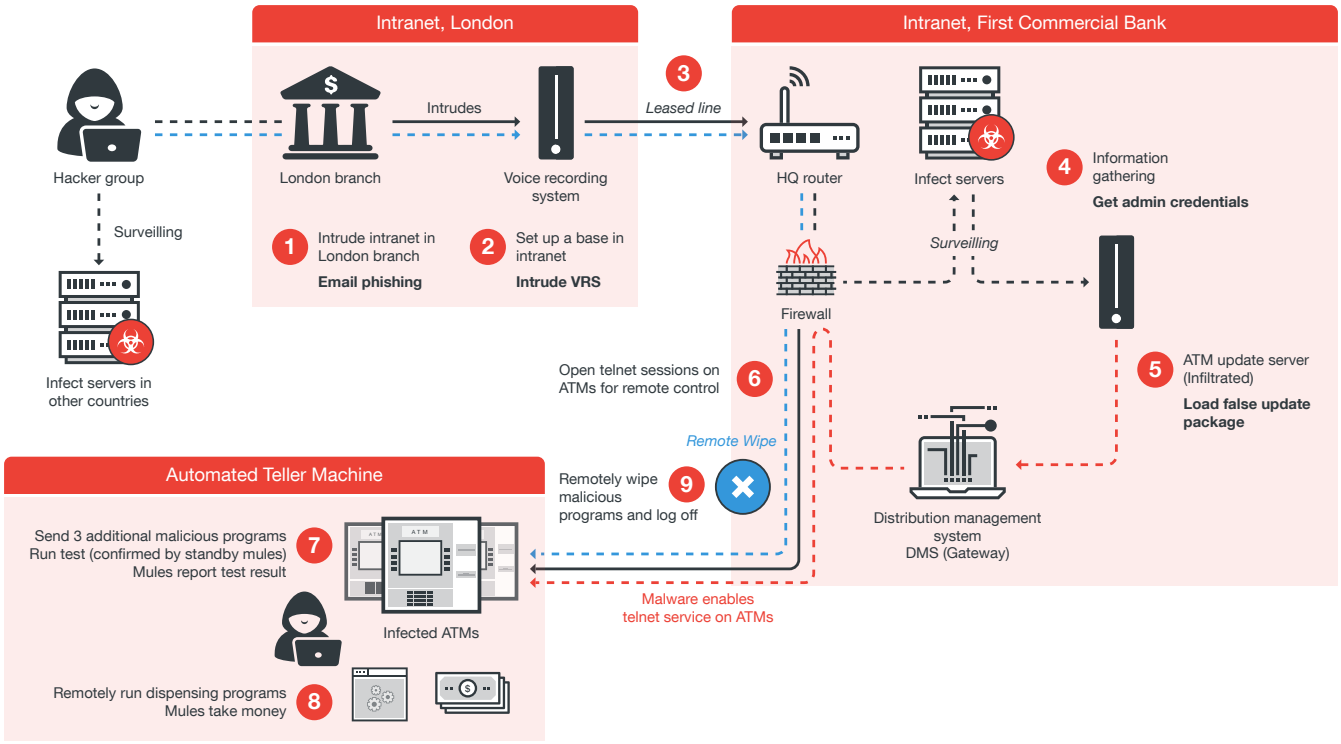

Figure 6. Taiwan network attack

1. Although the initial intrusion to the bank's network started elsewhere, the actual attack to the bank's ATM network began from its London branch.

2. Once inside the London branch network, the hackers accessed the bank's voice recording system and stole the domain administrator's account credentials.

3. Using these credentials, they hacked the VPN over the leased line into the bank's Taiwan branch, bypassing the router and firewall ports at headquarters and taking control of some servers in the Taiwanese network.

4. From these servers, the attackers were able to learn about the intranet topology. They identified the ATM update dispatcher and extracted its administrator credentials.

5. The attackers logged into the ATM update server and set up a fake update package to the distribution management system. They then uploaded it to the ATMs as if it were a real update. This package enabled the telnet service on the ATMs.

6. With the telnet service now turned on, the attackers opened telnet sessions to remotely access and control the ATMs.

7. The attackers uploaded three programs to certain ATMs and ran some tests (using standby mules) to ensure the cash dispenser doors would open. The mules in front of the machines reported the test results back to the remote hackers by using the Wickr Me secure messenger app on their mobile phones.

8. Once the hackers confirmed that the ATMs were ready for the attack, they uploaded and ran modified vendor test tools that dispensed 40 banknotes at a time. (This is the maximum number of notes that may be dispensed at one time due to hardware limitations.) The mules that were standing in front of the ATM took the money, drove to the next ATM, and repeated the process.

9. In the meantime, the remote hackers wiped the malicious programs off the victimized ATM and logged off.

This attack demonstrates how attackers can victimize ATMs via the bank's network. In this case, the network hack was so thorough that the attackers could not only install arbitrary software onto each of the machines (which in itself would have been enough to jackpot them) but also control them remotely via telnet.

Cobalt Strike: Leveraging Security Software

The next incident we are going to discuss has been dubbed Cobalt Strike by the security company who first brought it to light, Group-IB.[21] According to the paper the firm published, the criminals behind the attack first sent phishing emails to a certain Russian bank's employees containing exploits and password-protected archives with malicious executables. According to the same paper, the attackers used a security program called Cobalt Strike in order to penetrate the network, hence the name used to refer to the incident. This software is a legitimate penetration testing suite that white-hat hackers regularly use to evaluate a client's network security. The attackers also used the software Mimikatz to compromise domain and local accounts. Once the attackers had established a foothold in the network with the right credentials, they looked for the employees who could administrate the ATMs via Remote Desktop Protocol (RDP). Once the hackers had taken control of the machines, they could remotely log into any ATM and upload the software of their choice. The program they used to dispense cash seems to have been a custom-made executable that uses XFS to communicate with and empty the machine's cassettes.

