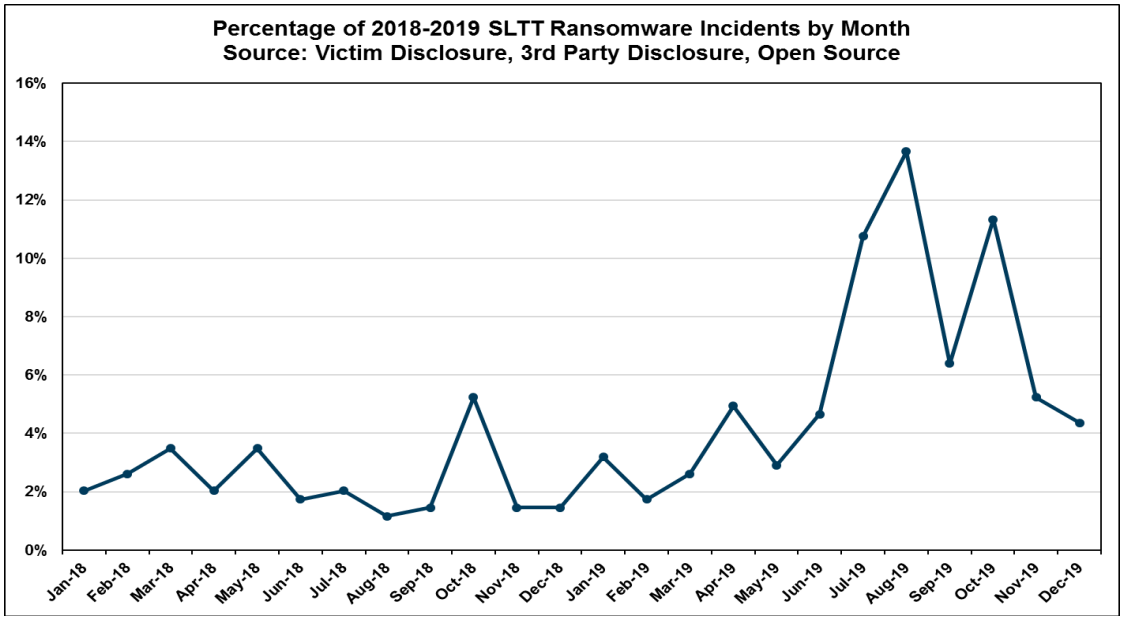
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
May 2020 • SP 2020-0002

Ransomware

The MS-ISAC in 2019 observed a 153% increase in the number of reported SLTT government ransomware attacks from the previous year. Many of these incidents resulted in significant network downtime, delayed services to constituents, and costly remediation efforts. The MS-ISAC largely attributes this increase to Ryuk ransomware infections and compromises affecting Managed Service Providers (MSP) that service SLTT governments. Not only are victims at risk of losing access to their systems and files, but they may also experience financial loss due to legal costs, purchasing credit monitoring services for employees/customers, or ultimately deciding to pay the ransom. The effects of a ransomware attack are particularly catastrophic when they impact emergency services and critical infrastructure, such as 911 call centers and hospitals.



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), threatens to erase files (wiper ransomware), or blocks system access (locker ransomware) for the victim. The ransom amount and contact information for the cyber threat actor (CTA) is typically included in a ransom note that appears on the victim's screen after their files are locked or encrypted. Sometimes the CTA only includes contact information in the note and will likely attempt to negotiate the ransom amount once they are contacted.

Opportunistic and Strategic Ransomware Campaigns

- **Opportunistic** ransomware campaigns employ "spray and pray" tactics, techniques, and procedures (TTPs). The ransomware is propagated through user-initiated actions, such as clicking on a malicious link in a spam e-mail, visiting a malicious or compromised

website, or via malvertising. A few variants of opportunistic ransomware spread via Server Message Block (SMB), sometimes through the use of the EternalBlue exploit. However, an initially opportunistic TTP, such as a victim opening a widespread malicious email attachment could turn into a strategic campaign, if the CTA takes further direct actions based on the specific target.

- **Strategic** ransomware campaigns occur when the victim is specifically targeted or, more often, the actors realize that a sensitive entity has been infected via initially opportunistic methods. After an initial network compromise, CTAs will map out the network to ensure the most critical data is identified and targeted during the ransomware encryption process. During this initial infection phase, CTAs seek to escalate privileges to an administrator or domain controller level, while also identifying and targeting data backups, so that the victim cannot easily regain control of the network or restore their files once their data is locked or encrypted. This helps ensure CTAs can deploy the ransomware fully across the network to achieve complete saturation. The ransom amount will often vary based on the CTA's assessment of the victim's network and data as well as their ability and need to pay.

Common Infection Vectors

Ransomware is primarily delivered through:

- Malicious attachments/links sent in an email. This is known as "malspam."
- Network intrusion through poorly secured ports and services, such as Remote Desktop Protocol (RDP) (e.g. Phobos ransomware variant).
- Dropped by other malware infections (e.g. initial TrickBot infection leading to a Ryuk ransomware attack).
- Wormable and other forms of ransomware that exploit network vulnerabilities (e.g. the WannaCry ransomware variant).

Additionally, open-source reporting indicates that CTAs are targeting managed service providers (MSPs) to push out the ransomware to multiple entities. This occurs when CTAs compromise an MSP and use their existing infrastructure to disseminate the ransomware to the MSP's clientele. This exploits the trusted relationship between the customer and their MSP.

