New Variant of Ploutus ATM Malware Observed in the Wild in Latin America

fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html

Breadcrumb

Threat Research

Daniel Regalado

Jan 11, 2017

8 mins read

Introduction

Ploutus is one of the most advanced ATM malware families we've seen in the last few years. Discovered for the first time in Mexico back in 2013, Ploutus enabled criminals to empty ATMs using either an external keyboard attached to the machine or via SMS message, a technique that had never been seen before.

FireEye Labs recently identified a previously unobserved version of Ploutus, dubbed Ploutus-D, that interacts with KAL's Kalignite multivendor ATM platform. The samples we identified target the ATM vendor Diebold. However, minimal code change to Ploutus-D would greatly expand its ATM vendor targets since Kalignite Platform runs on 40 different ATM vendors in 80 countries.

Once deployed to an ATM, Ploutus-D makes it possible for a money mule to obtain thousands of dollars in minutes. A money mule must have a master key to open the top portion of the ATM (or be able to pick it), a physical keyboard to connect to the machine, and an activation code (provided by the boss in charge of the operation) in order to dispense money from the ATM. While there are some risks of the money mule being caught by cameras, the speed in which the operation is carried out minimizes the mule's risk.

This blog covers the changes, improvements, and Indicators of Compromise (IOC) of Ploutus-D in order to help financial organizations identify and defend against this threat.

Previously unobserved features of Ploutus-D

- It uses the Kalignite multivendor ATM Platform.
- It could run on ATMs running the Windows 10, Windows 8, Windows 7 and XP operating systems.
- It is configured to control Diebold ATMs.
- It has a different GUI interface.
- It comes with a Launcher that attempts to identify and kill security monitoring processes to avoid detection.
- It uses a stronger .NET obfuscator called Reactor.

Commonality between Ploutus and Ploutus-D

- The main purpose is to empty the ATM without requiring an ATM card.
- The attacker must interact with the malware using an external keyboard attached to the ATM.
- An activation code is generated by the attacker, which expires after 24 hours.
- Both were created in .NET.
- Can run as Windows Service or standalone application.

Dissecting Ploutus-D

Ploutus-D (observed in the wild with the filename of “AgilisConfigurationUtility.exe”) can run as a standalone application or as a Windows service started by a Launcher (observed in the wild as “Diebold.exe”). Although multiple functionality is shared between the two components, the main difference is that Ploutus-D is the component with the capability to dispense money.

Launcher – Diebold.exe (.NET)

MD5	C04A7CB926CCBF829D0A36A91EBF91BD
.NET Obfuscator	Reactor
File Size	198 kB
File Type	Win32 EXE
Time Stamp	2016:11:16 04:55:56-08:00
Code Size	199168
File Version	0.0.0.1
Internal Name	Diebold.exe
Legal Copyright	Copyright © 2015
Original Filename	Diebold.exe
Product Name	Diebold
Product Version	0.0.0.1

Table 1: Launcher Properties

This time, the attackers put more effort into trying to obfuscate and protect their code from reverse engineering by switching from .NET Confuser to Reactor. A quick look at how the protected code appears is shown in Figure 1.

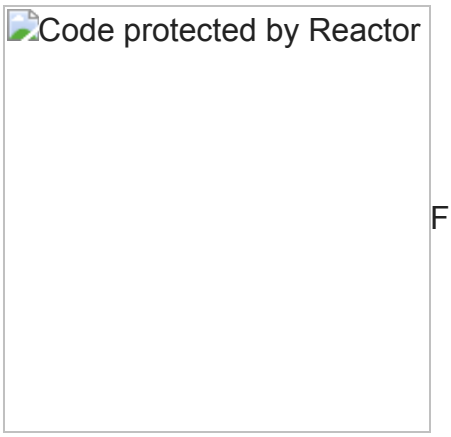

Figure 1: Code protected by Reactor

Inspecting the Launcher

Once the code is deobfuscated, it is easy to understand the internal workings. Before the Launcher execution starts, it will perform an integrity check on itself to make sure it has not been altered.