Based on Group-IB's report, two different modi operandi were in place for the triggering of the malicious code and cash-out by remote hackers: on-demand while the mules were standing in front of the machines waiting for it to deliver cash, or by the mules themselves, who on their mobile phones have messages with six-digit codes to trigger the cash-outs described in the malware section of this paper (similar to Skimer, Ploutus, GreenDispenser, etc.). These two possible scenarios would imply very different criminal

structures (more or less hierarchical) and different malware features (activation by command line script or a session code), both available at the same time. **Due to the public unavailability of the malware samples found on those ATMs, no additional analysis could be performed in this regard.**

Again, the attackers were able to access the ATM network by means of a hack into the bank's main corporate network. In this case, the ATMs were being remotely managed through RDP and that seemed to be the way in.

Anunak/Carbanak: From Phishing to Lateral Movement

This incident was remarkably similar to the previous one and also seemed to have been carried out against Russian banks. Group-IB and Kaspersky published papers that described the attack from different perspectives. Since Group-IB was the company that dissected the attack and it considered Cobalt Strike and Anunak/Carbanak separately, we assume that the attacks were performed by different attackers. Since we do not have all the information the two firms might have had as incident responders, we are in no situation to contest their claim, although from reading both of their papers, one can see striking similarities between the attacks.

Anunak/Carbanak started out via email phishing with infections enabled by web exploitation kits. Once they had infected a computer with local admin access, the attackers used password-cracking software, like Mimikatz, to increase their foothold in the network. The attackers were able to move laterally within the bank's corporate network and control other servers, which they used to find out domain admin credentials and eventually hack into a domain controller. From there, the hackers could find different network segments, and among those, the computers that could administrate the ATM network. According to Kaspersky's paper, the attackers could then use that special network access to remotely log into ATMs, upload software, and run it.[22] The software they used for dispensing money was a modified version of an ATM vendor's test tool. The mules were also instructed to stand in front of the machine to pick up the cash being dispensed. Unlike with the previous incident, there is more information about this tool, with some screenshots shared in Group-IB's paper.[23] Instead of ATM malware, the software looks like a modified non-legitimate version of a text-mode UI tool made by Wincor Nixdorf (now Diebold Nixdorf®) to test dispensing money on the machine.

Whether or not the attackers were the same as those behind the Cobalt Strike incident is not very important. The fact is that the attackers were able to find their way to the ATM network by means of a hack into the bank's corporate network. By monitoring and examining the network, the attackers in both cases could identify where the segregated ATM network was and they were able to steal the right credentials to remotely install and run software on the victimized machines.

Ripper: Dispensing in Large Quantities

In July and August of 2016, NCR ATMs of Government Savings Bank (GSB), headquartered in Bangkok, Thailand, were attacked with their cash deposits emptied out.[24] The attack used a new ATM malware dubbed Ripper.

NCR determined that the attackers first hacked into the bank's network, and once inside, they used a spoofed version of InfoMindz's Software Distribution and Management System v2.3.0 to distribute the malware to the ATMs.[25] In front of the victimized machines, the mules used modified payment cards to authenticate the Ripper malware on them to retrieve all of the cash in the safes up to 40,000 baht ($1,160).

Ripper shares features with previous ATM malware types (including Padpin and GreenDispenser) in that it can disable the machine's network interface, therefore preventing real-time anti-fraud detection on the bank's side, as well as delete attack-related data from the ATM to defeat post-infection forensics. In the samples we analyzed, this network-disabling functionality was not enabled but since the code is there, we can only assume that the developers have the intention of using this feature in the future or perhaps they have already used it in the past and they only enable it whenever it's needed; we can only guess. Ripper is also capable of infecting the ATMs of Diebold and Wincor Nixdorf (now Diebold Nixdorf) because it communicates with the hardware through the XFS API, allowing it to talk to the cash dispensers of the three vendors without modification. Another interesting fact is that the criminal in front of the infected ATM authenticates Ripper by means of a custom-built card with an EMV chip (similar to the Skimer malware).

What is peculiar about this attack is that it used the corporate network as the way of entry to the ATM network in order to install ATM malware. This is the first of its kind to infect ATMs without the need to physically open the machines. As banks and vendors start fortifying their ATMs against unauthorized physical access to the machines' innards, we believe this is the tendency that criminals will continue with regard to ATM malware.

It is also worth noting that in this new wave of ATM attacks, the weakest link is not the physical and offline defense mechanisms in place. In cases like this, online mechanisms are more applicable to protect banks against ATM victimization. We are talking about firewalls, whitelisting solutions, and other monitoring software installed on ATMs while the regular OS and applications are running.

Another observation is that the first way of entry into the network is again social engineering by way of phishing emails. The weakest link in the attack's chain of events, therefore, is the bank's personnel, particularly those employees who are likely to click on malicious links and open malicious executable attachments.

ATMitch: Reads Text File as Commands

ATMitch was first discovered by Kaspersky in April 2017 as part of an incident in a Russian bank. Only a dynamic-link library (DLL) could be recovered; therefore, we might not have the complete picture of the attack. There are a few facts that we have observed: On the one hand this malware seems to not have a user interface for the criminal to control and only accepts keyword commands sent through the keyboard; On the other hand we also received reports from trusted partners that it receives a text file and interprets the contents as commands to be executed by the malware. However, we don't know how that file would have gotten there. Therefore, we cannot make a final call regarding how the method exactly works.

If we assume that ATMitch is part of a physical attack, the attackers would need to have complete ownership of the machine, either by opening it and attaching an external keyboard on-site or perhaps by stealing the whole thing and bringing it home. The latter is unlikely, given that Kaspersky reports that the malware was retrieved from a real-world attack to a bank.

