

NCR SECURITY UPDATE

DATE: May 15, 2017

INCIDENT NO: 2017-05

REV: #1

Update on Global Ransomware attacks - WannaCry

Summary

There is a serious malware cyber threat called "WannaCry" 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.

There have been unconfirmed media reports that non-NCR ATMs in India have experienced this attack.

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 SECURITY UPDATE

Additionally, customers should install MS17-010 at their next monthly patch deployment, after testing in their lab, as per PCI guidance.

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 patch has been successfully deployed.

Windows 7 SP1 ATMs

The 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 SECURITY UPDATE

Guidance if end-point is infected

McAfee have updated their Stinger to detect this malware. 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 Generic Logical Attack Guidelines

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

NCR SECURITY UPDATE

NCR provides several solutions that 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 attacks.

For NCR Digital Banking (Digital Insight Customers)

A specific update will be sent to all current Digital Insight Customers

NCR Internal IT Activities

NCR Global Security teams are taking a number of steps to mitigate the risk of this attack to our internal systems. To date, we have not seen any cases of infection within our infrastructure or employee PCs. These are detailed later in the document.

As preventative measures to protect NCR's enterprise, we have:

1. Suspended any remaining access from outside the company using mechanisms (ports) associated with this attack.
2. Completed deployment of the Microsoft patch (MS17-010) to all internet-facing servers in our corporate datacenters.
3. Added security measures for attachments within our email security system.
4. All NCR workstations received the required Microsoft patch at the time of corporate network connection.

NCR SECURITY UPDATE

5. Forced updates to anti-virus software detection to all workstations with the newest variant signatures
6. Added new capabilities to our security monitoring platform to specifically identify this threat in our systems.
7. Provided more technical communication to specific high risk internal parties.

General Guidance to prevent phishing attacks:

- Be suspicious of emails from sources you do not know or recognize.
- Do not click on links or open attachments from unknown senders.
- Be suspicious if the message promises something "too good to be true."
- Be wary of any email requesting personal or financial information.
- Read the message content carefully and look for misspelled words and poor grammar. This is typically a sign of a phishing email.
- Beware if the message uses time-based constraints (i.e. "click the link within 24 hours or else").
- NEVER enter your password or personal data into a site or window you've arrived at by following a link in an email. Even if it's a site you trust like your bank, it's better to go directly to the site by using your bookmark or typing the site's address directly into your browser.

Relevant Articles

<https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/>

<https://support.microsoft.com/en-us/help/4012598/title>

<https://kc.mcafee.com/corporate/index?page=content&id=KB89335&elqTrackId=080d6d6426f34a2fb9b7fae0ca16d59a&elq=f9bb7df0610043a5b3d40ad436e945f8&elqaid=7257&elqat=1&elqCampaignId=4054>

<https://securingtomorrow.mcafee.com/business/analysis-wannacry-ransomware-outbreak/>

ftp://custftp2.nai.com/outgoing/msteg/ransom-wcry-stingers/STIN_W329001.zip

ftp://custftp2.nai.com/outgoing/msteg/ransom-wcry-stingers/STIN_W649001.zip

NCR SECURITY UPDATE

Malware Hashes

The following table lists the identified SHA-1 & SHA-256 hashes for the WannaCry malware.

SHA256	SHA1
dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696	fb18818fc383330b401fc5b332cc63a5bbd4cd30
201f42080e1c989774d05d5b127a8cd4b4781f1956b78df7c01112436c89b2c9	1bc604573ceab106e5a0e9c419ade38739228707
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9	8897c658c0373be54eeac23bbd4264687a141ae1
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa	87420a2791d18dad3f18be436045280a4cc16fc4
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
aae9536875784fe6e55357900519f97fee0a56d6780860779a36f06765243d56	Unavailable at Present
21ed253b796f63b9e95b4e426a82303dfac5bf8062bfe66995bde2208b360fd	Unavailable at Present
2372862afaa8e8720bc46f93cb27a9b12646a7cbc952cc732b8f5df7aebb2450	Unavailable at Present
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c	e889544aff85ffaf8b0d0da705105dee7c97fe26
f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235cbe782d85	51e4307093f8ca8854359c0ac882ddca427a813c
4a468603fcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79	47a9ad4125b6bd7c55e4e7da251e23f089407b8f
4b76e54de0243274f97430b26624c44694fbde3289ed81a160e0754ab9f56f32	f3839c1cde9ce18021194573fdf0cae09a62172f
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13	6352214c178b19a8ee321908b1c0c698214dad8b
78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df	276d2ec82c518d887a8a3608e51c56fa28716ded
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844	120ed9279d85cbfa56e5b7779ffa7162074f7a29
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9	02408bb6dc1f3605a7d3f9bad687a858ec147896
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf	4fdae49be25846ca53b5936a731ce79c673a8e1f
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a	64b8e679727e99a369a2be3ed800f7b969d43aa8
eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb	d8a2c1be4b47944d9afdf5e664e5db1364b66a5a
043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2	bc978db3d2dc20b1a305d294a504bb0ceb83f95a

NCR SECURITY UPDATE

57c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4	565e67fec07cfc67adc31f66747675343e82ebef
ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8	a52e025d579bebae7c64cb40236b469b3c376024
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494	432c1a5353bab4dba67ea620ea6c1a3095c5d4fa
3e6de9e2baac930949647c399818e7a2caea2626df6a468407854aaa515eed9	828001f20df60b6af286593c37644d39e5a6122a
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640	14249e7fb3fb6f4b363c47d5aae9f46dab2083c1
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec	af7db69cbaa6ab3e4730af8763ae4bf7b7c0c9b2
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c	e889544aff85ffaf8b0d0da705105dee7c97fe26
12d67c587e114d8dde56324741a8f04fb50cc3160653769b8015bc5aec64d20b	92a0631e364b355e9e8f3675ede0b2b19040c248
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186	18ba455efe2476730346c69cc7e7d6acfa5f074d
3f3a9dde96ec4107f67b0559b4e95f5f1bca1ec6cb204bfe5fea0230845e8301	3a0cbb76019cfbe520d9d493ac078e70465904cd

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