United States Secret Service Cybercrime Investigations

# PREPARING FOR A CYBER INCIDENT

## A GUIDE TO RANSOMWARE

## PREPARE

### What is Ransomware:

Ransomware is a type of malicious software (malware), which denies access to systems or data and/or exfiltrates data.

### How Ransomware Works:

Typically, the malware displays an on-screen alert advising the victim that their device is locked or their files are encrypted. In some cases, after an initial infection, ransomware attempts to spread to connected devices and systems.

### Characteristics:

Non-encrypting ransomware locks the screen and restricts access to files.

Encrypting ransomware prevents computers from being booted up in a live environment by encrypting the Master Boot Record (MBR).

Leakage or "extortionware" exfiltrates data.

Mobile device ransomware infects cellphones through drive-by downloads or fake apps.

### How Ransomware is Used:

Cyber actors hold systems or data hostage until a ransom is paid for a decryption key. Cyber actors also threaten to publish exfiltrated data, or sell it on the dark web. Increasingly, cyber actors request virtual currency transfers as a ransom payment method.

### Incident Response (IR) Planning:

The U.S. Secret Service developed a Preparing for a Cyber Incident - Introductory Guide, which describes what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations.

### Paying Ransom Demand:

Paying the ransom does not guarantee regaining access. In some cases, a decryption key was not provided in return to a paid ransom. In other cases additional ransom was demanded.

### Contacting Law Enforcement:

Reach out to law enforcement before contacting the cyber actor. Include law enforcement in your response plan. Contact the local U.S. Secret Service Cyber Fraud Task Force.

United States Secret Service Cybercrime Investigations

# PREPARING FOR A CYBER INCIDENT

## A GUIDE TO RANSOMWARE

## PREVENT

| | |
|---|---|
| **Patches** | Update operating systems, software, and firmware on devices with the latest patches. Consider using a centralized patch management system. |
| **User Permissions** | Restrict user permissions for installing and running software applications. Apply the principle of least privilege to all systems and services. |
| **Email Scanning** | Scan all incoming and outgoing emails to detect and filter threats, such as phishing and spoofing emails, and executable files (used to perform various functions or operations on devices). This will prevent them from reaching end users. |
| **Firewalls** | Configure your firewalls to block access to known malicious IP addresses. |
| **Application Whitelisting** | Use application whitelisting to reduce the risk of execution of malware, and unlicensed and unauthorized software. An application whitelist is a list of applications and application components that are authorized to execute on a host. |
| **Awareness** | Implement a training and awareness program for all employees. |
| **Controls** | Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations (temporary folders supporting popular Internet browsers, compression/ decompression programs). |
| **Remote Access** | Consider disabling Remote Desktop Protocol (RDP) if it is not being used. |
| **Virtualization and Separation** | Execute operating system environments or specific programs in a virtualized environment (multiple simulated environments). Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. |
| **Backups** | Have cold storage backups and test restoration of backup files regularly. This prevents the ransomware from infecting network-connected backup files. |

United States Secret Service
Cybercrime Investigations

# PREPARING FOR A CYBER INCIDENT

## A GUIDE TO RANSOMWARE

## RESPOND

**A.** Do not power down or shutoff any systems affected by ransomware.

**B.** Isolate the infected device and the compromised portion of your network as soon as possible.

**C.** Secure backups by taking them offline and ensure they are free of malware.

**D.** Use out-of-band methods of communication, and do not trust the entire network system.

**E.** Collect and secure partial portions of the ransomed data that might exist.

**F.** Collect all available log information.

**G.** Change online account and network passwords after removing the system from the network.

**H.** Use the oldest back-up to restore the system, if you have multiple backups.

## IDENTIFY AND RECORD THE FOLLOWING INFORMATION:

- ✓**Ransomware variant name.**
- ✓**What systems are affected.**
- ✓**Original emails with full headers and any attachments, if attack was executed by phishing.**
- ✓**Copies of executables or other files dropped onto the system after accessing malicious attachments, including a splash page.**
- ✓**Any domains or IP addresses communicated with just prior to or during infection.**
- ✓**Virtual currency addresses to which payment is requested, and the amount being requested.**
- ✓**Any forensic analysis or incident response reports completed.**
- ✓**Any memory captures taken during execution of the malware.**
- ✓**Status of the infection.**
- ✓**Provide network topology.**

**Contact the local U.S. Secret Service**
***Cyber Fraud Task Force Network Intrusion Team***