Ransomware Rescue Guide

What is Ransomware?

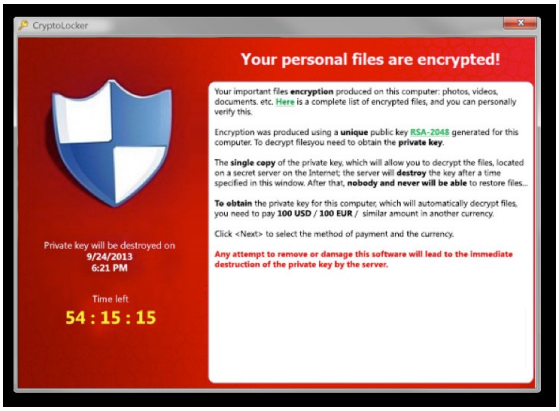
Ransomware is a malicious piece of software hackers place on your computer so they can encrypt your data and then demand payment from you to regain access to your files. Hackers use a variety of methods to install vectors to infect a machine: phishing emails, unpatched programs, compromised websites, online advertising and free software downloads.

Not only can ransomware encrypt the files on your computer, the software is smart enough to travel across your network and encrypt any files located on shared network drives. This can lead to the catastrophic situation whereby one infected user can bring an entire company to a halt.

Once the files are encrypted the hackers will display some sort of screen or webpage informing you your files are being held hostage and demanding payment to unlock the files. Also, typical ransomware has a 48-72 hour deadline after which the ransom increases. Hacker demand payment in e-currency such as Bitcoin.

How to Know if You're Infected

- You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
- An alarming message has been set to your desktop background with instructions on how to pay to unlock your files.
- The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files.



On Line Support
TECH SOLUTIONS

www.ols.technology info@ols.technology

Van: 360.993.0600 PDX: 503.227.0442

Ransomware Rescue Guide

I'm Infected, Now What?

1. **Disconnect:** Immediately disconnect the infected computer from any network it is on. Turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.

1. **Determine the Scope: Did the infected machine have access to any of the following?**

   Shared drives

   Shared folders

   Network storage devices of any kind

   External hard drives

   USB storage devices of any kind

   Cloud-based storage such as DropBox, Google Drive or One Drive.

3. **Determine Ransomware Strain:** For example CryptoWall, Teslacrypt, etc.

4. **Determine Your Response:** Now that you know the scope of your encrypted files as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

   Response A: Restore your files from backup and remove the ransomware from your infected system.

   Response B: Try to decrypt your files.

   Response C: Do nothing.. Meaning you will lose your files.

   Response D: Pay the ransom. Follow the instructions given to you by the hackers and pay the ransom to release your files. Ransomware is big business….over$1 billion in ransom was collected by hackers in 2018 Hackers know if they don't return your files to you after paying the ransom, at some point, people will stop paying ransoms altogether. Many of them actually have customer service numbers or chats you can reach out to who will assist you in paying your ransom and getting your files back. However, paying the ransom is no guarantee your files will be returned to you.

On Line Support
TECH SOLUTIONS

www.ols.technology info@ols.technology

Van: 360.993.0600 PDX: 503.227.0442

Ransomware Rescue Guide

Protect Yourself from Ransomware Attacks

1. Educate your users:

Educate your staff on what to look for to prevent criminal applications from being downloaded/ executed and conduct simulated phishing attacks to inoculate users against ransomware attacks.

2. Implement and Maintain Software Based Protection:

- Ensure you have and are using an up-to-date firewall.
- Install antispam/antiphishing protection such as SonicWall.
- Ensure all devices are using top notch and up-to-date antivirus software or advanced endpoint protection products.
- Have strong software restriction policies to prevent unauthorized applications from running.
- Be diligent about applying patches that update any and all applications with vulnerabilities.

3. Backup, Test, and Backup Again:

Consistently backup your files and regularly test restore procedures. Backups can be either on-site or in the cloud, but to help prevent your backups from being compromised, you should always have an off-site or redundant backup in place. Having off-site and recent backups is a standard best-practice to protect you against not only ransom attacks, but natural and other disasters. Be sure to test your restoration procedure to make sure your backed-up files actually work.

About On Line Support

Since 1998, On Line Support has partnered with businesses and organizations to provide IT solutions that enhance productivity, security and growth.

Managed IT Services

On Demand Support

IT Projects

Technology Consulting

Security Services

Security Testing and Training

Telecom and Internet Service

Allworx Phone Systems

On Line Support
TECH SOLUTIONS

www.ols.technology info@ols.technology

Van: 360.993.0600 PDX: 503.227.0442