The Launcher can receive different arguments in the command line to either install as a service, run Ploutus-D, or uninstall from the machine. The service properties can be seen in Figure 2.

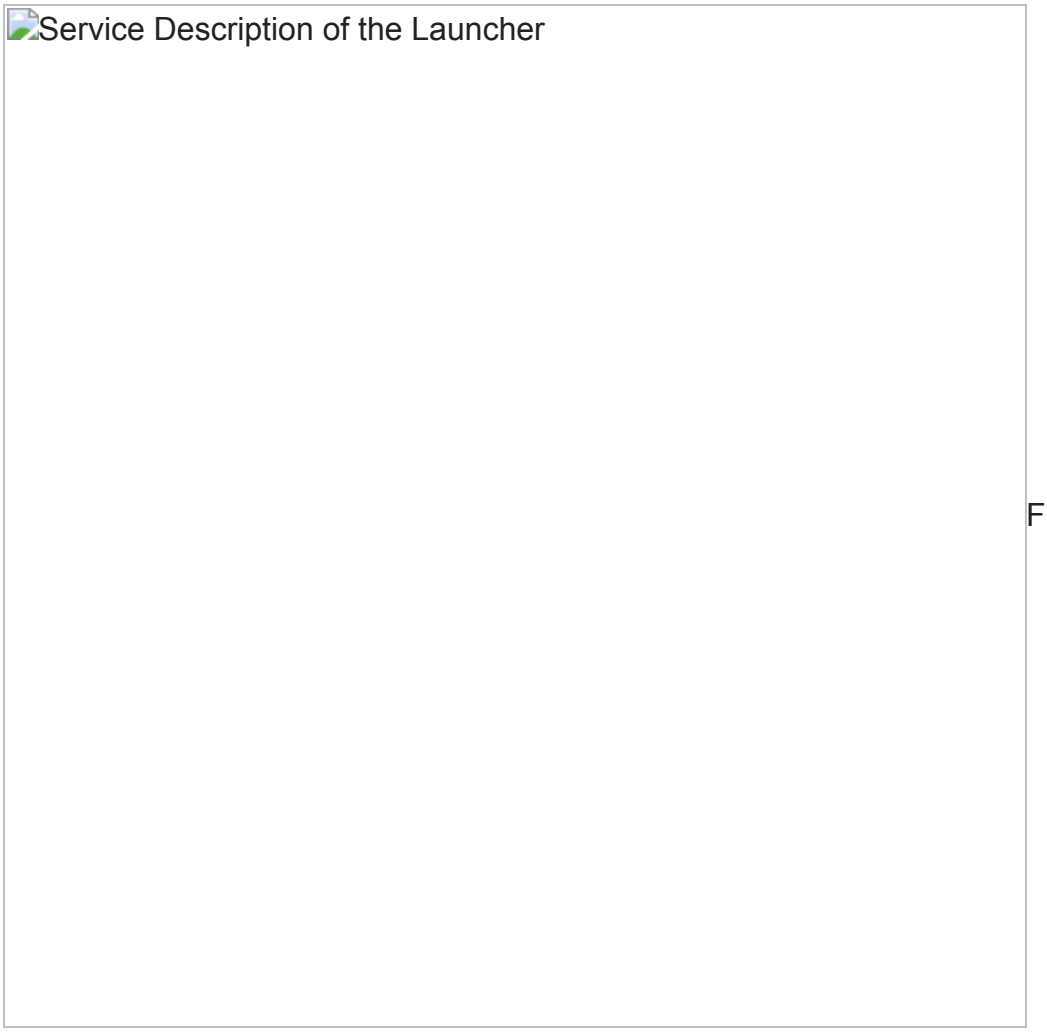

Figure 2: Service Description of the Launcher

Persistence

Using a very common persistence technique, the malware will add itself to the “Userinit” registry key to allow execution after every reboot. The key is located at:

\HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

Interacting with the Launcher

The attacker must interact with the Launcher by attaching a keyboard to the ATM USB or PS/2 port. Figure 3 below shows an example of this setup.

Figure 3: Keyboard attached to the ATM port

Once the Launcher has been installed in the ATM, it will perform keyboard hooking in order to read the instructions from the attackers via the external keyboard. A combination of “F” keys will be used to request the action to execute (see Figure 4).

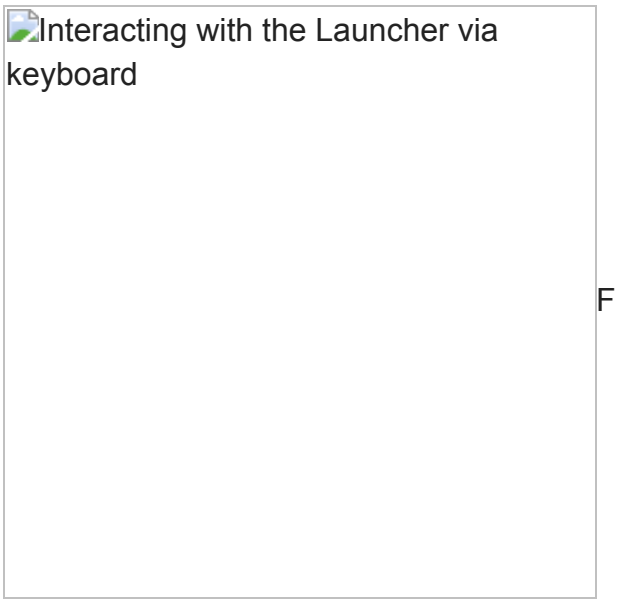

Figure 4: Interacting with the Launcher via keyboard

The main tasks supported are:

- Start programs on demand, some of which are decrypted from the resource section of the Launcher:
  - C:\Program Files\Diebold\Agilis Startup\AgilisShellStart.exe
  - Main.exe
  - XFSConsole.exe
- Kill Processes:
  - NHOSTSVC.exe
  - AgilisConfigurationUtility.exe
  - XFSConsole.exe
- Delete Files:
  - NetOp.LOG – Secure Remote Management solution
- Reboot Machine:
  - “wmic os where Primary='TRUE' reboot”

As seen in Figure 5, a request has been sent to run Ploutus-D (AgilisConfigurationUtility.exe) from command line.

