RANSOMWARE

What It Is & What To Do About It

What is Ransomware?

Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Government Efforts to Combat Ransomware

While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact of ransomware on the networks of state, local, tribal, and territorial governments, municipalities, police and fire departments, hospitals, and other critical infrastructure. These types of attacks can delay a police or fire department's response to an emergency or prevent a hospital from accessing lifesaving equipment. To combat this threat, the NCIJTF has convened an interagency group of subject matter experts to educate the public on ways to prevent ransomware attacks, to improve law enforcement coordination and response, and to enable and sequence whole-of-government actions that impose consequences against the criminals engaged in this malicious activity. The Cybersecurity and Infrastructure Security Agency (CISA) leads a number of efforts including —CISA Cyber Essentials—and—CISA Insights— to assist entities in protecting themselves from cyber incidents like ransomware. More about these efforts and the tools CISA offers can be found at https://www.cisa.gov/ransomware. The FBI's IC3.gov website has additional ransomware focused resources that can be found at https://ic3.gov/Home/Ransomware.

Common Infection Vectors

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.

- Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web market - places to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.

- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

RANSOMWARE

What It Is & What To Do About It

Best Practices To Minimize Ransomware Risks

1. Backup your data, system images, and configurations, test your backups, and keep the backups offline
2. Utilize multi-factor authentication
3. Update and patch systems
4. Make sure your security solutions are up to date
5. Review and exercise your incident response plan

How Ransomware Has Impacted The Public Sector

The examples below may show the impacts in terms of ransom paid or service restoration cost, but it is difficult to calculate the total impact/costs of a ransomware infection. In addition, paying a ransom does not guarantee that stolen sensitive data will not be sold on the dark web.

- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but they were not isolated from the network, allowing them to be infected as well. The county paid a $132,000 ransom.

- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

- A U.S. county's computer systems were infected by Ryuk. The attackers demanded over $1.2 million in Bitcoin for a decryption key. Officials decided to rebuild their systems rather than pay the ransom and spent $1 million in new equipment and technical assistance. A user allegedly opened a malicious link or attachment which caused the infection.

Reporting Information

- The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

Victims of ransomware can file a complaint with law enforcement or report incidents by:

- **Contacting your local federal law enforcement field office**
- **Filing a complaint with the Internet Crime Complaint Center (IC3)** https://ic3.gov/Home/Ransomware
- **Contacting NCIJTF CyWatch 24/7 support at 1-855-292-3937**
- **Reporting incidents, phishing, malware or vulnerabilities with CISA** https://us-cert.cisa.gov/report