Endpoint Protection - Symantec Enterprise

Archived: 2026-04-05 15:44:22 UTC

Contributor: Val S

It’s well-known that organized crime in Mexico is always finding new ways to steal money from people. Automatic teller machines (ATMs) are one of the common targets in this effort, but the challenge there is actually getting the money out of the machine. The three most common ways to accomplish this are:

1. Kidnapping: Criminals kidnap a person for as long as it takes to withdraw all the money from their account. The time depends on the money available in the account since normally there is a limit on the amount allowed to be dispensed per day.
2. Physically stealing the ATM: Criminals remove the ATM and take it to a location where they can go to work accessing the cash inside. In this scenario, the loss of cash is only one consequence as the criminals would also gain access to the software running on the ATM, which could be reverse-engineered in order to prepare an attack against all ATMs running the same software.
3. ATM Skimming: Devices are placed over the card reader in order to steal personally identifiable information (PII) data like PIN numbers. Fake number pad overlays can also be used to record which buttons are pressed.

While the above scenarios all rely on external factors to succeed, criminals would like nothing more than a way for them to make an ATM spew out all its cash just by pressing some buttons (similar to the demo presented by the late Barnaby Jack at 2010’s BlackHat conference). Unfortunately for banks, it seems as though the bad guys’ dreams may have come true. In parallel investigations with other AV firms, Symantec identified this sample on

August 31, 2013 and a detection has been in place since September 4, 2013. We detect this sample as Backdoor.Ploutus.

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 created an interface to interact with the ATM software on a compromised ATM, and are therefore able to withdraw all the available money from the containers holding the cash, also known as cassettes.

One interesting part to note is that the criminals are also able to read all the information typed by cardholders through the ATM keypad, enabling them to steal the sensitive information without using any external device.

Although no confirmation has been received from other countries being affected by this threat, banks in other countries using the same ATM software could be at risk.

Technical characteristics of Backdoor.Ploutus

1. It runs as a Windows service named NCRDRVPS
2. The criminals created an interface to interact with ATM software on a compromised ATM through the NCR.APTRA.AXFS class
3. Its binary name is PloutusService.exe
4. It was developed with .NET technology and obfuscated with the software Confuser 1.9
5. It creates a hidden window that can be enabled by the criminals to interact with the ATM
6. It interprets specific key combinations, entered by criminals, as commands that can be received either by an external keyboard (that must be connected to the ATM) or directly from the keypad

Actions performed by Backdoor.Ploutus

1. **Generate ATM ID**: Randomly generated number assigned to the compromised ATM, based on current day and month at the time of infection.
2. **Activate ATM ID**: Sets a timer to dispense money. The malware will dispense money only within the first 24 hours after it was activated.
3. **Dispense cash**: Dispense money based on the amount requested by the criminals.
4. **Restart** (Service): Reset the dispense time period.

The list of commands mentioned above must be executed in order, since it must use a non-expired activated ATM ID to dispense the cash.

The source code contains Spanish function names and poor English grammar that suggests the malware may have been coded by Spanish speaking developers.

Interacting with Backdoor.Ploutus through the keypad

As noted previously, this type of interaction does not require an additional keyboard to be connected.

The following command codes, entered using the ATM keypad, and their purpose are as follows:

12340000: To test if the keyboard is receiving commands.

12343570: Generate ATM ID, which is stored in the DATAA entry in the config.ini file.

12343571XXXXXXXX: Has two actions:

1. Activate ATM ID by generating an activation code based on an encoded ATM ID and the current date. This value is stored in the DATAC entry in the config.ini file. The eight bytes read in must be a valid encoded ATM ID generated by a function called CrypTrack(). A valid ATM activation code must be obtained in order for the ATM to dispense cash.
2. Generate timespan: Sets a timer to dispense money, the value will be stored in the DATAB entry in the config.ini file.

12343572XX: Commands the ATM to dispense money. The removed digits represent the number of bills to dispense.

Interacting with Backdoor.Ploutus through a GUI

This method requires the use of an external keyboard.

F8 = If the Trojan window is hidden then this will display it in the main screen of the ATM, enabling criminals to send commands.

After the Trojan window is displayed, the following key commands can be issued by pressing the appropriate key on the keyboard:

F1 = Generate ATM ID

F2 = Activate ATM ID

F3 = Dispense

F4 = Disable Trojan Window

F5 = KeyControlUp

F6 = KeyControlDown

F7 = KeyControlNext

F8 = KeyControlBack

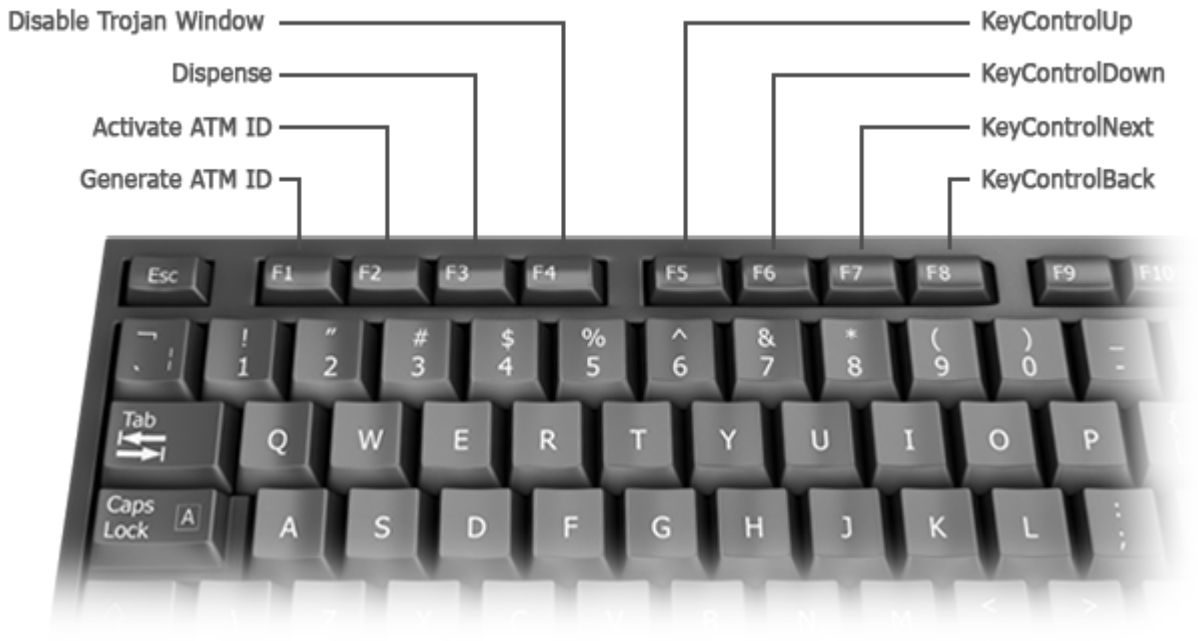

Figure. *Trojan key commands*

Dispense process compromised

It is clear that the criminals have reverse engineered the ATM software and came up with an interface to interact with it, and, although we are not ATM architects, based on the code we have reviewed we can infer that Backdoor.Ploutus has the following functionalities:

1. It will identify the dispenser device in the ATM.
2. It then gets the number of 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 provided, 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, instead of dispensing the amount requested, it will dispense all the remaining money available in that cassette.
5. Finally, it will repeat step four for all remaining cassettes until all the money is withdrawn from the ATM.

ATMs could be spewing cash at a location near you…

What this discovery underlines is 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, possibly at a bank machine near you.
