# NCR SECURITY UPDATE

**DATE:** August 29, 2016 **INCIDENT NO:** 2016-12 **REV:** #99

## Malware attacks in Thailand

### Summary

NCR is actively responding and investigating an attack on NCR ATMs associated with a single financial customer in Thailand.

Attackers are using network access points to connect to the bank's internal network and connect to ATMs locally.

This is a network attack. The attackers have breached the Financial Institutions internal network. Once inside the network, the attackers are spoofing the software distribution server as the means to deliver the malware to ATMs (Please note: In this case, the attack is performed on SDMS Version 2.3.0 from InfoMindz and at this time, we have no information regarding other versions of this software).

Network attacks are not new and are not unique to NCR ATM's, however this attack represents a newer variation of the network attack vector. Analysis of the malware indicates that it also targets other ATM vendors.

Current hashes of identified malware are:

Variant 1

| | |
|---|---|
| MD5: | b428c8af87e85522dc847f054f4d1e5f |
| SHA1: | 7dc0efabf70133fb8d30b4de75811c9d771d01da |
| SHA256: | 3d8c7fb9e55f96cf3073b321ee5e59ff2189d70b0662bc0b88990971bc8b73d8 |

Variant 2

| | |
|---|---|
| MD5: | 15632224b7e5ca0ccb0a042daf2adc13 |
| SHA1: | c9381c5d6f39c54aad5b57c3b1deecab6887af57 |
| SHA256: | cc85e8ca86c787a1c031e67242e23f4ef503840739f9cdc7e18a48e4a6773b38 |

Variant 3

| | |
|---|---|
| MD5: | c092bf1244c88b6e7e112e3614db79dc |
| SHA1: | bc32ac2ce56f12baae935b684b2022e4366a9117 |
| SHA256: | 22db6a994eb057715b499c5641cc608fb0380aeea25f78180436c35ecd81ce7d |

NCR continues to investigate this attack.

## Guidance and Recommendations:

These recommendations are targeted to any customers using the SDMS Software Distribution tool from InfoMindz (versions earlier than 2.3.3). Other versions of InfoMindz SDMS may also be at risk of compromise but we have had no reported attacks on versions other than 2.3.0.

To detect and remove known versions of this malware on your ATM estate:

- Deploy new Stinger to detect malware and delete. Perform the scan regularly. NCR may provide a new Stinger if further malware variants are identified. Stinger does not prevent reinfection.

A straight-forward security control that will reduce your attack surface and can be quickly deployed is to update your firewall:

- Modify the ATM firewall to block incoming SDMS port connections from non-SDMS server IP Addresses.

This will not wholly prevent this attack. However, it will disrupt the attacker.

Additionally, each of the following security controls would independently have minimized the chances of this attack being successful. You should assess which security control is the easiest/quickest for you to deploy. However, our recommendation would be to apply ALL of them in addition to those described within NCR Logical Attacks Configuration and Implementation Guidelines Document.

- Explicitly authorise the time window when software updates to your ATMs are permitted. For example:
    - Deploy Solidcore Suite for APTRA to only and configure it to:
        - Remove SDAgent from authorised updaters.
            - This will still allow screen downloads and EJ Uploads.
            - You can explicitly add SDAgent as an updater when you intend to perform any software updates. After the installation, SDAgent can then be removed as an Authorised Updater.
        - Block changes to SDAgent configuration file
        - Configure ePO to alert
            - When software updates occur
            - When McAfee agent is not contactable

        - Block malware based on its hash & name

- Prevent changes to the software distribution agent on the ATM and disallow binary updates onto the ATM via software distribution:

    - Deploy Solidcore for APTRA and configure it to:

        - Block changes to SDAgent configuration file
        - Do not make SDAgent an authorised updater. This will still allow screen downloads and EJ Uploads.
        - Block by malware hash & malware name locally

- Deploy a software distribution tool that provides Confidentiality, Integrity and Availability.

- Deploy a software VPN on the ATM to protect traffic between the ATM and the banks network.

We additionally recommend:

- Detect if ATM is offline or not contactable for a prolonged period.

- Consult a security enterprise specialist to deploy industry best-practice security controls within your enterprise. For example:

    - Network Access Control (for example, Kerberos).

    - Deploy Network Intrusion Detection/Protection system. Create a custom rule to detect and respond to unusual traffic behaviour. Specifically, alert and block ATM to ATM traffic.

    - Deploy Active Directory to allow only authorised devices (ATM) and applications to connect to the domain and only authorized devices can access specific services.

- Physically protect the GPRS routers.

This attack in its current form would be prevented by removing the SDAgent from the ATM. However, this may impact your ability to download software onto your ATM estate.

It is also critical to follow all guidelines summarized in the [NCR Logical Attacks Configuration and Implementation Guidelines Document] as this will protect against this malware being installed through another mechanism (e.g. through an offline or online malware attack).

# NCR SECURITY UPDATE

**Contacts**

ATM Crime Reporting : global.security@ncr.com<br>
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com<br>
Further information on this alert: owen.wild@ncr.com