The likeliest scenario would be to have the malware installed from the bank's network and then control it remotely to send the right commands to dispense cash[26], with a money mule standing at the ready in front of the ATM. This theory is reinforced by the fact that ATMitch does not seem to have an authentication mechanism to control the money mule's ability to go rogue and victimize any number of ATMs.

Key Points:

- ATMitch is only a component of a larger attack. We could not gather other components, so we lack the bigger picture.
- ATMitch receives commands by means of a text file pushed into the system.
- ATMitch does not have authentication mechanisms in place.
- ATMitch supports XFS and therefore can affect ATMs from any vendor.
- ATMitch does not have a menu or user interface. The attacker needs to know the commands to issue.
- ATMitch is possibly part of a network attack against a bank.

Other Noteworthy ATM Malware Attacks

NeoPocket: A Targeted Attack

NeoPocket is an information-stealing malware that targets ATMs manufactured by Diebold. S21sec discovered NeoPocket in April 2014.[27] Unlike the majority of ATM malware, NeoPocket does not steal cash from the ATM as it focuses on data theft only. The malware steals ATM transaction data using a man-in-the-middle (MitM) attack and keylogs user input from specific application windows. This stolen data can be sold in deep web markets for use in creating counterfeit payment cards and carrying out fraudulent fund transfers out of victims' accounts. Because no cash is stolen from the ATM, the compromise tends to remain undetected for prolonged periods and thus allows the criminal group behind NeoPocket to collect large amounts of sensitive data.

NeoPocket is a very specific kind of attack because of its very targeted nature. The attackers know exactly what kind of defenses the machines have in place, and the malware is also designed to run for a short time frame, after which it erases all of its traces. Since its ultimate purpose is to log all card transactions on the machine, its existence would normally go unnoticed by the bank's security team, which makes it all the more insidious. This kind of threat is extremely difficult to fight against and suggests that the criminals have an informant from inside the bank.

Key Points:

- Expert knowledge of Diebold Agilis® is mandatory to understand how the system is set up to successfully carry out the man-in-the-middle attack.
- Because no cash is stolen from the ATM, the compromise tends to remain undetected for prolonged periods and allow the criminals behind NeoPocket to collect large amounts of sensitive data.
- NeoPocket will not execute past a certain date. After that date, the malware will terminate its process but will not uninstall itself.

- Similar to other pieces of ATM malware, NeoPocket requires an installation key. This feature enables the attackers to track and control the infected ATMs and prevents a rogue low-level operator from installing the malware on random ATMs to steal the collected transaction data.
- NeoPocket is manually installed on the ATM. The operator uses a keyboard to input the installation key in the pop-up installation window. NeoPocket does not communicate with the ATM's peripheral devices and does not have access to the ATM's PIN pad.
- NeoPocket logs user input from windows with titles: "Enter the 'A' key," "Escriba la clave 'A'," etc. No information is available about what data is input in these windows and how it is input (keyboard or PIN pad). It is interesting to note that NeoPocket looks for window titles in both English and Spanish.
- NeoPocket has the functionality to terminate the *SMC.exe* process, which is the Symantec Endpoint Protection software. We believe that NeoPocket targets certain financial institutions in Latin America. The use of a Spanish verb such as *ingresar* is a clear sign that the threat comes from Latin America as opposed to Spain, since the word is used in this context in Latin America but not in Spain. Additionally, S21sec confirmed privately to us that the country where they found their sample is located in that region.
- Once operational, NeoPocket receives commands from a connected USB device. The malware uses unconventional methods to receive user commands through this USB device.

Suceful: The Attackers' Test Tool

Suceful is an ATM malware prototyping tool that was first blogged about in September 2015 by FireEye.[28] Two Suceful samples were uploaded to VirusTotal on Aug. 28, 2015; one sample was uploaded from France and the other from Russia. The origin country for VirusTotal submissions can be manipulated using a VPN service, and thus the actual origins of the tool remain inconclusive.

Based on reports about ATM malware families like Ploutus and Padpin-Tyupkin, Suceful was assumed to be a new ATM malware family. After careful code analysis, we have concluded that Suceful is really a prototyping tool instead of an actual piece of malware that would be deployed in ATMs. The fact that there haven't been any cases of Suceful infections discovered or reported in the wild supports our conclusion above. It is highly plausible that Suceful is being actively used in the development of ATM malware samples that are in the wild but are currently undetected.

Key points:

- The GUI shows Suceful is targeting ATMs manufactured by Diebold and NCR. The code reveals no evidence that NCR ATMs were being targeted.
- NCR ATMs are possibly a future target for the Suceful group, which may be the reason button labels for NCR were included in the GUI.

- Suceful can read track data from inserted payment cards.
- Suceful can read user input from the ATM's PIN pad.
- Suceful can control operations of the ATM's door sensors, alarm sensors, generic sensors, key switch sensors, lamp/sign indicators, auxiliary indicators, and enhanced audio controls physically attached to the machine.
- Modifying sensors and indicators unit (SIU) ports suggests that physical compromise of the ATM is a likely option.
- There is no user access control mechanism in Suceful. This is a common feature of ATM malware samples.
- Cash-dispensing functions were not tested in Suceful. The Suceful group may be targeting payment card data only.
- The Suceful group had access to leaked Diebold Agilis XFS manuals.

Although announced with a lot of fuss when it was first found by researchers, Suceful is just a test tool that has never played a direct part in an attack. It does have jackpotting capabilities as well as more advanced features, like enabling or disabling alarms and other special ATM hardware, but it seems to be a private way of testing these features by some malware developer. The Russian-language strings within the tool suggest that it originated from an Eastern European criminal outfit and only made it to the research community at large because of a mistake in the criminal gang's operation.

