MS-ISAC

MS-ISAC Security Primer

Ransomware

March 2017, SP2017-0716

Ransomware is a type of malware that blocks access to a system, device, or file until a ransom is paid. This almost always occurs when the ransomware encrypts files on the infected system (*crypto ransomware*), although a few variants are known to erase files or block access to the system using other methods (*locker ransomware*). The cyber threat actors behind ransomware most commonly demand that the victim pays $200 - $1,000 in bitcoins, though other currencies, gift cards, and ransoms of up to several thousand dollars are occasionally reported. Ransomware almost always involves opportunistic targeting, with dissemination through malvertising or spam emails containing malicious attachments. In the past several months, MS-ISAC has become aware of several ransomware variants that include additional, independent components, such as data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components.

RECOMMENDATIONS:

Securing Networks and Systems

- Know what is connected to and running on your network. Keep all hardware, operating systems, applications, and software up-to-date and patched.
- Use antivirus programs with automatic updates of signatures and software.
- Perform regular backups of all systems to limit the impact of data loss and store the backups offline as some ransomware is able to encrypt backup files if they are connected to the network. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Verify the backups are operational. Rebuilding or reimaging an infected system from a known good backup or fresh installation is the only known way to guarantee an infection has been removed from a system.
- Implement an anti-spam solution to help stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments. If possible, disable the use of macro scripts in Office.
- Apply the Principle of Least Privilege and consider implementing network segmentation.
- Consider the use of a proxy server for Internet access and/or ad blocking software.
- Implement software restriction policies or other controls to prevent unauthorized programs from executing, especially when stored in locations frequently used by malware, such as temporary folders.
- If possible, use virtual environments as they help provide isolation and enable faster recovery.
- Vet and monitor third parties that have remote access into the organization's network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
- Consider disabling user access to personal webmail and social media accounts.
- Ensure that staff know where and how to report suspicious emails and possible infections.

Securing the End User

- Provide social engineering and phishing training to employees. Urge them not to open suspicious emails, not to click links contained in such emails, not to post sensitive information online, and to never provide usernames and/or passwords to any unsolicited request

Responding to a Compromise/ Attack

- Unplug the infected systems from the network to prevent further infections.
- Restore files from regularly maintained backups

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.