MICROLAND
COMPUTER CENTER

Technical Bulletin

Ransomware: Preparing for the threat

What is Ransomware?

In the vast world of online interaction lives a multitude of nefarious entities attempting to steal, use, or sell your information to the highest bidder. One of the most devastating forms of this unknown threat is ransomware.

Ransomware's most potent ingredient in causing wide-spread damage is the end user.

How do I get Ransomware?

Ransomware can infect an end user's system through the opening an email attachment, a malicious URL link embedded in an email, and even downloading programs that may look like legitimate software.

Once your computer is infected with the ransomware virus, it installs an agent behind-the-scenes that begins encrypting ALL of your files. This can mean word documents, spreadsheets, pictures, PDFs, videos, audio files, accounting data, and much more.

After the virus is done encrypting files on your computer, it then moves on to encrypt the files on the network shares and mapped drives.

Age of the Ransomware

• • •

The concept of file-encrypting ransomware was invented and implemented by Young and Yung at Columbia University and was presented at the 1996 IEEE Security & Privacy conference. Another term used to describe ransomware is "cryptoviral extortion" and the term's inspiration sprung from the fictional facehugger in the science fiction movie *Alien*.

What happens after my files are encrypted?

Once encrypted, there is no guarantee that the infected files can be recovered. Your best bet is a recent, uncompromised backup.

Created by Kirk Lampo November 2015 - Updated July 2019

If you try to open an infected file, you will get an error message stating that the file is corrupted, unsupported, or unrecognized.

How do I protect myself from ransomware?

The best practice to keep files protected from ransomware is <u>prevention</u>.

Regularly updating your computer's security and operating system components, resetting passwords several times per year, having trusted and up-to-date antivirus and antimalware software, maintaining updated firewall protection on device's network, and of course, a frequent remote backup system with up-to-date software licensing.

What else can I do?

DO educate your staff on how to practice safe web surfing and email usage.

DO communicate to your technical support and management team the <u>moment</u> you think you accidentally clicked on something suspicious or if your device seems to be acting "out of the ordinary" (slow to open programs, new software icons suddenly appearing, programs crashing, files not opening, etc.).

DO keep antivirus and antimalware protection on your computer at all times and keep it up to date.

DO frequently backup your workstation using a secure, cloud based software.

What should I not do?

DO NOT open email attachments or click on URL's from email addresses you do not recognize.

DO NOT allow a program to make changes to your device unless you know exactly what it does.

DO NOT save your files on your local computer.

> *Your local documents will always be the first line of destruction in the event of ransomware. Ask your technical support team where you should be storing your files to ensure your files are stored remotely and backed up.*

DO NOT over rely on your system's security. As a user, you give your system permission to download files and software that are potentially dangerous.

And lastly…

DO NOT panic or pay the ransom.

Where can I find additional information?

https://www.us-cert.gov/Ransomware

https://en.wikipedia.org/wiki/Ransomware

https://www.malwarebytes.com/ransomware/

MICROLAND
COMPUTER CENTER
4431 Iberville Street
Mandeville, LA 70471
985-626-7900
www.microlandcomputers.com

Created by Kirk Lampo November 2015 - Updated July 2019