Ransomware Response Guide

Gillware™
Digital Forensics

1802 Wright Street
Madison, WI 53704
forensics@gillware.com

***Ransomware** is malware that denies access to files on your computer, mobile device, or network by encrypting them or making them otherwise inaccessible, and demands that payment be made in order to regain access.*

There are some basic actions you can take which will be helpful in nearly every Ransomware case. Here's how to respond in order to have the best chance for data recovery.

Disconnect the affected computer from any attached network and from the Internet. This includes any Wi-Fi, Bluetooth, or other wireless connections.

- Ransomware is designed to reach out to attached data storage connections, drives, and devices in order to encrypt as many files as possible. Disconnecting will interrupt that process and minimize damage. Also, some ransomware attacks include human intervention, meaning that there might be an unauthorized individual on your network. Disconnecting interrupts that person's access to your systems.

Think before you act. Ransomware attacks are high stress situations, and can result in hasty actions that inadvertently do more harm than good.

- Actions such as moving and copying files, running malware remediation software, and attempting to restore stale backups to affected data storage devices will likely negatively affect the possibility of potential data recovery without paying the ransom.

Determine the scope of the problem. Check for unauthorized encryption of:

- External hard drives and USB Devices (including mobile phones) that were attached to the affected computer at the time of infection
- Mapped or shared network drives, directories, and folders
- Backups
- Cloud based data storage accounts
- Determine if the attack involved potential transfer of data in addition to encryption of files

Know your options. The "proper" response to a ransomware attack varies, and will ultimately depend *upon:*

- *The specific variant of ransomware*
- *Regulatory requirements for your organization*
- *The potential impact and importance of the hostage data*
- Your organization's risk tolerance
- *The impact of the attack on business continuity*
- *Whether there are backups or redundant systems available*

Potential response options include:

- **Hire a reputable data recovery, forensics, or incident response entity to assist.** Ransomware attacks present complex problems that can call for expert advice and experience. It may be possible to recover some or all of the affected data. An expert can help you assess the damage and provide sound advice about how to most efficiently and effectively recover from a ransomware attack, as well as preventing future occurrences. They can also help you determine the source of the infection or beach, and assist in remediation of the problem. An expert may be needed to provide documentation about the ransomware attack for insurance or regulatory purposes. They may assist as a knowledgeable go-between to communicate with law enforcement or even with the person(s) demanding the ransom and to assist in obtaining Bitcoin or other acceptable payments.

- **Do nothing.** Restore your encrypted data from unaffected recent backups or simply accept the loss of some or all of the encrypted data, remove the ransomware malware.
    - You may want to keep a copy of the encrypted data in the event a decrypting program becomes available in the future.
    - Determine how your computer or network was infected and make remediation efforts in order to prevent re-infection.
    - Consider contacting law enforcement and/or appropriate regulatory agencies if determined to be appropriate or legally necessary.

- **Attempt to decrypt the data on your own.**
    - Determine the type and version of ransomware involved and attempt to find a decrypting program. Attempts to decrypt on your own may or may not be successful depending upon the ransomware involved, and attempting to decrypt data may overwrite unused space on data storage volumes affecting potential data recovery efforts.
    - Whether you are successful or not, you will want to determine how your computer or network were infected and make remediation efforts in order to prevent re-infection.
    - Determine how your computer or network was infected and make remediation efforts in order to prevent re-infection.
    - Consider contacting law enforcement and/or appropriate regulatory agencies if determined to be appropriate or legally necessary.

- **Pay the ransom, or have someone do so on your behalf.** This is a controversial and high risk response. There are those who believe that payment of ransom encourages additional illegal behavior and exasperates the problem. Depending upon the circumstances, ransom payment may be a necessary evil in order to recover data crucial to the continued operation of a business, which cannot be otherwise recovered. Unfortunately, there is no guarantee that payment of the ransom will result in successful decryption of the data.
    - Communicate with the ransomware actors and obtain instructions regarding payment.
    - Provide payment to ransomware actors. Payment is generally accepted via crypto-currency methods such as Bitcoin.
    - Follow the instructions provided by the ransomware actor in order to decrypt your data.
    - Determine how your computer or network was infected and make remediation efforts in order to prevent reoccurrence.

No amount of paranoia is improper when working to remove Ransomware from your network infrastructure. We see an alarming amount of Ransomware reoccurrence. Reoccurrence is typically timed to happen within a few months after the original infection event. After the victim has paid a bounty of bitcoins, and right around the time the company gets back to normal operations, they get hit again because the bad guy placed backdoors in the network or gained a different, distinct intrusion mechanism during the original hack.