NCR ATM SECURITY UPDATE

DATE: June 28, 2017 **INCIDENT NO:** 2017-06 **REV:** #1

Petya Ransomware

Summary

There is yet another serious malware cyber threat called “Petya” that is impacting many organizations worldwide. This type of threat is known as ransomware. It will encrypt the files on your end-points running Microsoft operating system software, rendering them inaccessible. ATMs are at risk of this attack. Additionally, this malware attempts to infect other end-points on the same network. NCR has taken a number of steps to respond to this threat.

Who is at risk

Customers running any Windows OS who have not applied the Microsoft security patch MS17-010. For Windows 7 customers, NCR advised in March 2017 that this patch be deployed.

Security updates for the range of Windows OS are available at:

http://www.catalog.update.microsoft.com/search.aspx?q=4012598

Guidance and Recommendations for ATM endpoint security:

As preventative measures to protect our customers, we have worked with our security partner McAfee and Microsoft to understand the malware and identify mitigations.

McAfee have informed us that when Solidcore for APTRA or Solidcore Suite for APTRA is enabled it will block any hash values that are not whitelisted. This will prevent this attack from being successful.

NCR ATM SECURITY UPDATE

Additionally, NCR recommends that customers should install MS17-010 immediately, after testing in their lab.

Customers using an alternative anti-malware solution should contact their anti-malware vendor for guidance and also deploy the Microsoft security patch after testing in their lab.

Customers who are not using any anti-malware solution must install the Microsoft patch immediately. The patch should be tested in a lab environment prior to deploying to a live ATM.

Deploying the Microsoft Security Patch

All Windows XP SP3 and Windows 7 SP1 ATMs should install the patch for MS17-010 as soon as possible.

APTRA Vision's inventory capabilities can be used to determine whether or not this this patch has been successfully deployed.

Windows 7 SP1 ATMs

> Patch can be obtained from the link below as part of March 2017 Security convenience roll up
>
> http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212

Windows XP SP3 ATMs

> Microsoft have made the patch for the vulnerability causing the WannaCry ransomware infections available on Windows XP. The XP SP3 patch is available at:
>
> http://www.catalog.update.microsoft.com/search.aspx?q=4012598

The MS Security patch for other Windows OS are available at:
http://www.catalog.update.microsoft.com/search.aspx?q=4012598

NCR ATM SECURITY UPDATE

Guidance if end-point is infected

McAfee has released a new .dat file to include coverage for this variant.

Protecting against modified Petya ransomware variant (June 2017)

https://kc.mcafee.com/corporate/index?page=content&id=KB89540

If you are concerned about infection across your enterprise, then run Stinger to detect and delete this malware on end-points that have not yet been fully compromised.

McAfee Stinger is available at: https://www.mcafee.com/uk/downloads/free-tools/stinger.aspx
Ensure you read the Stinger documentation prior to using this utility. This documents the range of OS supported by the utility.

If any ATMs are infected/locked with the ransomware, then every other ATM and end-point on the same network must be checked for infection as well. Once the malware infects one end-point on the network it will replicate itself to other vulnerable systems.

The only way to recover an infected and encrypted ATM is to reimage from scratch. There is NO other option. Ensure that the patch is installed as part of the reinstall.

With regards to malware attacks, NCR's security strategy is designed to provide guidelines and solutions that will prevent all malware from being loaded onto the ATM.

NCR Monthly Microsoft Security Updates Email

For customers on annual software maintenance, NCR can provide monthly notification of the Microsoft security convenience roll-ups. To subscribe to the list please contact your account team.

NCR ATM SECURITY UPDATE

NCR Generic Logical Attack Guidelines

The guidelines are set out in the **NCR Logical Attacks Configuration and Implementation Guidelines Document.**

NCR provides several solutions customers can deploy to prevent the loading of malware on the ATM:

- NCR Secure Hard Disc Encryption
- Solidcore Suite for APTRA
- NCR Secure Remote BIOS Update
- Security for APTRA

All of these solutions are required to provide a layered and comprehensive approach to preventing malware and other logical attacks. The failure to follow all of the guidelines and implement all of these solutions results in the customer's ATMs remaining vulnerable to ATM attacks.

NCR ATM SECURITY UPDATE

Malware Hashes

File	SHA1	SHA256
main 32-bit DLL	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
main 32-bit DLL	9717cfdc2d023812dbc84a941674eb23a2a8ef06	64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
64-bit EXE	38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf	02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f
32-bit EXE	56c03d8e43f50568741704aee482704a4f5005ad	eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998
signed sysinternals "PSEXEC.EXE" (Not strictly malware, but is used for malware remote control and customers may wish to blacklist it)	cd23b7c9e0edef184930bc8e0ca2264f0608bcb3	f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5

Contacts

ATM Crime Reporting : global.security@ncr.com
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com
Media Inquiries or Questions: aaron.gould@ncr.com
Further information on this alert: owen.wild@ncr.com