The only relevance this tool has in the overall ATM malware story is in showing how these criminal gangs understand the programming capabilities that XFS as a platform has to offer and how they can use these capabilities to their advantage. Other than that, the tool is not — and probably never will be — part of a real attack to ATM infrastructure.

The Perpetrators of ATM Malware Attacks

When we look at the earlier malware families and where they originate from, a clear pattern emerges. There are two older malware pieces stemming from South America with Spanish-language strings. These strings are likely to have been written by the developers, so their South American origin is difficult to deny. From those two older threats — Skimer and Ploutus — one specifically targets NCR ATMs, while the other targets Diebold ATMs.

A theory starts shaping up: Those two threats might come from the same source, or else from similar sources, and could have been created to establish comprehensive coverage of the ATM market (the third largest ATM vendor is missing here but apparently it is not so common in this region). Remember that these threats surfaced before XFS made it easier for ATM developers to share software, so the criminals had to write platform-specific code. The one variable that is missing is a version of Ploutus that can only skim, instead of dispensing cash only. If it exists, such a malware has never been seen in the wild. By design, software skimmers are not easy to spot — unlike purely cash-dispensing malware — and they can be active for years before a live sample is found.

The only variable left hanging is the fact that Skimer v2009 was first found in Russia and Ukraine. There is a clear link between v2009 and v2011 in terms of coding style and the way they go about infecting the system and accessing ATM-specific hardware. It is most likely that the original code was developed in Eastern Europe and was reused by the Latin American criminal group that evolved it into a skimming-only attack.

GreenDispenser is a more recent piece of malware from the same region. This particular malware seems to be a dispense-only version of Skimer and Ploutus with multivendor support. Since Skimer and Ploutus are still active, we can theorize that GreenDispenser belongs to a rival group or — given the accumulated knowledge the program seems to have — an ex-member of the first criminal group, now competing against them.

Then, we have NeoPocket, a virtual skimming malware from Latin America. We cannot rightfully associate NeoPocket with any of the previous malware (Skimer, Ploutus, GreenDispenser), since this seems to be much more targeted. NeoPocket looks more like a custom-made operation against a specific bank with the help of an insider, or perhaps the whole attack is an inside job. In any case, it looks like it is completely different from the others we have analyzed.

On the other side of the world, we have a second criminal group coming from Russia, or at least a Russian-speaking region. This Eastern European criminal outfit seems to be behind Padpin and is targeting Russia and surrounding countries first, and then moving on to other Western European countries. We have recently seen how a Moldovan citizen was arrested after moving to the U.K. and victimizing more than 50 ATMs in and around the city of London.[29] This gives credence to the existence of such a group, whose members would be in charge of creating cells in different western countries. We have also heard from private sources about isolated victimization of separate ATMs in tourist towns in Turkey with high Russian affluence. This supports the belief that Eastern European criminal group members are behind Padpin.

How does Suceful fit into this model? It is possible that the same Eastern European criminal group created this tool to test and debug the routines that would make it into the production-level malware, either Padpin or some other undetected Trojan.

The next biggest incident we need to carefully analyze is the one that happened in Malaysia in 2014. There are different theories around it, with the two main ones being:

1. Some sources describe the attacks as coming from South America. The malware involved was also described as being able to dispense 40 bills per batch.[30] This is consistent with the characteristics of Ploutus, which originates from South America. Also, some reports note that the suspects captured on the bank's camera systems were described to have South American looks.[31]

2. A different take is based on the findings of most antivirus vendors that attribute it to Padpin, which would link this incident to Eastern European criminals. There have also been media reports linking the same person arrested in London with the attacks in Malaysia, since the same person was in that country on the dates the attacks took place.[32] We do not have official police reports for this incident, but based on the technical facts we have, it seems most likely that the Malaysian attack was performed by a criminal cell from Eastern Europe using Padpin. The theory of this Eastern European criminal group victimizing foreign sites and holiday resorts is consistent with the picture we painted above.

On Jan. 5, 2016, the Romanian law enforcement agency DIICOT arrested what seemed to be a whole criminal organization[33] that used Padpin to victimize ATMs in the Romania-Moldova region. This is yet another example of the activities of these groups and the way they operate. Whether these criminals created Padpin or they acquired it from other criminals remains unknown.

As things stand, it looks like different criminal groups have already graduated from physical to virtual skimming via malware, thanks to the lack of security measures implemented by commercial banks worldwide. This is common in Latin America and Eastern Europe, but these criminals are exporting the technique and have started to victimize other countries.

