## UNDERSTANDING YOUR NETWORK:

# RANSOMWARE

409-899-4438

936-634-1952

www.cmsiptech.com

CMS IP TECHNOLOGIES

Delivering Technology - Making a Difference

# RANSOMWARE

## Theft

*A criminal act in which property belonging to another is taken without that person's consent.*

The term ***theft*** is sometimes used synonymously with Larceny. ***Theft***, however, is actually a broader term, encompassing many forms of deceitful taking of property, including swindling, embezzlement, and false pretenses. Some states categorizes all these offenses under a single statutory crime of theft.



## What is Ransomware?

Ransomware is a type of malware that can be installed on a computer without the user's knowledge. This malware restricts access to computer files located directly on the computer or on external drives or mapped drives to servers. Typically, it will encrypt the files making them unusable.

## How Ransomware Works

Ransomware is commonly installed on a computer through a Trojan. This Trojan can be delivered in the form of an email attachment or embedded into a website. Once ransomware has encrypted the files on a workstation, the virus can then travel across your network and encrypt any files located on both mapped and unmapped network drives and stopping all productivity. After encryption has taken place, a screen will appear explaining how to pay to unlock the files using a type of e-currency such as Bitcoin. If ransom is paid, the hijacker states that they send you the necessary information to "decrypt" your files. Unfortunately at this point, you can only take them for their word and there are never any guarantees.

# RANSOMWARE

## So Where Did it Come From?

Ransomware typically comes from three places, email attachments, free software downloads, and what's commonly called a "drive-by-download".

**Email attachments** are the most common method for installing ransomware. Users receive an email with an attachment and by simply clicking on the attachment to open, install the virus on their PC. The attachment may open to a blank document or not open at all, but the damage is done without ever seeing it happen.

**Free software downloads** is a very tempting offer. Usually, it is a "free version" or called a "cracked" version of rather expensive software. By enticing and getting you to click to download on your own, it makes it easier for the virus to bypass the PC's securities that are in place.

**"Drive-by-Downloads"** are installed by visiting websites that have infected content within the site. These websites can be compromised by using out of date browsers or plugins or unpatched 3rd-party applications. Hackers will find security flaws in out of date applications and use it to their advantage until the security bug is patched.

# RANSOMWARE

## Tools of the Trade

***Some of the most common terms that you may hear in regards to ransomware may include, TOR & Bitcoin.***

**TOR (Anonymity Network)** is a network and browser developed to enhance and anonymize Internet traffic. TOR sites cannot be browsed to by a regular browser and all traffic is encrypted. The network was designed completely to anonymize and hide the originating and ending destination of the traffic. Because of the anonymity, it has become a well used tool by cybercriminals to communicate or host files, making it difficult for law enforcement or government to track their actions.

**Bitcoin** is an form of e-currency has no physical form is stored in a digital wallet. Bitcoins (or BTC) are completely untraceable and transfers to and from accounts are done with complete anonymity, providing the perfect scenario for illegal activities.

## Signs You Are Infected

Here are some of the most common signs of infection:

- A popup screen alerting you that you are infected and must pay a ransom to gain access to your files again
- Opening files and not seeing legible content, but what appears to be random characters
- Errors when opening files, telling you that your file is corrupted or the file extension is not correct
- A window that opens to a ransomware program and does not allow you to close it
- Files listed in your file explorer with names like DECRYPT.TXT or DECRYPT_INSTRUCTIONS.HTML

# RANSOMWARE

## What to Do When You Are Infected

### Disconnect

Immediate disconnect your PC from the network to prevent any further spreading of the virus to the network. Turn off wireless or Bluetooth and disconnect any USB or external drives. *If you are a CMS NetWatch Managed Services customer*, the Help Desk will have you turn the PC off while we dispatch an engineer onsite.

At this point, we highly recommend you contact your IT administrator. Evaluations will be done to determine the extent of the infection and if other devices on the network were affected, including the server.

## Securities to Prevent or Reduce your Risk

We fully believe in layers of security. Having the right tools in place does not guarantee this will not happen to your business, but it does reduce the risk and makes recovery afterwards less costly.

### Here are Some of Our Recommendations:

**Antivirus–** A professional level antivirus program will help eliminate a majority of threats to your computers.

**Mananged Firewall with Content Filtering—**A managed firewall with security services in place will prevent users from visiting websites which could threaten your network.

**Email/SPAM services—**A managed services for email will help block SPAM and viruses that come through email in the form of attachments or “dangerous” links.

**Network Data Backup & Recovery—**Having a reliable data backup and recovery solution in place will prevent you from losing critical data in the event your network is threatened.

**User Education—**Proper training for staff to know where to save their data for backups and what should and should not be downloaded or click on.

# RANSOMWARE

## In Conclusion

Nothing is fool-proof, but with user awareness and proper network security policies in place, we can reduce the likelihood of infection and prevent a complete and total loss afterwards with a reliable recovery plan in place.

# ABOUT CMS IP TECHNOLOGIES

**www.cmsiptech.com**

***Interested in What Managed Services Can Do For You?***

CMS IP Technologies offers over 30 years of IT experience. As the demand for network security has grown, so has CMS. With offices located in both Beaumont and Lufkin, we are prepared to answer your questions.

409-899-4438

936-634-1952

www.cmsiptech.com

CMS IP TECHNOLOGIES

Delivering Technology - Making a Difference