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 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**

The guidelines are set out in the NCR Logical Attacks Configuration and Implementation Guidelines Document.
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
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>dff26a9a44ba33ce109b8df41ae0a301d9e4a28a7bd7721bab7cc137bfdf6e6</td>
<td>fb18818f3c83330b401fcb53b322cc63a5bbd4cd30</td>
</tr>
<tr>
<td>201f42080e1c98774d055d5b127a8cd4b478f1f956b78df7c01112436c89b2c9</td>
<td>1bc604573ceab106e5a0e9c419ade38739228707</td>
</tr>
<tr>
<td>ed01ebfbc95eb5bea545af4d01bf5f1071661840480439cf65bab8ee0800e81a</td>
<td>5ff465aafabcbe0f150d1a3ab2ce74f3a4426467</td>
</tr>
<tr>
<td>c365ddaa345cfa3f3d629505572a484cf5f2219336d84ea52130bb7badfa9</td>
<td>8897c658c0373e54eeac23bbed4264687a141ae1</td>
</tr>
<tr>
<td>09a46b3e1beb080745a60d88d85bd531b1c7586aed094d0c238ee36421cafa</td>
<td>87420a2791d18dad3f18be436045280a4cc16fc4</td>
</tr>
<tr>
<td>b9c5d43398090e0ad9a00d4d33d26df44a32819a45aba8f846bb956081391c25</td>
<td>45356a9dd616ed7161a3b9192e2f318d0ab5ad10</td>
</tr>
<tr>
<td>aae95368757846e5357900519f7ee056d6780860779a36f06765243d56</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>21ed253b796f63b9e95b4e426a82303dface5bf8062b6fe69996bcb2208b60fd0f</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>2372862a8a8e782b0c46f93cb27a9b12646a7dbc952cc732b8f5df7aeabb2450</td>
<td>Unavailable at Present</td>
</tr>
<tr>
<td>2ad004a104d54503dcbf7ca2a4b19a11f39008a575aa6146aa04307490b1022c</td>
<td>e88954af8f5ffaf8b0dd07a705105ddd7c97fe26</td>
</tr>
<tr>
<td>f8812f1deb8001fb767266c85640eeb123bc3204b536728e6235ccbee782d85</td>
<td>51e430709f8ca8854359c0ac882ddca427a813c</td>
</tr>
<tr>
<td>4a468603f92cb7a2eb577070898c9f8f37ade5332a796462ecc070a477494b79</td>
<td>47a9ad4125b6bd7c55e4ed7a251e23f089047bf</td>
</tr>
<tr>
<td>4b76e54ade204327f497430b26624c4469f4bde3289ed81a160e0754ab95f632</td>
<td>f83839c1cdce9e18021194573df0cae9a62172f</td>
</tr>
<tr>
<td>9cc32c943a7dc6e48f86704725b6cd0fda2dcd07a7d769e4ddeb1776903e5a13</td>
<td>63522141c178b19a8ee32190b810c6e698214ad8bb</td>
</tr>
<tr>
<td>78e3f87f3168335c0f539317b2d87d303bd87ee3656c5a7c80f0561ee8606df</td>
<td>2762de2ec82e512d887a8a3608e51c56afa28716ded</td>
</tr>
<tr>
<td>be22645c61949a6da077373a7d6cd85e3fae43415632f161ad4c9d5a8e8d44</td>
<td>120ed9297d85c6fa56e5b7779ff7a716207f7a29</td>
</tr>
<tr>
<td>5d268355bec2f4f8f2b3efff301c06d05035da09e33aafacc71dfff2185395c0b</td>
<td>02408bb6dc1f3605a7d3f9bad687a2586ec147896</td>
</tr>
<tr>
<td>76a3666ec9119295104db69e7aaf3f2845d234f0b48a7e987f79806312bbdf</td>
<td>4fdaee49be25846ca535b5936a731ce79c673a8e1f</td>
</tr>
<tr>
<td>fc626fe1e04df77b34851a860c0d11172472da3b9325bfe288ac83d4267c10a</td>
<td>64b8e679727e99a369a2be3ed800f7b969d43a8</td>
</tr>
<tr>
<td>eebbcd6a1c4b3949b2ff3134a77d7637635979f7519bc97c11483b5caeb1c1fb</td>
<td>d8a2c1be4b479449afdf5e66e4ec5bd1364666a5a</td>
</tr>
<tr>
<td>043e0dd8b8cda5685f5b853f244f77bd1fd50f869075ef7fa111077f70c2</td>
<td>bc978db3d2dc20b1a305d294a504b0ceb8395a</td>
</tr>
</tbody>
</table>
Contact Information:

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.