Security Notification – Petya Ransomware Cyber-Threat

Affected Products:

Product Line	Category	Device	Version
DeltaV and AMS	Workstations and Servers	All unpatched devices or deployed systems that do not follow the recommendations included in the DeltaV Security Manual	All

Overview

On the 27th of June 2017, the "Petya" ransomware/malware cyber-attack spread throughout the world causing computers to be encrypted and victims may see a request for a ransom on their computer screens. This malware is a variant of the "Trojan.Cryptolocker.AJ" ransomware which encrypts the master boot records of the infected computers making them unusable. This cyber-threat has been compared to the "WannaCry" ransomware as they both seem to exploit the same Microsoft Windows vulnerabilities.

The information about the "Petya" ransomware is unfolding and Emerson continues to investigate and monitor the methods by which the malware can propagate. Emerson has released a DeltaV and AMS Security Notification with additional information about this cyber-threat, and it is referenced in the DeltaV Security Notices Catalog: Knowledge Base Article (KBA) NK-1500-0102, available on Emerson's Guardian Support web portal.

Initial analysis indicates that transmission to other machines is possible via harvested usernames and passwords on the infected machine; enabling propagation to a new target system, if a harvested username and password matches.

Recommended Considerations

If you do not follow overall best practices for network segmentation, you may be at higher risk for infection. Key points that need to be considered:

- install the latest Microsoft Security Patches on your Windows devices (workstations and servers)
- update your antivirus signature files on your devices with the latest signature files
- ensure that your Backup & Recovery service is active and verify your backups
- do not use the same credentials for both the control system and enterprise level accounts
- ensure that your firewalls are all operational and have the appropriate restrictive settings enabled
- restrict the use of portable media within your DeltaV system
- review the DeltaV Security Manual for additional ways to secure your DeltaV system

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 Technical Support.

Legal Disclaimer

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, is at your own risk. Emerson reserves the right to change or update notifications at any time.