Recently Observed TTPs

Over the past few years, the MS-ISAC observed an increase in TTPs that allow CTAs to evade detection and maximize the impact of their attacks. These TTPs include "living off the land" (LOTL): deploying publicly available pen testing suites or tools (e.g. Cobalt Strike, Metasploit, or Mimikatz), to specifically target domain controllers and Active Directory to gain network wide access and deploy fileless ransomware to evade signature-based antivirus.

LOTL involves using legitimate or whitelisted network administration tools on the network or system to accomplish the CTA's main objective, such as finding and encrypting critical data. For example, CTAs are known to use PowerShell and PsExec to execute commands and obfuscate traffic (i.e., using Base64 encoding to mask activity until execution) on compromised networks. The use of legitimate administration and pen testing tools allow CTAs to easily enumerate the network to find more systems and higher privileged accounts with the goal of targeting the domain controller and pushing out the ransomware via Active Directory.

Decryption

Backing up important data is the single most effective way of recovering from a ransomware

infection. If the victim has backup copies then they can restore their files once infected systems are quarantined.

- Organizations should ensure that backups are appropriately protected and stored offline or out-of-band, so that attackers cannot target them. Using cloud services could help mitigate ransomware infections since many retain previous versions of files, allowing you to roll back to the unencrypted data.
- With any backup strategy, it is important to verify that the backup data you are restoring from is not also infected.

In the event that backups are not an option, victims may consider:

- Checking available tools online to decrypt files, as security researchers have already broken the encryption algorithms for some ransomware variants. The NoMoreRansom Project has decryptors available for such variants.
- Rebuilding the network from scratch.
- Paying the ransom, which is ultimately a business decision. The MS-ISAC does **not** encourage victims to pay the ransom as it further incentivizes this criminal behavior, but understands this may sometimes be the only available option.

Payment

The ransom demand is typically in the form of cryptocurrency, which is most often Bitcoin though this varies between variants. Ransom demands range from as little as several hundred dollars up to and exceeding one million dollars. It is not uncharacteristic to see multi-million-dollar ransom demands in the current threat landscape. The ransom note often entails a sense of urgency, designed to socially engineer victims into paying the ransom quickly. CTAs may also place additional pressure on the victim by increasing the ransom amount on scheduled intervals (e.g., every 24 hours). Additionally, CTAs may threaten to delete the decryption keys, ransomed data, or publicly post exfiltrated data if the victim fails to pay or exceeds the predetermined pay deadline.

Recommendations

The following recommendations are provided to help mitigate the risk of ransomware infections:

- Update or create an incident response plan that includes what to do during a ransomware event.
- If not already being done, perform regular system backups. As ransomware is known to delete Volume Shadow Copies, ensure that backups are created and stored off-site or out-of-band. Also, use a backup strategy that allows multiple iterations of the backups to be saved and stored, in case the backups include encrypted or infected files. Routinely test backups for data integrity and to ensure you can recover from them.
- For any publicly-exposed services, such as Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and File Transfer Protocol (FTP), assess the need for exposure to the Internet. Consider applying additional controls, such as IP whitelisting or multi-factor authentication, where possible.
- Assess the need to have Remote Desktop Protocol (port 3389) and Server Message Block (SMB) (port 445) open on systems and, if required, consider limiting allowed connections to only specific, trusted hosts.
- Enable heightened monitoring for SMB activity throughout the network. Make sure to disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
- Consider filtering inbound and outbound traffic based on IP addresses (and ports), leveraging geographic blocking and threat-based blocking.

- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Provide end-user training to help users identify suspicious emails or links and ensure that users are aware of the potential dangers of opening unsolicited emails. Also ensure users are aware of any support policies and procedures in place for assistance.
- If you do not have a policy regarding suspicious emails, consider creating one and specify that all suspicious emails should be reported to the security and/or IT departments.
- Ensure all user accounts fall under (and are not exempt from) acceptable policies associated with password aging, password complexity, and account lockout.
- Perform network segmentation according to organizational functionality and apply access controls between trust zones.
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators and never reuse the same credentials across multiple accounts or systems.
- Review any vendor accounts and their associated passwords to ensure they have been changed from their default settings.
- If remote access for the user account is required by a third-party vendor, consider developing a process that keeps the user account disabled until access is needed.
- Implement robust Windows Event logging, including an increase in the maximum file size for the Event Logs. Centralize and protect these logs out-of-bound and consider a backup solution, to help prevent counter-forensic log during an active compromise.
- Utilize application whitelisting on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing. (CIS Subcontrol 2.7)
- Restrict PowerShell execution to signed scripts and trusted scripts used for administration.
- Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis. (CIS Subcontrol 8.2)
- Strongly consider utilizing behavioral-based detection methods, as they can help identify the malicious use of open source penetration testing suites and legitimate network administration tools.
- Implement a centrally-managed, up-to-date anti-malware solution. In addition to valuable preventive and corrective capabilities, detective controls provided by anti-malware software are beneficial in providing awareness of any threats which may become active within the environment.
- Keep all operating systems, applications, and essential software patched and remove unsupported legacy systems to mitigate easy exploitation. This may include purchasing extended support for legacy systems that are critical to operations.
- If not already being done, consider implementing an Intrusion Detection System (IDS) to detect command and control (C2) activity and other potentially malicious network activity, such as the MS-ISAC's Albert system.
- Ensure that systems are hardened with industry-accepted guidelines, such as those provided by the CIS Benchmarks division.
- Review and consider implementation of the 20 CIS Controls, where appropriate, as a means of bolstering your organization's security posture.

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. For more information about this topic, please contact intel@cisecurity.atlassian.net. For 24x7 cybersecurity assistance, please contact 866-787-4722 or SOC@cisecurity.org. The MS-ISAC is interested in your comments - an anonymous feedback survey is available.