
# Ransomware “WannaCry” Cyberattack Update

As you are likely aware, a large-scale malicious ransomware campaign is spreading and impacting organizations globally, including banks, airlines and the National Health Service in the United Kingdom. The ransomware encrypts data on the compromised system and demands a ransom be paid to restore operations. The impact of the ransomware includes temporary or permanent loss of sensitive/proprietary information, disruption to regular system and business operations, financial losses incurred to restore systems and data, and potential harm to an organization's reputation.

The ransomware commonly goes by the name ‘WannaCry’ and spreads easily when it encounters unpatched or outdated software. The ransomware exploits a publicly known vulnerability in all Windows operating systems that was identified by Microsoft, and a critical security update subsequently was released on March 14, 2017, to address the vulnerability. Most of the time, there is no way to reverse a ransomware infection. In many cases, the only resolution is to restore from recent backups. Prevention is key.

**ACTION REQUIRED:**

- Ensure backup system and processes are in place, and copies of the most recent backup are stored in an offline/disconnected state as to not be susceptible to infection.
- Immediately install Microsoft Security Update 4013389 on all servers and workstations to prevent infection of this malware.
    - If you encounter a problem with your Host ID, please refer to this Tridium knowledge article
- Ensure anti-virus software is up-to-date.
- Take care when opening emails and attachments, as this is a primary infection vector.
- Ensure control system servers and workstations are not being used for email access or general web browsing.

**Additional steps for securing Niagara-based systems**
For Niagara customers, please use this as an opportunity to review our Niagara security documentation, which contains step-by-step guidance and best practices for securing and configuring Niagara AX- and Niagara 4-based systems:

- Niagara AX Hardening Guide
- Niagara 4 Hardening Guide

**Additional information**
Ransomware is a type of malicious software that infects a computer and restricts access until a ransom is paid to unlock it. This can cause prolonged disruption to operations and loss of data. Ransomware generally replicates itself through the network. For example, if a workstation was to become infected, it would attempt to spread across all servers and workstations on the network. Governments discourage organizations and individuals from paying the ransom, as this does not guarantee access will be restored.

- Microsoft Security Bulletin MS17-010 (March 14, 2017, Rating: Critical): https://technet.microsoft.com/library/security/MS17-010
- US-Cert Alert on Multiple Ransomware Infections Reports (May 12, 2017): https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported
- US-Cert Alert on Ransomware Variants: https://www.us-cert.gov/ncas/alerts/TA16-091A

In addition to the details above, we received the following information directly from Microsoft:

**Summary**
The first and most important piece of guidance is to immediately deploy the security update associated with Microsoft Security Bulletin MS17-010, if you have not done so already. Customers who have automatic updates enabled or have deployed this update are already protected from the vulnerability these attacks are trying to exploit.

**Malware detection**
Windows Defender, System Center Endpoint Protection and Forefront Endpoint Protection detect this threat family as Ransom:Win32/WannaCrypt.

In addition, the free Microsoft Safety Scanner http://www.microsoft.com/security/scanner/ is designed to detect this threat, as well as many others.

**Recommendations**
Review the Microsoft Security Response Center (MSRC) blog at Customer Guidance for WannaCrypt Attacks for an overview of the issue, details of the malware, suggested actions and links to additional resources.

Keep systems up-to-date. Specifically, for this issue, ensure Microsoft Security Bulletin MS17-010 Security Update for Microsoft Windows SMB Server is installed.

Customers who believe they are affected can contact Customer Service and Support by using any method found at this location: https://support.microsoft.com/gp/contactus81?Audience=Commercial.

**Microsoft malware detection and removal tools**
Use the following free Microsoft tools to detect and remove this threat:

- Windows Defender: https://www.microsoft.com/en-us/windows/windows-defender
- Microsoft Safety Scanner: http://www.microsoft.com/security/scanner/

**Additional resources**

- Microsoft Security Response Center Blog: http://blogs.technet.microsoft.com/msrc
- Microsoft Malware Protection Center Blog: http://blogs.technet.microsoft.com/mmpc
- Microsoft Safety and Security Center webpage: http://www.microsoft.com/security/default.aspx

**Regarding information consistency**
We strive to provide you with accurate information in static (this mail) and dynamic (web-based) content. Microsoft's security content posted to the web is occasionally updated to reflect late-breaking information. If this results in an inconsistency between the information here and the information in Microsoft's web-based security content, the information in Microsoft's web-based security content is authoritative.