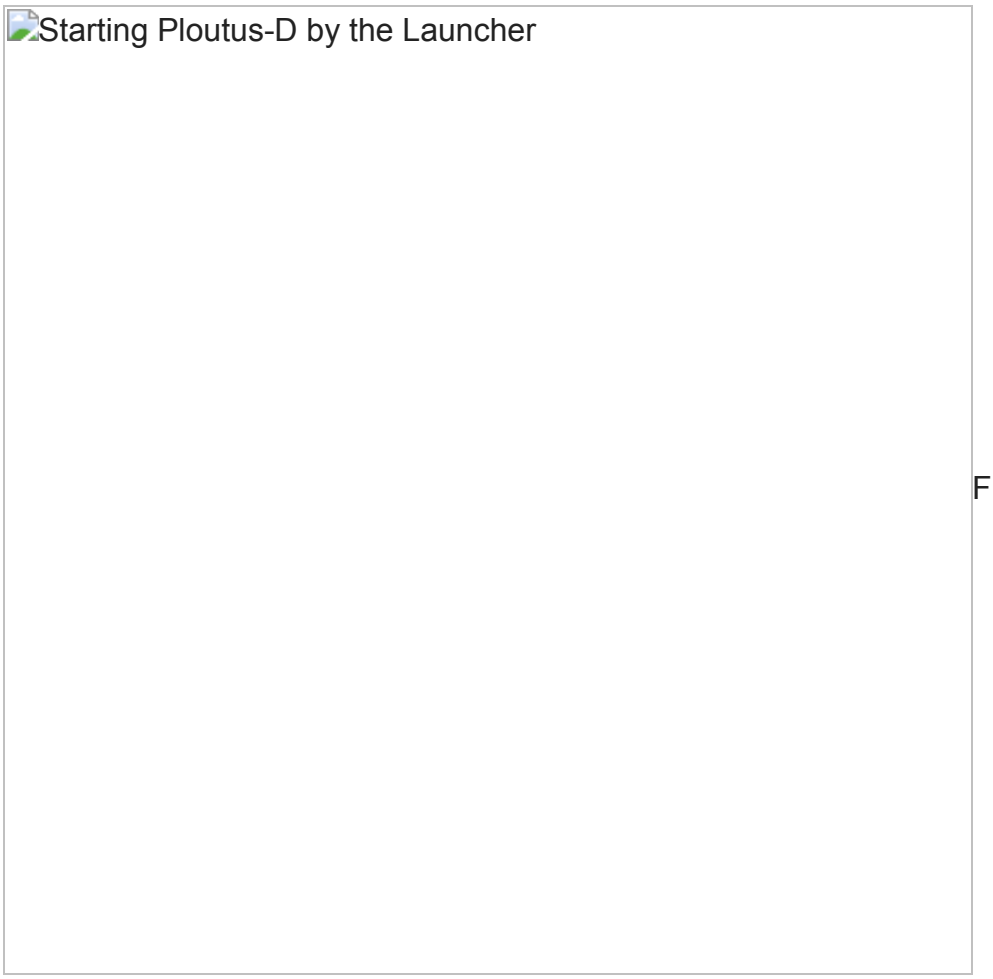

Figure 5: Starting Ploutus-D by the Launcher

Legitimate KAL ATM software is dropped into the system along with Ploutus-D, as shown in the Figure 6. The reason for this is to make sure that all the software and versions needed to properly run the malware are present in the same folder to avoid any dependency issues. The same technique was also used by the first version of Ploutus.

Figure 6: Dropped files by the Launcher
The K3A.Platform.dll DLL will load the Kalignite Platform to allow Ploutus-D to control the ATM.

This shows that the attackers likely have access to the targeted ATM software. They can either buy physical ATMs from authorized resellers, which come preloaded with vendor software, or they could just steal the ATMs directly from the bank's facility. An example of a real incident reported in Mexico is shown in Figure 7.

Figure 7: Attackers physically stealing ATMs

Ploutus-D – AgilisConfigurationUtility.exe (.NET)

MD5	5AF1F92832378772A7E3B07A0CAD4FC5
.NET Obfuscator	Reactor
File Size	274 kB
File Type	Win32 EXE
Time Stamp	1992:06:19 15:22:17-07:00
Code Size	29696
OS Version	4.0
Image Version	0.0
Subsystem Version	4.0

Table 2: Ploutus-D Properties

Similar to the Launcher, this binary also came protected with Reactor obfuscator (see Figure 8).

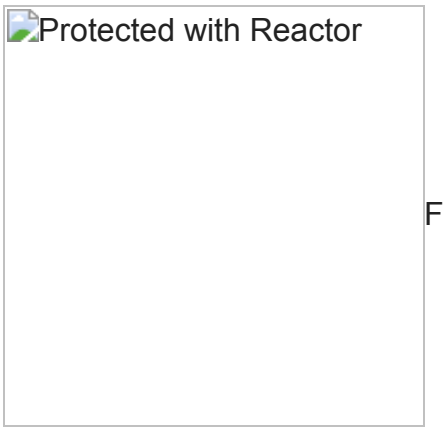

Figure 8: Protected with Reactor

Looking at the unprotected code (see Figure 9), the connection with Ploutus became evident since the names of most of the functions are the same as in the first version.

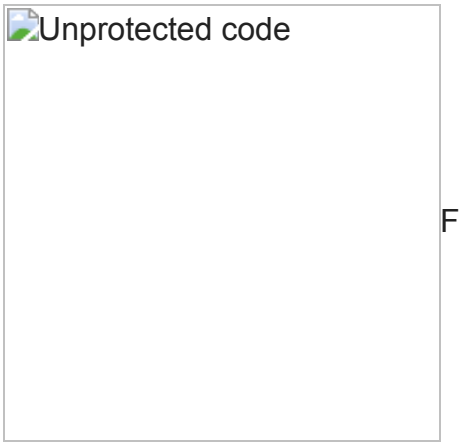

Figure 9: Unprotected code

Ploutus-D will make sure a mutex with the name “KaligniteAPP” does not exist in the system in order to start running. Similar to the Launcher, Ploutus-D will hook the keyboard in order for the attackers to interact with it; however, apart from receiving commands from “F” keys, it will also read from the numeric pad (numbers).

