DIEBOLD NIXDORF PERSPECTIVE

Defending against logical attacks on ATMs

By Joerg Reuter, Business Development Lead, Security

Joerg Reuter
Diebold Nixdorf

Are you doing enough to protect your ATMs against logical attacks? Two jackpotting attacks this past summer in Taiwan and Thailand illuminate the emerging threats facing ATM networks. The fraudsters used malware and creative hacking techniques to force terminals to dispense large amounts of cash (the equivalent of $2 million in the Taiwan heist alone). Most likely the culprits are not the same, which makes one particular similarity between the two incidents even more striking and a harbinger of things to come: in both cases, the software distribution mechanism of the victimised banks was exploited to introduce malware to the ATMs. Unlike typical jackpotting fraud, in which criminals gain physical access to each individual ATM to install malware, here we saw remote distribution of malicious software.

If we ignore for a moment the quality of the existing endpoint security on the attacked ATMs, the very fact that the attack came from the network itself poses new challenges in setting up defensive measures:

- How can an ATM distinguish whether it is talking to a legitimate back-end system or a spoofed one, like in the incident in Thailand?
- How can an ATM determine whether a software package it receives is legitimate or the result of a server hack, like in the Taiwan case?
- How can an attempted or successful breach be detected in a timely fashion?

The very fact that the Asian attacks came from the network itself poses new challenges in setting up defensive measures

The answer begins with acknowledging that the hardware, software and processes on and around the ATM are quite different from that of an office PC, and this should be reflected in the security measures being implemented.

At a basic level, banks must ensure that must-have standard security features such as full-disk encryption and hardening of the operating system are in place. They must be sure software protection is up-to-date and locked down – that is, that the proper whitelisting or sandboxing controls have been implemented.

Diebold Nixdorf's Terminal Security Suite enables all these measures in multi-vendor environments, which is critical to ensuring consistent security across a network. Combined, these precautions will typically cover more than 99% of the day-to-day operation, such as customer transactions, replenishment of cash and consumables, and routine maintenance.

It can be challenging, however, to secure the less common or unplanned tasks: a field engineer fixing hardware or software issues may require temporarily lowered security settings, but in a controlled and verifiable manner. Software updates have to be regarded as a potential attack vector; therefore software packages must be authenticated before installation. ATM access rights are a crucial third layer of defence: a separation of power can ensure that critical tasks, such as creating software packages, can only be performed by designated staff.

We combine the security features of our Terminal Security Suite with advanced monitoring and management tools that enable our clients to implement this holistic approach to security. When selecting a security partner, consider these factors:

- Are they experienced in the unique challenges of self-service terminal security?
- Do they offer cryptographic signatures to authenticate software updates?
- Are their solutions refined enough to, for example, open up the security settings on an ATM's PC for a restricted amount of time, without handing out passwords?
- Security-related events, such as unplanned reboots or attempts to connect unregistered devices, should be logged in real-time at the server so an alert can be triggered quickly.

Is your organisation prepared for the increasingly sophisticated fraud facing the banking industry? Get in touch with your Diebold Nixdorf contact or go to DieboldNixdorf.com/Security to learn more about how you can raise the bar on ATM security and stop attacks before they happen. ■

DIEBOLD NIXDORF