WannaCry/WannaCrypt Ransomware Attack

Issue

Starting early Friday morning (May 12), ransomware attacks using an exploit for the SMB (Server Message Block) protocol on Microsoft Windows were executed across businesses in hundreds of countries. The ransomware effected a number of businesses in a variety of industries. The ransomware goes by various names such as WannaCry, Wcry, WannaCrypt, or Wanna Decryptor.

Description

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 (link is external) vulnerability on March 14, 2017 for Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012, and Windows 10. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 (link is external) operating systems on May 13, 2017. The WannaCry ransomware will spread through the SMB vulnerability from an infected machine.

One possible infection vector may be through phishing or opening infected documents from unknown sources.

Affected Units

Customers using Microsoft Windows operating systems are affected by WannaCry ransomware. Woodward controls (MicroNet, MicroNet+, Atlas, 505) are not affected by the ransomware. Microsoft Windows devices may be used with a Woodward control to provide HMI (Human Machine Interface) capabilities in the control system.

Impact to NT CPU and Atlas PC (NT version):
Investigation regarding the impact of WannaCry on the NT CPU revealed at least one vulnerable port is open (TCP Port 139). Further probing of this port with tools designed to test the WannaCry exploit were not successful in spreading the virus via the known methods to the NT CPU. This port cannot be disabled in the operating system; it is advised to block this port with an external firewall as an in-depth defense measure.

Corrective Action

The following description and guidance is from US-CERT Alert (TA17-132A). Woodward recommends reviewing the **Impact** and implementing the **Recommended Steps for Prevention** and **Recommendations for Network Protection:**

Impact

Woodward controls (MicroNet, MicroNet+, Atlas, 505) are not directly affected by the WannaCry ransomware. However, devices used to monitor and control Woodward products (Windows-based HMI computers, for example) may be impacted. Devices impacted by WannaCry may lead to a disruption of control system operations or a loss of control system visibility.

Other consequences: Ransomware not only targets home users but businesses as well. Businesses infected with ransomware can experience negative consequences that include:

- temporary or permanent loss of sensitive or proprietary information
- disruption of regular operations
- financial losses incurred to restore systems and files
- potential harm to an organization's reputation

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Solution for Microsoft-based devices (computers and servers)

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
    - Ensure that anti-virus and anti-malware solutions are set to automatically conduct regular scans.
    - Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should use them only when necessary.
    - Configure access controls including file, directory, and network share permissions with least privilege in mind. If users only need to read specific files, they should not have write access to those files, directories, or shares.
    - Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
    - Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
    - Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.
    - Test your backups to ensure they work correctly upon use.

Recommendations for Network Protection

Apply the patch (MS17-010). If the patch cannot be applied, consider:

- Disabling SMBv1 and
- Blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Customer Action

Review Corrective Action above for impact on your industrial control system. Review **Additional Information** below.

Additional Information

ICS-CERT Indicators Associated with WannaCry Ransomware:
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01C

ICS-CERT Factsheet on WannaCry Ransomware:
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware.pdf

Microsoft Support - Disabling SMB:
https://support.microsoft.com/enus/help/2696547/how-to-enable-anddisable-smbv1,-smbv2,-and-smbv3-inwindows-vista,-windows-server-2008,--windows7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

WOODWARD

PO Box 1519, Fort Collins CO 80522-1519 USA
1041 Woodward Way, Fort Collins CO 80524 USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.