DIEBOLD NIXDORF

018-04/0005 –Potential Jackpotting US (Update on 017-34/0002)

20180126/BR/01 **January 25, 2018**

Summary

On the 26 of January we were informed by US authorities about potential Jackpotting attacks moving from Mexico to the United States within the next days (GIOC Reference #18-007-A)

The explanation provided with the warning describes the MO of the alert 017-34/0002 issued in October last year used against Front-load AFD based Opteva terminals. Therefore, the same countermeasures are applicable as for 017-34/0002 and should be deployed if not already implemented. As in Mexico last year, the attack mode involves a series of different steps to overcome security mechanisms and the authorization process for setting the communication with the dispenser. This communication authorization needs to be used when the mainboard or the hard disk has to be exchanged for legitimate reasons.

According to the authorities' description, MO will be targeting Front-load Opteva terminals with the Advanced Function Dispenser (AFD), but also other terminals and ATM vendors without physical authentication could be affected.

Description of attack (From Mexico cases)

In a Jackpotting attack, the criminal gains access to the internal infrastructure of the terminal in order to infect the ATM PC or by completely exchanging the hard disk (HDD). In recent evolutions of Jackpotting attacks portions of a third party multi-vendor application software stack to drive ATM components are included. In cases where the complete hard disk is being exchanged, encrypted communications between ATM PC and dispenser protects against the attack.

In this attack vector the top-hat of the terminal is opened in order to execute different activities based on the currently known information. The original hard disk of the terminal is removed and replaced by another hard disk, which has been prepared by the criminals before the attack and also contains an unauthorized and/or stolen image of ATM platform software.

In order to pair this new hard drive with the dispenser, the dispenser communication needs to be reset, which is only allowed when the safe door is open. As a preparation a cable is unplugged to manipulate the sensor state to allow the pairing functionality to become available. In order to initiate the dispenser communication additionally a dedicated button inside the safe needs to be pressed and held. With the help of an extension, which is inserted into existing gaps next to the presenter, the button is depressed. According to customer CCTV footage the criminals use an industrial endoscope to achieve this.

Terminals at risk

Potentially all Front-load AFD based Opteva models are affected by this MO. While there is also a risk for Rear-load AFD based Opteva terminals, due to the design and construction the Rear-load models would be extremely difficult to attack with this MO. Opteva models utilizing the ECRM module are not directly affected by the MO due to a different safe design.

The MO is independent of the protocol used for encrypted communications for an Opteva model, as the attack does not target and tamper the communication. It circumvents the physical security and the authorization to allow the dispenser to be paired to a different HDD and platform.

The MO currently is not effective on Diebold Series, ProCash series or CINEO series with recent firmware updates applied.

Recommendation for countermeasures

Diebold Nixdorf understands the impact of this threat and supports customers in identifying and deploying potential solutions. From a holistic security approach, Diebold Nixdorf recommends implementing the following countermeasures:

1) Limit Physical Access to the ATM

- Use appropriate locking mechanisms to secure the head compartment of the ATM.
- Control access to areas used by personnel to service the ATM.
- Implement access control for service technicians based on two-factor authentication.

2) Implement protection mechanisms for cash modules

- Use firmware with latest security functionality
- Use the most secure configuration of encrypted communications incl. physical authentication:
  - Agilis® XFS for Opteva®, Advanced Function Dispenser (AFD) Version 4.1.41 incl.AFD Application Firmware Version - 6.0.1.0 (or later)
  - Agilis® XFS for Opteva®, Core Version 4.1.59 (or later)
  - Optional – OSD+/DSST 3.3.30 (or later)

3) Set up additional measurements

- Monitor unexpected opening of the top hat compartment of the ATM.
- Ensure proper hardening and real-time monitoring of security relevant hardware and software events. This should include encryption of the harddisk(s)
- Investigate suspicious activities like deviating or non-consistent transaction or event patterns, which are caused by an interrupted connection to the dispenser.
- Keep your operating system, software stack and your configuration up to date.

For further information, please contact your local sales representative or your Diebold Nixdorf Professional Services.

Additional Information & Contact:

Diebold Nixdorf | Corporate Security & Fraud Management security@dieboldnixdorf.com