Endpoint Protection - Symantec Enterprise

Archived: 2026-04-05 17:53:45 UTC

On September 4, 2013, we were the first to discover and add detections for a new malware targeting ATMs named Backdoor.Ploutus, as reported by our Rapid Release Definitions. Recently, we identified a new variant of this threat and realized that it has been improved and translated into English, suggesting that the ATM software is now being used in other countries.

Symantec added a generic detection for this new variant as Backdoor.Ploutus.B on October 25, 2013, so Ploutus can be detected when it is inactive and when it is running.

Infection methodology

According to external sources, the malware is transferred to the ATM by physically inserting a new boot disk into the CD-ROM drive. The boot disk then transfers malware.

Impact

The criminals have ported the malware to a more robust architecture and translated to English which suggests that they know the same ATM software can be exploited in other countries outside of Latin America.

The number of banks affected by Backdoor.Ploutus.B is out of the scope of this research and it should be handled by the affected parties.

New characteristics for Backdoor.Ploutus.B

The binary name of the English version is “Ploutos.exe” instead of “PloutusService.exe” and it has been changed from a standalone program to a modular architecture.

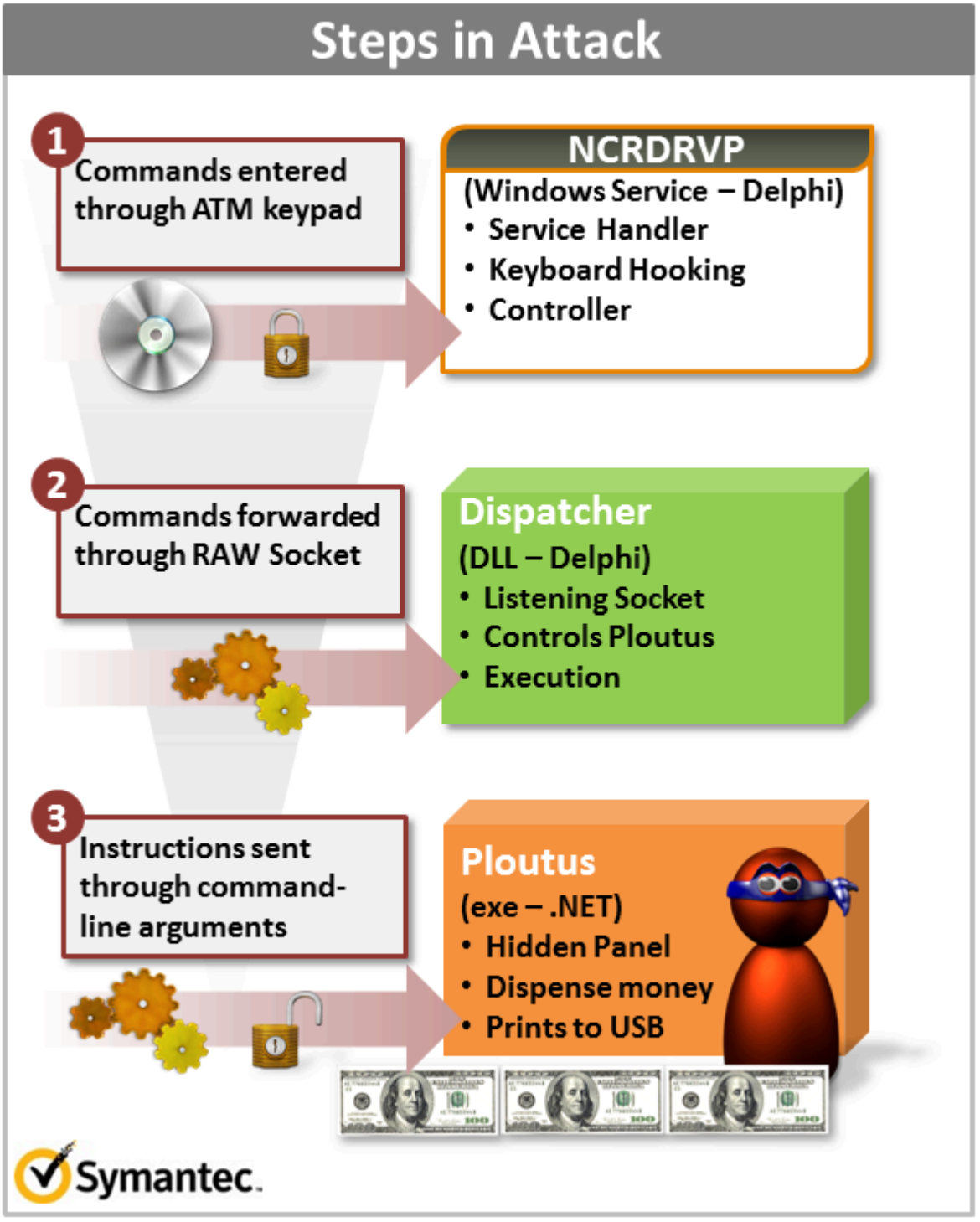

Figure 1. *Ploutus modular architecture*

The new NCRDRVP service is highly obfuscated, hides its malicious actions to avoid detection, and may perform the following actions:

- Install or uninstall the service
- Perform keyboard hooking
- Load the Dispatcher DLL
- Receive commands from the criminals through the ATM keypad
- Forward the commands to the Dispatcher through a raw socket

The Dispatcher will listen for instructions by creating a raw socket. The raw socket is not easy to discover because it is not listed in the TCP or UDP protocols that the system uses. The Dispatcher may perform the following actions:

