ENTERPRISE
information services

CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

July 2023 | Volume 1

IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER

What is Ransomware? & How Does it Happen?

Ransomware is a type of malicious software that encrypts the data on a victim's device or network and demands a ransom for its decryption. The ransom is usually paid in cryptocurrency or other untraceable forms of payment.

If the ransom is not paid within a specified time, the data may be permanently deleted or exposed to the public. Ransomware attacks can cause significant damage to individuals, businesses, and organizations by disrupting their operations, compromising their privacy and security, and extorting large sums of money.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's been infected with malware. Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

Cyber Security Services Webinar - Save the Date!

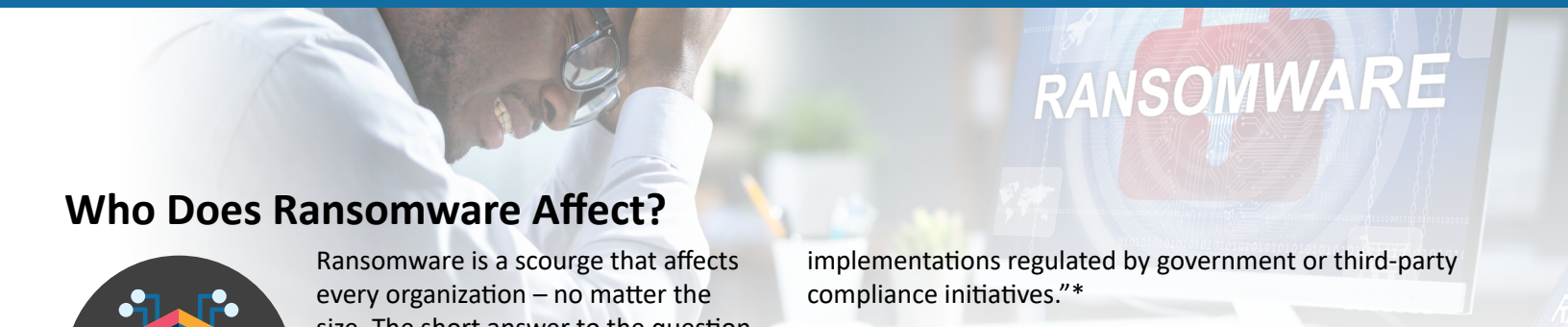
» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

SOME COMMON RANSOMWARE VECTORS OF ATTACK ARE:

- Phishing emails with malicious attachments or links
- Exploiting unpatched vulnerabilities in software or systems
- Remote desktop protocol (RDP) compromise or brute force
- Drive-by downloads from compromised websites
- Network propagation through shared drives or devices

For more information scan the QR code or visit our website
ransomwareinfo.oregon.gov

ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.



Who Does Ransomware Affect?

Ransomware is a scourge that affects every organization – no matter the size. The short answer to the question is 'everyone.' Every small business, midsized company, enterprise, and organization is fair game.

"No vertical, government, or organization is immune to its effects. Unfortunately, some are more susceptible to successful attacks, based on the type of technologies they deploy, their age, cost for replacement, identity governance and privilege maturity, and overall cyber security hygiene implementations regulated by government or third-party compliance initiatives."*

Everyone is a target of ransomware. While ransomware typically spreads to impact as many assets as possible, it might only impact one user. In these situations, the threat actors may ask the user for a small fee to decrypt their files. The threat actors may not see your organization's data as important, but they know your data is important to you and your ability to do your daily activities. The goal is to hinder your ability to do those activities. It is important to train users to never negotiate and pay these ransoms.

*Morey Haber, vice president of technology for BeyondTrust

QUESTIONS TO ASK YOUR IT STAFF OR IT PROVIDER:

- How often do you backup our data? Do you maintain offline backups?
- How do you monitor and respond to suspicious activity on our network?
- What are the steps to restore our systems in case of a ransomware infection?
- How do you train and educate our staff on ransomware awareness?
- Do we have an incident response retainer that will provide additional incident response capabilities and computer forensics?

Additional Resources:

National Institute of Standards and Technology (NIST)
csrc.nist.gov

Cybersecurity & Infrastructure Security Agnecy (CISA)
cisa.gov/stopransomware
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
fbi.gov/contact-us/field
Portland Office 503-224-4181
Ransomware Safety Resource

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

Oregon Cybersecurity State Incident Response Team
503-378-5930 | eso.soc@das.oregon.gov

Oregon Emergency Response System
(OERS) 1-800-452-0311

Statewide Interoperability Team
503-373-7251 | swic.or@das.oregon.gov

For more information scan the QR code or visit our website
ransomwareinfo.oregon.gov

ENTERPRISE information services

ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.