GLOBAL SECURITY ALERT

DIEBOLD NIXDORF

017-34/0002 – Jackpotting in Mexico - Pairing of rogue hard disk

20171013/AG/01 **October 13, 2017**

Summary

Recently Diebold Nixdorf has become aware of a new type of Jackpotting attack involving different hardware and software activities against Opteva Terminals in Mexico.

In this attack mode, a series of logical and physical steps are performed to overcome layered security mechanisms. During the recent incident criminals used a variant of Ploutus.D malware on a prepared hard disk combined with manipulation of sensors in the dispenser to enforce pairing of the devices.

At this time front-load Opteva terminals including Advanced Function Dispenser ("AFD") have been targeted. The respective patch provided by Diebold Nixdorf however is available for all AFD based ATMs.

Description of attack

In general, Jackpotting attacks are typically performed by either using Malware infecting the original ATM image or by connecting a Black Box directly to the dispenser to circumvent the ATM PC. This new incident does not utilize either of these MOs in their traditional way and also involves usage of an additional physical device.

In the recent attack, the top hat of the ATM was opened to replace the original hard disk with a maliciously manipulated disk. The rogue hard disk contained parts of a third party ATM platform software combined with a variant of the Ploutus malware. The criminals then used an industrial endoscope, which was inserted into the safe using existing openings to manipulate sensors required for physical authentication. This then enabled the malicious software to communicate with ATM hardware.

After the preparation, the criminal restarted the ATM with the maliciously modified software stack to illegitimately dispense cash.

GLOBAL SECURITY ALERT

Recommendation for countermeasures

Diebold Nixdorf understands the impact of this threat and supports customers in identifying and deploying potential solutions.

Diebold Nixdorf released an update to the Advanced Function Dispenser (AFD), which enhanced the physical authorization needed in order to establish secure communication.

From a holistic security approach, Diebold Nixdorf recommends implementing the following countermeasures:

1) Implement protection mechanisms for cash modules

- Use software stack with latest security functionality
  For this particular incident use versions greater or equal to 4.1.39 (XFS 4) or 6.0.20 (XFS 6)
  Deploy update package “as is”, customization of the respective package should be avoided.
- Use the most secure configuration for encrypted communication applicable

2) 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.
- Operator should conduct frequent visual inspections of the terminal

3) Set up additional measurements

- Monitor unexpected opening of the top hat compartment of the ATM.
- Ensure real-time monitoring of security relevant hardware and software events.
- 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 configuration up to date.

For further information, please contact your local sales department, a hardware integration representative or your Diebold Nixdorf security experts.

Additional Information & Contact:

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