- Parse the received commands to make sure they are valid
- Execute Ploutus through command line arguments

Backdoor.Ploutus.B has the same interface (the NCR.APTRA.AXFS class) and still concentrates on dispensing money, but there are several differences. This version has the following characteristics:

- It can print the entire ATM configuration if a USB Printer is connected to the machine (the Spanish version sends this information to a log file instead)
- It does not feature a graphical user interface (GUI) and instead accepts commands from the ATM keypad
- It will display a window to the attacker describing the money available in the ATM and a transaction log while dispensing the money
- It does not offer support for a keyboard to be connected to the ATM
- It withdraws money from the cassette with the most available bills, but lacks the option to enter a specific bill amount

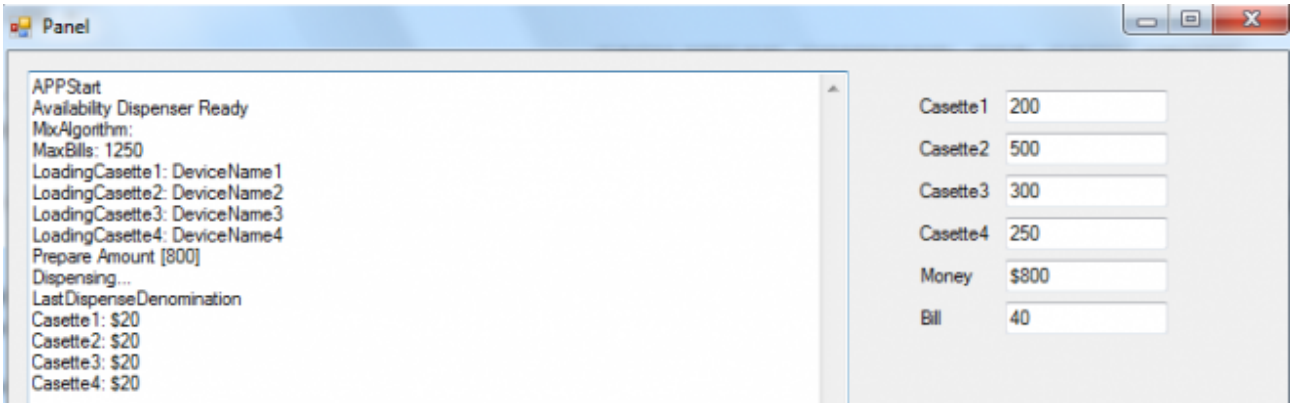

Figure 2. *Window showing money available in compromised ATM*

Actions performed by Backdoor.Ploutus.B

The new version has the same functionalities as the old version:

- Generates a random number and assigns it to the compromised ATM based on the current date at the time of infection

- Sets a timer to dispense money (the malware will only dispense money in the first 24 hours after it is activated)
- Dispenses money from the cassette with the most available bills

Interacting with Backdoor.Ploutus.B through the ATM keypad

The attackers send a 16-digits command code using the ATM keypad which is received by the NCRDRVP Service:

- 123456789ABCDEFG

The code is then forwarded to the Dispatcher through a raw socket. The Dispatcher then sends a 33-digit instruction to Ploutus through the command line:

- cmd.exe /c Ploutos.exe 5449610000583686=123456789ABCDEFG

If the last 16 digits are equal to: 2836957412536985, then Ploutus will generate an ATM ID. If Ploutus generates an ATM ID, the attackers can enter the same 16 digits, but will replace the final two digits in order to perform various actions.

If the final two digits are 99:

- Ploutus will be terminated

If the final two digits are 54:

- The ATM ID will be activated through a code generated based on an encoded ATM ID and the current date. This value is stored in the DATAC entry in the confg.ini file. A valid ATM activation code must be obtained in order for the ATM to dispense cash.
- A timer will be set to dispense the money and the value will be stored in the DATAB entry in the config.ini file.

If the final two digits are 31:

- The ATM will dispense money and print the entire ATM configuration if a USB printer is connected

Dispense process compromised

1. Ploutus will identify the number of dispenser devices in the ATM.
2. It then obtains the number of available cassettes per dispenser and loads them. In this case, the malware assumes there is a maximum of four cassettes per dispenser since it knows the design of the ATM model.
3. Next, it calculates the amount to dispense based on the bill count set as 40, which is multiplied by the cash unit value.
4. It then starts the cash dispensing operation. If any of the cassettes have less than 40 units (bills) available, then it will find the cassette with more available units and dispense all the money from that cassette only.
5. It will open a panel (see Figure 2) that displays the details of the transaction as well as the remaining money in the ATM. It will then hide the panel.

6. Finally, it will repeat step four every time Ploutus is requested to dispense money.

ATMs spewing cash at a location near you

This discovery underlines the increasing level of cooperation between traditional physical world criminals with hackers and cybercriminals. With the ever increasing use of technology in all aspects of security, traditional criminals are realizing that to carry out successful heists, they now require another set of skills that wasn't required in the past. The modern day bank robbers now need skilled IT practitioners on their team to help them carry out their heists. This type of thing isn't just happening in films, it's happening in real life, but this issue does not directly affect ATM users. In this case, financial institutions are the targets. Symantec recommends the following best practices:

- Configure the BIOS boot order to only boot from Hard Disk (no CD/DVD, USB)
- Secure the BIOS with a password so that the attackers cannot reconfigure the boot options
- Consider removing hardware that allows the BIOS to read and start from boot
- Ensure that AV signatures and security solutions are up to date

---