NCR ATM SECURITY UPDATE

DATE: November 2019 **INCIDENT NO:** 2019-07 **REV:** #1

An Update on ATM Jackpotting Attacks

Summary

NCR is aware of inaccurate media reporting of a new malware variant impacting ATMs. The FireEye group, Mandiant, has identified this malware as “Boostwrite.” The reporting that it is infecting NCR ATM software is incorrect, and not what Mandiant reported.

The "RDFSNIFFER" malware is not compatible with ATM devices or the ATM Software Stack. Additionally, the "BOOSTWRITE" malware infection described by Mandiant that would be required to load the "RDFSNIFFER" malware into memory uses a well-known Windows attack vector called "DLL Search order hijacking.", which is blocked by NCRs Solidcore Suite Whitelisting Solution. This software prevents the loading of modified executables and DLLs and locking down ATMs as per the NCR Logical Protection best practices whitepaper.

Malware attacks on ATMs remain an issue for all ATMs from all manufacturers. From our review of recent attacks and reports NCR has seen a possible change in trend in logical attacks. Ee are seeing more incidents where criminals are aiming the point of attack at the network, rather than at the individual ATM. These network attacks can access customer data, as well as provide a way for malware to be delivered to the ATM.

It is a result of this complex attack landscape that NCR continued to remind ATM operators that they must mitigate against logical attacks by fully aligning to the NCR best practices found in the attached whitepaper.

Contacts

ATM Crime Reporting: Global.Security@ncr.com

Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com

Please contact your NCR Account Manager if you have any questions or need additional information.