“PETYA” RANSOMWARE CYBER-THREAT

<table>
<thead>
<tr>
<th>ID and revision</th>
<th>OE06282017-1</th>
<th>Aggregate Severity: Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product(s) addressed</td>
<td>OpenEnterprise</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>28 June 2017</td>
<td></td>
</tr>
</tbody>
</table>

Overview

On the 27th of June 2017, we became aware of the “Petya ransomware/malware” (also called NotPetya) cyber-attack spreading throughout the world, causing computers to be encrypted and victims to see a request for ransom on their computer screens.

This ransomware is still under investigation; however, it appears to be similar to the “WannyCry ransomware.” The Petya malware exploits a Microsoft® Windows® vulnerability in the SMB (Server Message Block) protocol as well as other unconfirmed exploits (including credential harvesting and remote execution utilities), which allows it to spread within networks. The ransomware also appears to overwrite the Master Boot Record (MBR). Multiple global organizations have reported network outages, including government and critical infrastructure operators.

Ransomware attacks are becoming much more common, but they are now seen paired with exploits that spread as a network worm. The recent WannaCry attacks in May 2017 highlighted that many Windows O/S systems were not (maybe still are not) patched for the SMB vulnerability. Further to this, the fact that Petya ransomware spread using this same vulnerability shows that many systems may still be vulnerable, despite the recent attention from the WannaCry infection.

The vulnerability that was being exploited by the WannCry ransomware was patched by Microsoft in their March 2017 patch release (MS17-010). Emerson provides monthly details about the approved patches to be used on OpenEnterprise systems as part of the OpenEnterprise Gold Level Support package.

Affected Products

Affects all unpatched versions of Microsoft Operating Systems
Infection Factors

Customers should not have email clients on any PC’s or servers that are part of the SCADA or Control System Network, or that are connected to it at any time. Another method of infection is leveraging network shares and weaknesses in the Microsoft SMB implementation. SCADA and Control System Networks should always be isolated from external networks (including corporate and business networks) using firewalls or similar technology that block all communications protocols that support file sharing (including SMB, FTP, etc.) Any file or data transfer from SCADA or Control System Networks should be implemented using a ‘push’ technology to initiate transfer from within the secure area to a less secure area, rather than permitting clients external to these networks from requesting data. Customers that do not follow Emerson best practices for network segmentation may be at higher risk for infection.

Recommended Considerations

Emerson recommends that customers follow our best practices for network segmentation and email use on the distributed control systems:

- Be very aware of this latest malware attack currently underway.
- Ensure the application of Microsoft Security Updates in MS17-010.
  - Note: Microsoft released “WannaCry-related” updates in MS17-010 notification release. All the latest Emerson approved Microsoft Security Updates should be applied as they become available.
- Ensure the application of the latest signature files from Symantec (as installed).
- Never install or use email clients on any machine or device attached to the SCADA or Control Networks, or on any machine or device that will be attached to the networks at any time.
- Do not use the same username and passwords for both the control system / SCADA system and enterprise level accounts (which is a large risk in this latest attack).
- Use extreme caution opening any files on any machines within the SCADA network. This includes files received as email attachments, or copied from USB thumb drives or external hard drives.
- Control and SCADA Networks must always be isolated from Corporate LANs, the Internet and other less secure networks using current firewall technology. As a general rule, it shall not be possible for any external IP client to access any IP Server within the SCADA or Control Networks from outside of the SCADA or Control Networks.
• Ensure that firewalls are all operational and have the appropriate restrictive setting enabled.

• Create and maintain high integrity, comprehensive system back-ups, ensuring if an infection occurs, data may be restored.

Emerson recommends that customers keep systems patched and up-to-date with Microsoft Security Patches. A list of all approved Microsoft Security patches for OpenEnterprise can be found on SupportNet for all Gold Level Support contract customers.

**Actions and Next Steps**

The Windows patch testing for the month of May, including the patches included in the Microsoft Security Notification MS17-010, has been completed for both OpenEnterprise v2 and v3 for the operating versions listed below. Emerson recommends at a minimum to deploy the Microsoft security patch referenced in the Microsoft Security Notification MS17-010. Please follow all best practices for installing new software and patches.

OpenEnterprise v3
- Windows 2008 R2 (64bit)
- Windows 2012 R2 (64bit)
- Windows 7 (64bit)

OpenEnterprise v2
- Windows 2008 (32bit)
- Windows 2003 (32bit)
- Windows 7 (32bit)

The OpenEnterprise Microsoft Windows patch testing for the month of June is currently underway and the latest approved Microsoft patch list will be published on the Emerson SupportNet website by July 7, 2017. If any new or updated Microsoft patches are released to address the Petya Ransomware, these patches will be included in the normal Emerson OpenEnterprise scheduled Microsoft patch testing.

**Contact Information**

Services are delivered through our global services network. To contact your Emerson local service provider, click Contact Us. To contact the Global Service Center, click OpenEnterprise SupportNet.
Disclaimer

The urgency and severity ratings of this notification are not tailored to individual users; users may value notifications differently based upon their system or network configurations and circumstances. THIS NOTIFICATION, AND INFORMATION CONTAINED HEREIN, IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. THE USE OF THIS NOTIFICATION, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THIS NOTIFICATION, IS AT YOUR OWN RISK. EMERSON RESERVES THE RIGHT TO CHANGE OR UPDATE NOTIFICATIONS AT ANY TIME.

OpenEnterprise Security Notification

Notice: OpenEnterprise products are used in many unique applications and each user must determine the potential impact of this issue upon their respective systems and act accordingly.