Similar to the previous version, the GUI will be enabled by entering a combination of “F” keys. Then, a valid 8-digit code must be entered in the GUI in order to be able to dispense money. Ploutus-D also allows the attackers to enter the amount to withdraw (billUnits – 4 digits) and the number of cycles (billCount – 2 digits) to repeat the dispensing operation (see Figure 10).

Figure 10: Parsing amount and cycles

The Ploutus-D GUI is displayed in Figure 11. It is configured to list properties of 18 cassettes (C1-C18). Letter “D” shows the status of the cassette and “CV” is a value taken from the registry. The message “Estado:Activado”, which means “State: Activated”, is displayed if a valid code has been entered. The ATM ID and HW_ID are unique to the ATM. The amount to be retrieved is displayed as: “Cantidad: 500” (default value if no amount entered in the GUI). The total amount depends on the currency, which is also calculated by the malware.

Figure 11: Ploutus-D GUI enabled

All the actions are logged into a file with the name “Log.txt”. An extract can be seen in Figure 12.

Figure 12: Log File recording actions

Dispensing the Money

In order for the mule to be able to start dispensing money, a valid 8-digit code must be entered. This code is provided by the boss in charge of the operation and is calculated based on a unique ID generated per ATM, and the current month and day of the attack.

Once a valid activation code has been entered (which expires in 24 hours), the dispensing process will start by pressing “F3” from the external keyboard.

The malware will first identify the cassette’s denomination by querying the registry denomination table from Diebold Dispenser Logical Name “DBD_AdvFuncDisp” at:

\HKLM\SOFTWARE\XFS\PHYSICAL_SERVICES\DBD_AdvFuncDisp\Denomination Table

A similar strategy will be used to get the cassette’s status and type, to make sure they are working properly, and, more important, to identify that it has at least one bill to withdraw.

Ploutus-D will load “KXCashDispenserLib” library implemented by Kalignite Platform (K3A.Platform.dll) to interact with the XFS Manager and control the Dispenser (see Figure 13).

