Reduce the Risk of Ransomware Awareness Campaign

January 2021

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) is leading a ransomware awareness campaign, ***Reduce the Risk of Ransomware***, with information and resources for organizations and individuals to use. Also, CISA is emphasizing nine smart cyber habits individuals and organizations should implement to avoid falling victim to ransomware.

WHAT IS RANSOMWARE

Ransomware is a type of malicious software, or malware, designed to infect computers and encrypt files until a sum of money or other form of ransom is paid. After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible devices.

Malicious cyber actors commonly distribute ransomware through phishing emails or "drive-by downloads." Phishing emails are messages that appear to be from a legitimate organization or a contact familiar to the victim, which can entice the user to click on a corrupt link or open an infected attachment. A "drive-by download" is a program that automatically downloads from the internet without the user's consent and often without their knowledge. It is possible the corrupt code may run after download, without user interaction. After the code has run, the computer becomes infected with ransomware.

WHY SHOULD YOU CARE?

Consequences of a ransomware attack can be severe, and there is no guarantee a user will recover their data, even if they chose to pay the ransom money. On a personal level, an infection can result in financial damage or disclosure of sensitive information. On an organizational level, ransomware can cause business operation disruptions, financial damage from a payout or costly investigations, and reputational damage causing loss of current or potential customers.

Additionally, the goal of ransomware is not always to get money but potentially to serve as a distraction for other malicious purposes. These distractions could be hiding a traditional attack against the network, covering traces of an earlier attack, providing cover while data is stolen from the network, or even limiting or destroying productivity of the system while the IT team is busy dealing with a very visible ransomware infection.

SMART CYBER HABITS

During this awareness campaign, CISA emphasizes nine key messages that promote smart cyber behaviors or actions that individuals and organizations should implement to help prevent and mitigate ransomware attacks.

1. **Keep Calm and Patch On** – Patching is essential for preventive maintenance that keeps machines up-to-date, stable, safe, and secure against malware and other cyber threats.
2. **Backing Up Is Your Best Bet** – It is critical to set up offline, encrypted backups of data and to regularly test your backups. The more you automate your backup system, the more frequently you can back up your data.
3. **Suspect Deceit? Hit Delete.** – If an email looks suspicious, do not compromise your personal or professional information by responding or opening attachments. Delete junk email messages without opening them.
4. **Always Authenticate** – Implement multifactor authentication (MFA) to prevent data breaches and cyber-attacks. This includes a strong password and at least one other method of authentication.
5. **Prepare and Practice Your Plan** – Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

6. **Your Data Will Be Fine If It's Stored Offline** – Local backups, stored on hard drives or media, provide a sense of security in case any issues occur. Keep your backup media in a safe and physically remote environment.

7. **Secure Your Server Message Block (SMB)** – SMB vulnerabilities allow their payloads to spread laterally through connected systems like a worm. CISA recommends all IT professionals disable their SMB protocols to prevent ransomware and other malware attacks.

8. **Paying Ransoms Doesn't Pay Off** – The U.S. government recommends against paying any ransom to cyber-crime organizations or malicious cyber actors. Paying a ransom only funds cybercriminals, and there is no guarantee that you will recover your data if you do pay.

9. **Ransomware Rebuild and Recovery Recommendations** – Identify the systems and accounts involved in the initial data breach and conduct an examination of existing detection or prevention systems. Once the environment is fully cleaned and rebuilt, issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility.

CISA RESOURCES

In addition to the tips listed above, CISA's new Ransomware webpage is revamped to feature crucial information such as:

- Official Alerts, Updates, and Statements from CISA, to help system administrators and other technical staff bolster their organization's security posture.
- Guides and Services, including tips and best practices for individuals, organizations, and technical staff to guard against ransomware.
- Fact Sheets and Infographics featuring easy-to-use, straightforward information to help organizations and individuals better understand the threats and the consequences of a ransomware attack.
- Trainings and Webinars with information for technical and non-technical audiences, including managers, business leaders, and tech specialists with an organizational perspective and strategic overview.

Other key features and resources on the Ransomware webpage are:

- Ransomware Guide – Prevention Best Practices and Response Checklist: a customer-centered, one-stop resource with best practices and ways to prevent, protect and respond to a ransomware attack
- CISA INSIGHTS – Ransomware Outbreak: provides background information on specific cyber threats and the vulnerabilities they exploit, as well as a ready-made set of mitigation activities
- Ransomware Reference Materials for K-12: information about increased cyber-attacks on K-12 schools and remote learning and best practices to avoid becoming a victim of ransomware

Ransomware has become a significant cyber threat to our nation, claiming victims such as local governments, hospital networks, and most recently K-12 schools. While ransomware incidents are prevalent among government entities and critical infrastructure organizations, individuals are still very much at risk. Malicious actors can target anyone with a device connected to the internet or important data stored on their network. In some cases, personal attacks may be more detrimental considering home users don't typically have a backup strategy in place.

If you are become a victim of ransomware attack, you should report it to CISA at https://us-cert.cisa.gov/report.