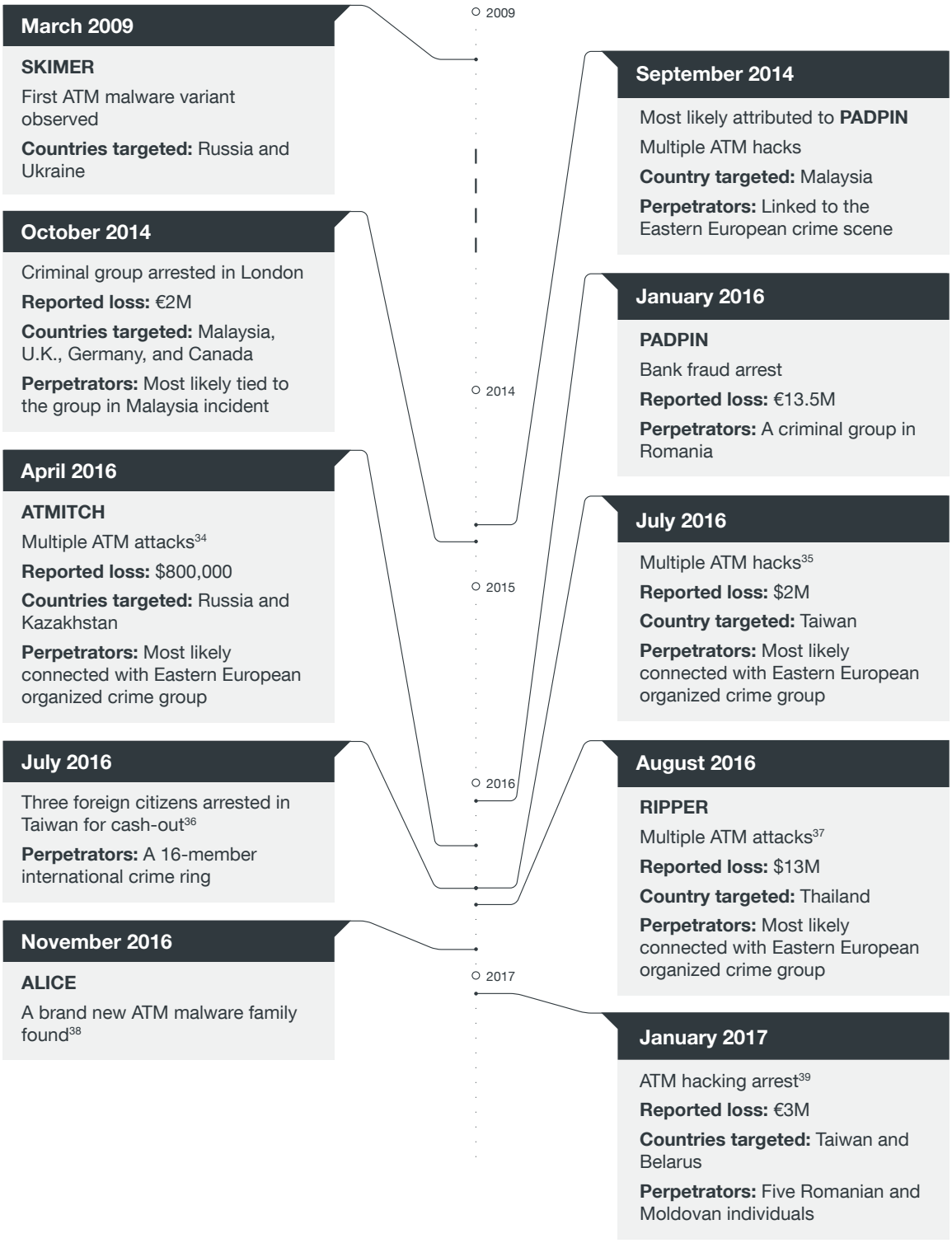

Figure 7. A timeline of noteworthy ATM malware incidents

As described, we have seen network-based ATM attacks take off with both malware payloads and manufacturers' test tools being used to jackpot the machines. Something that all the network attacks appear to have in common is that they all come from Eastern Europe.

The current criminal landscape affecting ATM installations worldwide looks very similar to the Latin American side still busy developing and using their malware, with Ploutus being the most often updated.

On the other side, we still have the Eastern European gangs, with two different business models. One of these business models is practiced by the Padpin developers, who seem to make money by reselling their malware to smaller gangs, which then organize smaller physical attacks in different countries with very short durations, often spanning only one weekend.

The second kind of Eastern European gang that has recently surfaced uses hackers to infiltrate the bank's network, locate and take over the ATM network, and victimize the machines. This is a very different business model from that of the Padpin gang. The appearance of the Ripper gang in the malware scene crosses this gap very nicely: Ripper is the first ATM malware that uses the network as an infection vector. The fact that this newcomer does not use any authentication method suggests that the developers and the criminals are the same group of people. We believe this is the first of others to come.

It is also worth mentioning that the criminals behind the Padpin malware is very active in trying to monetize their creation. These people are reselling in the underground both access to the malware and instructions on how to access the insides of ATMs to enable the infection. They seem to be doing this mostly from the Tor network in order to remain anonymous.

In the same way, the authors of Ploutus — or somebody, who claims to have the source code — are also reselling it. These criminals might not be the original developers, since they do not seem to provide full instructions and they leave it up to the seller to figure out how the malware works. It might also be a fake claim and these people could be trying to swindle other would-be criminals. In any case, the fact remains that ATM malware is picking up notoriety in criminal circles.

