Ploutus ATM Malware

By Muhammed Camara, Abdullahi Omar & Nathaniel Baffour-Sulzle

Threat Description

- It is a family of malware first detected in 2013 by Symantec as Backdoor.Ploutus.
- In 2014, Symantec detected a new version called Backdoor.Ploutus.B.
- With this attack, hackers can connect their mobile phones to ATMs via USB tethering and executed commands in the form of specifically crafted SMS messages.
- Another version called, Ploutus-D, was detected in 2016. This attack's target was the ATM vendor, Diefold.

Technical Description

- What it does is that it allows attackers to withdraw cash from an ATM on command
- How it works is that it is installed once the ATM's CD-ROM is accessed and replaced by a new boot disk that delivers the malware.
- Next, an external keyboard is connected to the ATM in which the attacker presses, 'F8', in order to display a hidden trojan window.
- We should be concerned about this threat as other commands include, F1 (Generate ATM ID), F2 (Activate ATM ID), & F3 (Dispense Cash)

Summary of Impact

Discovered for the first time in Latin America back in 2013

Mexico: 64,864,864.00 USD; 73,258 ATMs have been found to be compromised

- Dynamite, fake fronts, ATM (in)security

In a report in 2016, a total of 492 attacks in Europe;

a rise of 80 percent compared to the same period in 2015 ($177.5 million)

WITHDRAW CASH FROM ATM USING A PHONE... HOW DO THEY DO IT?

Threat Procedure

The process of stealing money from ATMs using malware usually consists of four stages:

- The attacker gains local/remote access to the machine.
- Malicious code is installed in the ATM system.
- REBOOT of ATM
- JACKPOT!

Risk Mitigating After Effect

- Shut down the ATM
- Detach Usb port used to install malware
- Monitor unexpected openings of the head compartment of the ATM
- Investigate suspicious activities like non-consistent transactions or event patterns which are caused by an interrupted connection to the dispenser
- Keep your operating system, software stack and configuration up to date

Mitigating Risk For Future Threat

- Conduct a thorough threat assessment to identify any gaps in the ATM security program
- Use appropriate locking mechanisms to secure the head compartment of the ATM
- Use two factor authentications to implement access control for service technicians
- Operators should operate frequent visual inspections
- ATM Vendors should implement code-level protection to the ATM middleware

Sources

https://www.cyber.nj.gov/threat-profiles/atm-malware-variants/ploutus

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

https://securelist.com/atm-malware-from-latin-america-to-the-world/83836/