MS-ISAC®

MS-ISAC Security Primer

Ransomware

May 2018, SP2018-0424

Ransomware is a type of malware that blocks access to a system, device, or file until a ransom is paid. This is achieved when the ransomware encrypts files on the infected system (crypto ransomware), although some variants erase files (wiper) or block access (locker ransomware) to the system using other methods. If the crypto ransom is not paid within a specific time frame, the cyber threat actors will destroy the decryption keys, making decryption impossible. If the wiper ransomware is not paid within a specific time frame, the ransomware generally starts permanently deleting files. Currently there are opportunistic and strategic forms of ransomware.

Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT and legal costs, network modifications, and/or the purchase of credit monitoring services for employees/customers.

- *Opportunistic* ransomware seeks to infect as many victims as possible. Once access to the system or files is blocked, the ransomware demands a ransom in order to unlock the files, frequently $200 - $1000. The majority of opportunistic ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website. More rarely, ransomware infects computers through malvertising. A few variants of opportunistic ransomware spread via Server Message Block (SMB) vulnerabilities and use of the Eternal Blue tool.
- *Strategic* ransomware may also be referred to as extortion. In these instances the victim entitiy is strategically targeted or the actors realize that a sensitive entity has been infected. The ransom/extortion demand's amount will often vary based on the cyber threat actor's assessment of the victim's ability and need to pay. These dollar amounts can range from a few thousand dollars to $50,000 or more. The result of the infection is the same, with all files being permanently encrypted or deleted if the extortion is not paid. The Multi-State Information Sharing and Analysis Center (MS-ISAC) has observed a notable increase in ransomware variants that strategically target networks through unsecured or brute forced remote desktop protocol (RDP) or virtual network computing (VNC) connections.

Payment - The most common variants of ransomware require payment in bitcoins, although other cryptocurrencies, gift cards, and payment methods are sometimes indicated. However, paying the ransom does not guarantee an organization will regain access to its data as not all cyber threat actors will respond to payments, and some variants are unable to decrypt files or may have deleted the files.

Decryption - Due to coding and other mistakes, some variants of ransomware can be unlocked or decrypted without paying than ransom. NoMoreRansom.org, a website run by multiple cybersecurity vendors and government agencies, collects and shares all known decryption keys.

Additional Capabilities - Since 2016, ransomware variants features have expanded to include data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components. One wiper variant deletes files regardless of whether or not a payment was made. Another variant includes the capability to lock cloud-based backups when systems continuously back up in real-time (a.k.a. during persistent synchronization). Other variants target smartphones and Internet of Things (IoT) devices.

Although not as common, some variants claim to be from a law enforcement agency and that the user owes a "fee" or "fine" for conducting illegal activities, such as viewing pornography. In an effort to appear more legitimate, these variants use techniques to identify the victim's geographic location in order to use the name of a specific law enforcement agency. *No U.S. law enforcement agency will ever remotely lock or disable a computer and demand a fine to unlock it.*

RECOMMENDATIONS

The following recommendations are provided to help mitigate the risk of ransomware infections. These recommendations are not comprehensive but provide general best practices.

Securing Networks and Systems

- **Have an incident response plan** that includes what to do during a ransomware event.
- **Backups are critical.** Use a backup system that allows multiple iterations of the backups to be saved and stored offline, in case the backups include encrypted or infected files. Routinely test backups for data integrity and to ensure you can recover from them.
- **Keep all systems patched,** including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date. Use a centralized patch management system if possible. Ensure that patch MS17-010 (CVE-2017-0147) is applied to all systems to protect against SMB exploitation via Eternal Blue.
- **Use antivirus and anti-spam solutions.** Enable regular system and network scans with antivirus programs enabled to automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network.
- **Implement application white-listing and software restriction policies (SRP)** to prevent the execution of programs in common ransomware locations, such as temporary folders.
- **Disable macro scripts**. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Consider **adding a warning banner** to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.
- **Restrict Internet access.** Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.
- **Apply the principles of least privilege and network segmentation.** Categorize and separate data based on organizational value and where possible, implement virtual environments, and the physical and logical separation of networks and data. Apply the principle of least privilege.
- **Increase security controls** for all network protocols that could allow for lateral movement within a network.
- **Audit for unauthorized access attempts, brute forcing, and the use of common pen-testing tools**, such as Metasploit.
- **Secure Server Message Block (SMB)**
    - Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
    - Disable the use of SMB (port 445) between endpoints and where possible, restrict SMB to communication between endpoints and file servers.
    - Limit and audit files accessible via SMB shares.
    - Patch the Windows MS17-010 / CVE-2017-0147 vulnerability.
- **Secure Remote Desktop Protocol (RDP)**
    - Assess the need to have RDP, port 3389, open on systems and, if required, whitelist connections to specific, trusted hosts.
    - Verify cloud environments adhere to best practices, as defined by the cloud service provider.
    - After cloud environment setup is complete, verify that RDP ports were not accidentally re-enabled, unless required for a business purpose.
    - Place any system with an open RDP port behind a firewall and require users to VPN in through the firewall.
    - Perform regular checks to ensure RDP is not open to the public Internet.
- **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.
- **Participate in cybersecurity information sharing** programs and organizations, such as MS-ISAC and InfraGard.

Securing the End User

- **Provide social engineering and phishing training to employees.** Urge them not to open suspicious emails, not to click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites.
- **Consider blocking file attachments** that are commonly associated with malware, such as .dll and .exe, and attachments that cannot be scanned by antivirus software, such as .zip files.
- **Remind users to close their browser** when not in use.
- **Have a reporting plan** that ensures staff know where and how to report suspicious activity.

Responding to a Compromise/Attack

- **Immediately implement the incident response plan.**
- **Identify, disconnect, and shutdown** infected and non-infected systems, isolating them from the network, to prevent further propagation. Consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.
- **If the incident appears to involve strategic targeting** and an extortion demand, immediately notify the local Federal Bureau of Investigation (FBI) field office.
- **Determine the affected data,** as some sensitive data, such as electronic protected health information (ePHI) may require additional reporting and/or mitigation measures.
- **Determine if a decryptor is available.** Online resources, such as NoMoreRansom.org, can help.
- **Restore** files from regularly maintained backups and rebuild systems as appropriate.
- **Determine the infection vector** and ensure the vulnerability is mitigated.
- **Report the infection.** It is highly recommended that SLTT government agencies report ransomware incidents to MS-ISAC. Other sectors and home users may report infections to the local FBI field office or to the Internet Crime Complaint Center (IC3).

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.