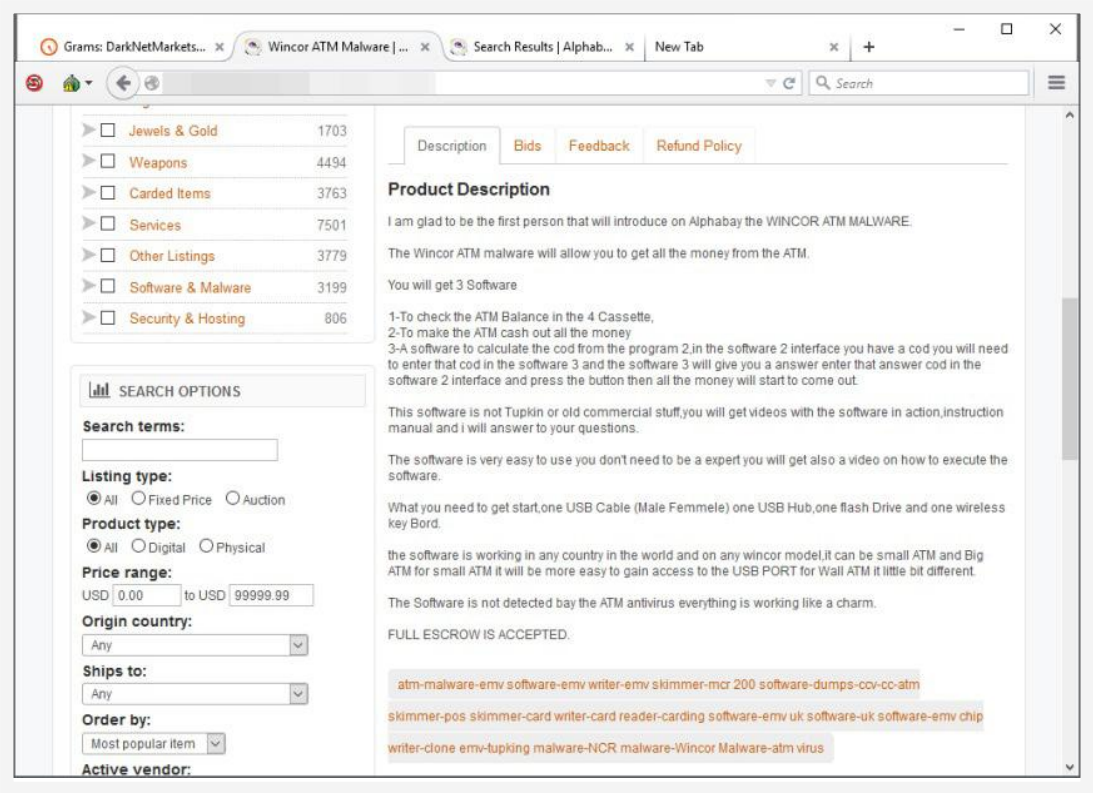

Figure 8. Product description for Ploutus in a listing posted by an alleged author of the malware on a deep web marketplace

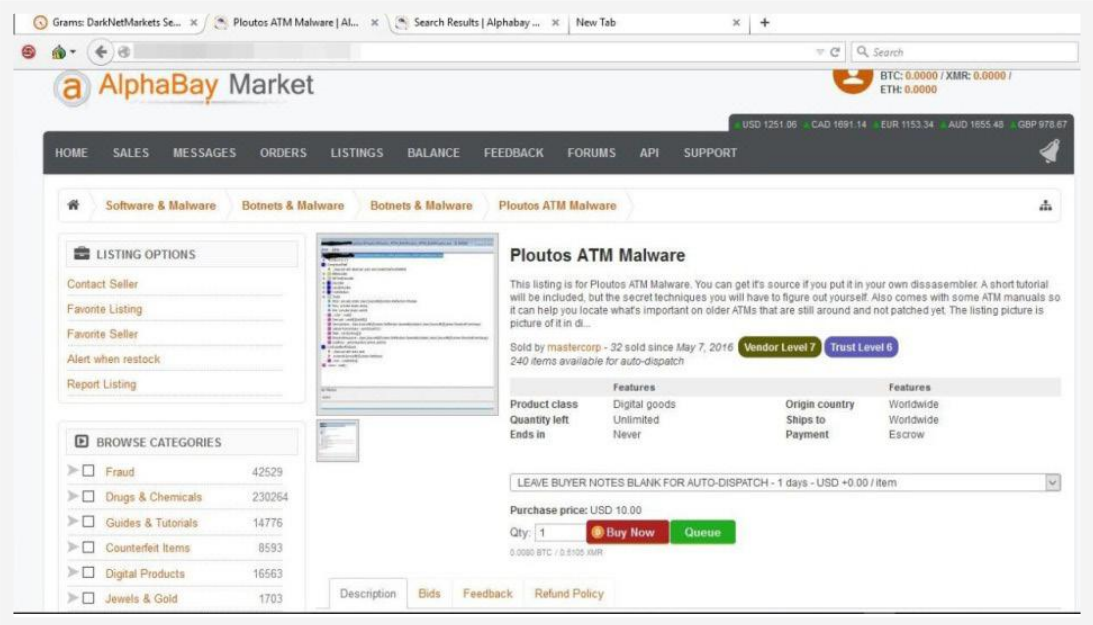

Figure 9. Listing for Ploutus posted by another alleged author of the malware on a deep web marketplace

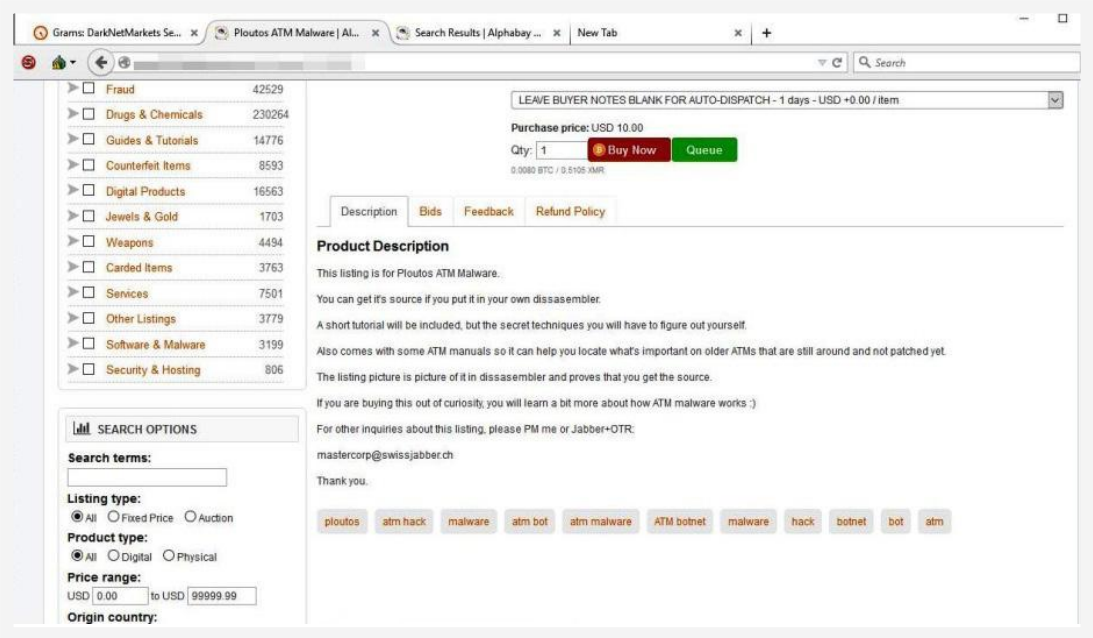

Figure 10. Ploutus is sold on a deep web marketplace by an alleged author of the malware for as little as $10

During the course of this research, we have not seen any noteworthy or prevalent ATM malware attacks in the United States and Canada. This is perhaps because of cybercriminals thinking that they are less likely to get caught by prominent law enforcement agencies if they stay away from attacking bigger countries. However, with amateur to highly skilled cybercriminals continuing to develop, sell, and use ATM malware in the underground, we believe it is only a matter of time before we see attacks in those regions.

Conclusion

Cybercriminals had already discovered that ATMs were vulnerable to software hacking and malware infections at around 2009. Since then, more and more criminal groups have tried their hand at these types of attacks and succeeded. More malware families have been surfacing and this trend has been picking up speed since 2015. Through Trend Micro's joint efforts with Europol, we have presented that 2016 brought us a new and unnerving development: The criminals have realized that not only can ATMs be physically attacked, but it is also very possible for these machines to be accessed through the network. Once cybercriminals manage to install malware and get hold of the network, they can go ahead and steal cash from the machines.

Cybercriminals who compromise networks have the same end goal as those who carry out attacks via physical access: to dispense cash. However, instead of manually installing malware on ATMs through USB or CD, the criminals would not need to go to the machines anymore. They have standby money mules that would pick up the cash and go.

It could be that these are regular criminal groups that already had access to the bank's network and eventually realized that they could hop onto the ATM network. In Ripper's case, though, it shows that some of these criminals are specifically looking for the ATM network as a target and not stumbling upon it by mere chance. These gangs have both the inclination and the technical knowledge to target these machines over any other resources of the targeted bank. While network attacks have not been reported in bigger regions such as the United States and Canada, we believe this to be a new tendency that is probably going to consolidate in 2017 and beyond.

In this respect, the cat is out of the bag. In the past, banks might have thought that network segregation was enough to keep their ATM networks safe from cyber crooks. This is no longer the case. Law enforcement agencies should be well-informed that criminals have ATMs firmly in their crosshairs, and financial organizations need to take more steps to secure their ATM installations by deploying more security layers.

It's also worth pointing out that there has been a considerable effort undertaken by banks, ATM vendors and security companies to create and deploy solutions that solve all of the security gaps outlined in every single attack vector covered in this paper. This does not mean that ATMs can be 100 percent secured because at the end of the day nothing can be. However, a well-designed security plan can go a long way towards ensuring that an ATM installation can become very difficult to exploit and victimize.

References

1. International Organization for Standardization. (2003). "ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values." Last accessed on 29 May 2017 at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31628.

2. International Organization for Standardization. (1998). "ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 2: Application and registration procedures for Institution Identification Codes (IIC)." Last accessed on 29 May 2017 at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=23632.

3. International Organization for Standardization. (2003). "ISO 8583-1:2003 Financial transaction card originated messages – Interchange message specifications – Part 3: Maintenance procedures for messages, data elements and code values." Last accessed on 29 May 2017 at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35363.

4. EFT Lab. (2015). "TPDU – The Transaction Protocol Data Unit." Last accessed on 29 May 2017 at https://www.eftlab.co.uk/index.php/site-map/our-articles/295-tpdu-the-transaction-protocol-data-unit.

5. Brian Krebs. (2014). "Thieves Planted Malware to Hack ATMs". Last accessed on 2 June 2017 at https://krebsonsecurity.com/2014/05/thieves-planted-malware-to-hack-atms/.

6. Wikimedia Foundation, Inc. (2015). "CEN/XFS." Last accessed on 2 June 2017 at https://en.wikipedia.org/wiki/CEN/XFS.

7. European Committee for Standardization. (2000). "Extensions for Financial Services (XFS) interface specification - Release 3.0 – Part 1: Application Programming Interface (API) - Service Provider Interface (SPI); Programmer's Reference." Last accessed on 1 August 2017 at http://read.pudn.com/downloads135/sourcecode/others/573815/01-Application%20Programming%20Interface.pdf.

8. Kazan First. (2015). "С карты 18-летнего челнинца в Елабуге мошенники сняли 340 000 рублей." Last accessed on 2 June 2017 at http://kazanfirst.ru/online/54389.

9. Vanja Svajcer. (2009). "Credit card skimming malware targeting ATMs." Last accessed on 29 May 2017 at https://nakedsecurity.sophos.com/2009/03/17/credit-card-skimming-malware-targeting-atms/.

10. Kim Zetter. (2009). "New ATM malware captures PINS and Cash – Updated." Last accessed on 29 May 2017 at http://www.wired.com/2009/06/new-atm-malware-captures-pins-and-cash/.

11. Graham Cluley. (2009). "More details on the Diebold ATM Trojan horse case." Last accessed on 29 May 2017 at https://nakedsecurity.sophos.com/2009/03/18/details-diebold-atm-trojan-horse-case/.

12. Daniel Regalado. (2013). "Backdoor.Ploutus Reloaded – Ploutus Leaves Mexico." Last accessed on 29 May 2017 at http://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico.

