Health Advisory:

Recent Attacks With WannaCry Ransomware: Prevention and Remediation

May 18, 2017

This document will be updated as new information becomes available. The current version can always be viewed at http://www.health.mo.gov.

The Missouri Department of Health & Senior Services (DHSS) is now using 4 types of documents to provide important information to medical and public health professionals, and to other interested persons:

Health Alerts convey information of the highest level of importance which warrants immediate action or attention from Missouri health providers, emergency responders, public health agencies, and/or the public.

Health Advisories provide important information for a specific incident or situation, including that impacting neighboring states; may not require immediate action.

Health Guidances contain comprehensive information pertaining to a particular disease or condition, and include recommendations, guidelines, etc. endorsed by DHSS.

Health Updates provide new or updated information on an incident or situation; can also provide information to update a previously sent Health Alert, Health Advisory, or Health Guidance; unlikely to require immediate action.

Office of the Director
912 Wildwood
P.O. Box 570
Jefferson City, MO 65102
Telephone: (800) 392-0272
Fax: (573) 751-6041
Website: http://www.health.mo.gov

Health Advisory
May 18, 2017

FROM: **RANDALL WILLIAMS, MD**
DIRECTOR

SUBJECT: **Recent Attacks With WannaCry Ransomware: Prevention and Remediation**

A widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States. The software can run in as many as 27 different languages. The latest version of this ransom-ware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, and has spread rapidly. One possible infection vector is via phishing emails. In addition, according to news reports, it is already inspiring imitators.

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware spreads easily when it encounters unpatched or outdated software. The WannaCry ransomware may be exploiting a vulnerability in Server Message Block 1.0 (SMBv1). Microsoft released a patch in March that addresses this specific vulnerability, and installing this patch will help secure your systems from the threat.

Specific steps for prevention and remediation from the Cyber Division of the Federal Bureau of Investigation (FBI) are shown in the Appendix.

For additional information on mitigation, users and administrators are encouraged to review the article from the United States Computer Emergency Readiness Team (US-CERT) on Microsoft SMBv1 Vulnerability (https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability) and the Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/library/security/MS17-010).

For general advice on how to best protect against ransomware, review US-CERT Alert TA16-091A (https://www.us-cert.gov/ncas/alerts/TA16-091A). Please report any ransomware incidents to the Internet Crime Complaint Center (IC3) (https://www.ic3.gov/default.aspx).

Individual users are often the first line of defense against this and other threats, and everyone is encouraged to update his or her operating systems and implement vigorous cybersecurity practices at home, work, and school. These practices include:

- Update your systems to include the latest patches and software updates.
- Do not click on or download unfamiliar links or files in emails.
- Back up your data to prevent possible loss, whether you are at a home, work, or school computer.

Sources:

1. Indicators Associated With WannaCry Ransomware (FBI) https://content.govdelivery.com/attachments/USDHSCIKR/2017/05/13/file_attachments/816377/FLASH_WannaCry_FINAL.PDF
2. DHS Statement on Ongoing Ransomware Attacks (DHS) https://www.dhs.gov/news/2017/05/12/dhs-statement-ongoing-ransomware-attacks
3. Multiple Ransomware Infections Reported (US-CERT) https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported

Appendix

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 e-mails from reaching the end users and authenticate in-bound e-mail using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent e-mail spoofing.
- Scan all incoming and outgoing e-mails to detect threats and filter executable files from reaching the end users.
- Ensure 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 only use them when necessary.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs 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 e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Develop, institute and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Have regular penetration tests run against the network, no less than once a year, and ideally, as often as possible/practical.
- Test your backups to ensure they work correctly upon use.

Recommended Steps for Remediation

- Contact law enforcement. You are strongly encouraged to contact a local FBI field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser.