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:


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.
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 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


**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:


The MS Security patch for other Windows OS are available at:

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](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**

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.
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
Malware Hashes

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

<table>
<thead>
<tr>
<th>SHA256</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>dff26a9a44baa3e109b8df41a0e301d9e4a28aad7bd77212bb7ccd137bdf696</td>
<td>fb18818f3c83330b401fc5b332cc63a5bbd4cd30</td>
</tr>
<tr>
<td>201f42080e1c989774d05db5b127a8cd4b3748f1956b78df7c01112436c89b2c9</td>
<td>1bc604573ceab106ea5a9e9c419ade387399228707</td>
</tr>
<tr>
<td>ed01e6bfb9eb5b7ea54af4d01bf5f10176618404804396e56ab8e608e041a</td>
<td>5ff465afaabcfbf0150d1a3ab2c2e74f3a4426467</td>
</tr>
<tr>
<td>c365d6aa345cfca6f629505572a484cf52f21933d684ea52130bb8bb7bada9f</td>
<td>8897c658c0373be54eeae23b2db4264678a141ae1</td>
</tr>
<tr>
<td>09a46b3e1be080745a6d88d8d6b5bd351b1c7586a0ed94d2c3836421cafa</td>
<td>87420a2791d18add3f18be436045280a4cc16fc4</td>
</tr>
<tr>
<td>b9c5d43398909e0a9d90a0d4d3d26fd44a2819a54a6bf8466b956d681391c25</td>
<td>45356a9dd616ed7161a3b9192e2f318d0ab5ad10</td>
</tr>
<tr>
<td>aae956875784fe6e5357900519f7e0e56d6780860779a36f06765243d56</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>21ed253b79f63eb9e5b4ae426a8230dfacfb5f8062bfe669995bde2208b306fd0</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>2372862aaf8e8720bc46f93cb37a9b12646a7c952cc732b8f5df7aebb2450</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>24d00d4a104d5d403db4bcbfca2a4b1911f39008a575aa614ea04703480b1022c</td>
<td>e889544aff5af8f8b0dd0da7a05105dee7c97fe26</td>
</tr>
<tr>
<td>f8812fe1deb8001f3b76726b8f8640eceb123bc234b63728e6235cbe782d85</td>
<td>51e430709f8a85435900ac882ddca427a813c</td>
</tr>
<tr>
<td>4a468603f0cb7a2eb5770705898c9ef37aade532a7964642ec705a7494b79</td>
<td>47a9ad4125b6bd7c55e4e7da251e23f089047b8f</td>
</tr>
<tr>
<td>4b76e54de023427f497430b26624c44694f4bede3289ed81a1600e754ab9f5f32</td>
<td>f8393c1cde9ce18021194573ff0fcae90a62172f</td>
</tr>
<tr>
<td>9cc32c94ac7ed6e48f86704725b6cd0fda0d2cd7a7d769e4d0db1776903e5a13</td>
<td>6352214c178b19aee321908b10ce698214dad8b</td>
</tr>
<tr>
<td>78e3f87f31683550cf398317b2db87d803bd78e53655ca7c80f0561ec8606df</td>
<td>276d2ec8c2518d887a8a3608e51c56fa28716ded</td>
</tr>
<tr>
<td>be22645c61949ad6a0f773737a7d6cd85e3faee44315632f161adc4c9d5a8e6844</td>
<td>120ed9279d85cbf65e65b7779fa71620747a29</td>
</tr>
<tr>
<td>5d26835be2c4f8b2eef0f301c06050350a09ec3afacc71df22813595c0b9</td>
<td>02408bb6dc1f3605a7d3f9bad687a858ec147896</td>
</tr>
<tr>
<td>76a3666ce9119295104bb69ee7af3f2b85f234f084b63ace79877f9b06312bdf</td>
<td>4fdaee49be25846ca53b5936a731ce79c673a8ef1f</td>
</tr>
<tr>
<td>fc626fe1e0f4d77b3b4851a8c60ccdd11172472da3b9325b6288ac8342f6c710a</td>
<td>64b8e679727e99a369a2e3ed800f7b969d43aa8</td>
</tr>
<tr>
<td>eebc9dc6a1c4b3949b2f3f134a77d76736b359779f519bc97c11438b5caeb1c1fb</td>
<td>d8a2c1be4b47944d9afdf5e664e5db1364666a5a</td>
</tr>
<tr>
<td>043e0dd8b8cda5e6851f8b5853f244677b1df5f869075e7f7ba111077170c2</td>
<td>bc978db32dc20b1a305d294a504bb0ceb839f5a</td>
</tr>
</tbody>
</table>

© 2017 NCR Corporation. All rights reserved.
NCR SECURITY UPDATE

57c12d85732df3883a8a08ba1a9e3ee02a21c61ded6b675b6c01d6e2213c7777f4 565e67fec07cf67adc31f66747675343e82ebe

c29de1dc881786893e54b09f557fe1e4e40083c0955294d55b91f52ba469c8 a52e025d579b6bae7c64cb40236b469b3c76024
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5b6d3494 4321a5353bab4d6ba67ea620ea6c1a5095c5df4a
3e6de9e2baaf930949647c399818e7a2caea2626df6a468407854aaa515eed9 828001f20df60b6aa2a2bf28659fc3764439e6a122a
9b60ce62256dc455ca64df935b71c26c68f4886d6f8a811944db4e23db93356a0 14249e7fb3fb6f4b3c3c47d5aee9f46da2083c1
4ad4ef9d0c01d26c6f3277c3ce0b4d4951d4b94aa19aa097341aff2aacaec af7df69cbac6a6b3e4730af8763ae4bf7b7c09b2

24d004a104d5403db6bdf2a4b19a11f39008a575aa614eaa04703480b1022c e889544aff85fa88b0d0da705105dee7c97fe26
12d67c5b8e114d8de6324741a8f04b50cc3160653769b8015bc5aad64d20b 92a0631e364b3555e9ef3675ede0b2b19040c248
85ce324b8f78021ecfc9b811ec478f19b82616b0933f6f2eaeb457f19e186 18ba455e4e2476730346c69cc7e7d6acfa5f074d
3f3ae9dfe496e4107f67b0559b4e95f5f1bca1ec6cb204b6e5f6e0a230845e8001 3a0cbb76019cbfe520d9d493ac078e70465904cd

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

© 2017 NCR Corporation. All rights reserved.