13. Daniel Regalado. (2014). "Texting ATMs for Cash Shows Cybercriminals Increasing Sophistication." Last accessed on 29 May 2017 at https://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication.

14. Daniel Regalado. (2014). "Backdoor.Padpin." Last accessed on 29 May 2017 at https://www.symantec.com/security_response/writeup.jsp?docid=2014-051213-0525-99.

15. FSLabs. (2014). "NCR ATM API Documentation Available on Baidu." Last accessed on 29 May 2017 at https://www.f-secure.com/weblog/archives/00002751.html.

16. Kaspersky Lab's Global Research & Analysis Team. (2014). "Tyupkin: manipulating ATM machines with malware." Last accessed on 29 May 2017 at https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/.

17. Suzanne Cluckey. (2014). "Can the ATM industry stop Tyupkin in its tracks?" Last accessed on 29 May 2017 at http://www.atmmarketplace.com/articles/can-the-atm-industry-stop-tyupkin-in-its-tracks/.

18. Thoufique Haq. (2015). “Meet GreenDispenser: A New Breed of ATM Malware.” Last accessed on 29 May 2017 at https://www.proofpoint.com/us/threat-insight/post/Meet-GreenDispenser.

19. David Sancho and Numaan Huq. (2016). “Alice: A Lightweight, Compact, No-Nonsense ATM Malware.” Last accessed on 6 June 2017 at http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/.

20. Huang Yan Fen. (2016). “【詳細圖解】駭客入侵一銀ATM流程追追.” Last accessed on 6 June 2017 at http://www.ithome.com.tw/news/107294.

21. Group-IB. (2016). “Cobalt: logical attacks on ATMs.” Last accessed on 6 June 2017 at http://www.group-ib.com/cobalt.html.

22. Kaspersky Labs. (2015). “Carbanak APT: The Great Bank Robbery.” Last accessed on 6 June 2017 at https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

23. Group-IB and Fox-It. (2014). “Anunak: APT against Financial Institutions.” Last accessed on 6 June 2017 at http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf.

24. Wichit Chantanusornsiri and online reporters. (2016). “10,000 ATMs nationwide hack-prone.” Last accessed on 6 June 2017 at http://www.bangkokpost.com/archive/10-000-atms-nationwide-hack-prone/1069237.

25. NCR Corporation. (2016). “NCR Security Update: Malware Attacks in Thailand.” Last accessed on 6 June 2017 at https://www.ncr.com/sites/default/files/ncr_security_alert_-_2016-12_network_malware_attack_in_thailand_-_sdms_160829_final_for_review.pdf.

26. Sergey Golovanov. (2017). “ATMitch: remote administration of ATMs.” Last accessed on 6 June 2017 at https://securelist.com/77918/atmitch-remote-administration-of-atms/.

27. Jozsef Gegeny and Santiago Vicente. (2014). “NeoPocket: A new ATM malware.” Last accessed on 31 May 2017 at https://www.s21sec.com/en/blog/2014/04/neopocket-a-new-atm-malware/.

28. Daniel Regalado. (2015). “SUCEFUL: Next Generation ATM Malware.” Last accessed on 2 June 2017 at https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html.

29. Sam Adams. (2015). “Grigore Paladi: Gang member jailed for helping steal £1.6m from cash machines in ONE weekend.” Last accessed on 5 June 2017 at http://www.mirror.co.uk/news/uk-news/grigore-paladi-gang-member-jailed-5115228.

30. Finance Twitter. (2014). “Here’s How Malaysian ATMs were Hacked of RM3 Million by Latin Americans.” Last accessed on 5 June 2017 at http://www.financetwitter.com/2014/09/here-is-how-malaysian-atms-were-hacked-of-rm3-million-by-latin-americans.html.

31. Opalyn Mok. (2014). “Bank in Bayan Baru latest target of ATM hacking.” Last accessed on 5 June 2017 at http://www.themalaymailonline.com/malaysia/article/bank-in-bayan-baru-latest-target-of-atm-hacking.

32. Atiqa Hazellah. (2014). “ATM theft suspect to be charged in UK.” Last accessed on 5 June 2017 at http://www.nst.com.my/news/2015/09/atm-theft-suspect-be-charged-uk.

33. DIICOT. (2016). “Comunicat de presa 05.01.2016.” Last accessed on 5 June 2017 at http://www.diicot.ro/index.php/arhiva/1643-comunicat-de-presa-05-01-2016.

34. Bradley Barth. (2017). “Clues from Russian banking machine theft leads investigators to ATMitch malware.” Last accessed on 1 June 2017 at https://www.scmagazine.com/clues-from-russian-banking-machine-theft-leads-investigators-to-atmitch-malware/article/648423/.

35. Ivana Kottsova. (2016). “Hackers steal millions from ATMs without using a card.” Last accessed on 1 June 2017 at http://money.cnn.com/2016/07/14/news/bank-atm-heist-taiwan/.

36. Faith Hung. (2016). “Taiwan says foreign suspects arrested over $2 million ATM cyber robbery.” Last accessed on 1 June 2017 at http://www.reuters.com/article/us-taiwan-banks-theft-idUSKCN0ZX0N7.

37. Daniel Regalado. (2016). “RIPPER ATM Malware and the 12 Million Baht Jackpot.” Last accessed on 1 June 2017 at https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html.

38. David Sancho and Numaan Huq. (2016). “Alice: A Lightweight, Compact, No-Nonsense ATM Malware.” Last accessed on 1 June 2017 at http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/.

39. Mohit Kumar. (2017). “Police Arrest 5 Cyber Thieves Who Stole 3.2 Million From ATMs Using Malware.” Last accessed on 1 June 2017 at http://thehackernews.com/2017/01/atm-hack-malware.html.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com