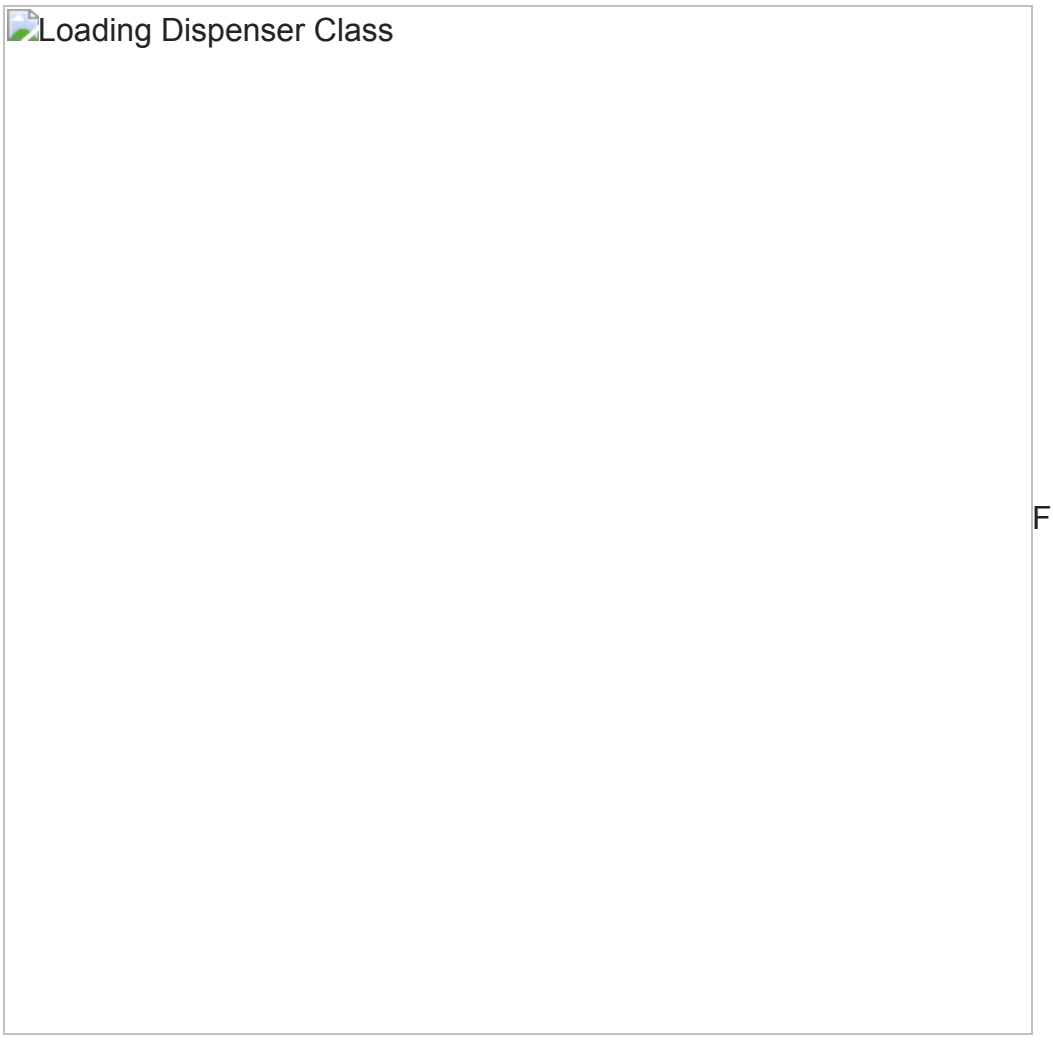

Figure 13: Loading Dispenser Class

Figure 14 shows a graphical representation of the XFS Manager and its interaction with Kalignite Platform via KXCashDispenserLib.

Figure 14: XFS Manager

The knowledge shown in the code to properly implement all the different classes and methods to control the Dispenser suggests that the developers of the malware have either access to real ATMs during the development or they hired individuals with experience coding on these machines.

Expanding Ploutus to other ATM vendors

Kalignite Platform is said to support 40 ATM vendors. Looking at the code to dispense money, the only pieces adjusted to target Diebold are the different registry keys to read the cassette (DBD_AdvFuncDisp) parameters (see Figure 15).

Figure 15: Getting Diebold Cassette parameters
Since Ploutus-D interacts with the Kalignite Platform, only minor modifications to the Ploutus-D code may be required to target different ATM vendors worldwide.

Conclusion

As anticipated in our 2017 predictions report, the use of ATM malware will continue to increase, especially in underdeveloped countries with weaker physical security controls. By leveraging the Kalignite Platform, Ploutus can be easily modified to attack various ATM vendors and operating systems.

Frequently Asked Questions

1. When was Ploutus-D first discovered?
   Ploutus-D was uploaded to VirusTotal in November 2016.

2. Does Ploutus-D target cardholder information?
   No. It is designed to dispense cash from within the ATM.
3. Is Ploutus-D already affecting ATMs in the wild?
   Yes. It has been observed in Latin America.
4. What type of ATMs are affected?
   - Ploutus-D affects Diebold ATMs.
   - Minor modifications could be made to Ploutus-D to affect other vendors using the Kalignite Platform.
5. How is Ploutus-D installed on the ATM?
   Through physical access to the ATM.
6. How do attackers interact with Ploutus-D?
   Via an external keyboard that needs to be connected to the ATM.

IOCs

FileSystem:

[D-Z]:\Data\P.bin
C:\Diebold\EDC\edclocal.dat

The following files should be found at the same place where the service Diebold.exe is located:

Log.txt
Log2.txt
P.bin – Mac address of the system, plus string: “PLOUTUS-MADE-IN-LATIN-AMERICA-XD”
PDLL.bin – Encoded version of P.bin

Mutex names:

Ploutos
DIEBOLDPL
KaligniteAPP

Services:

Service Name: DIEBOLDP

Registry:

\\HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit=”Diebold.exe,%system32%/userinit.exe”