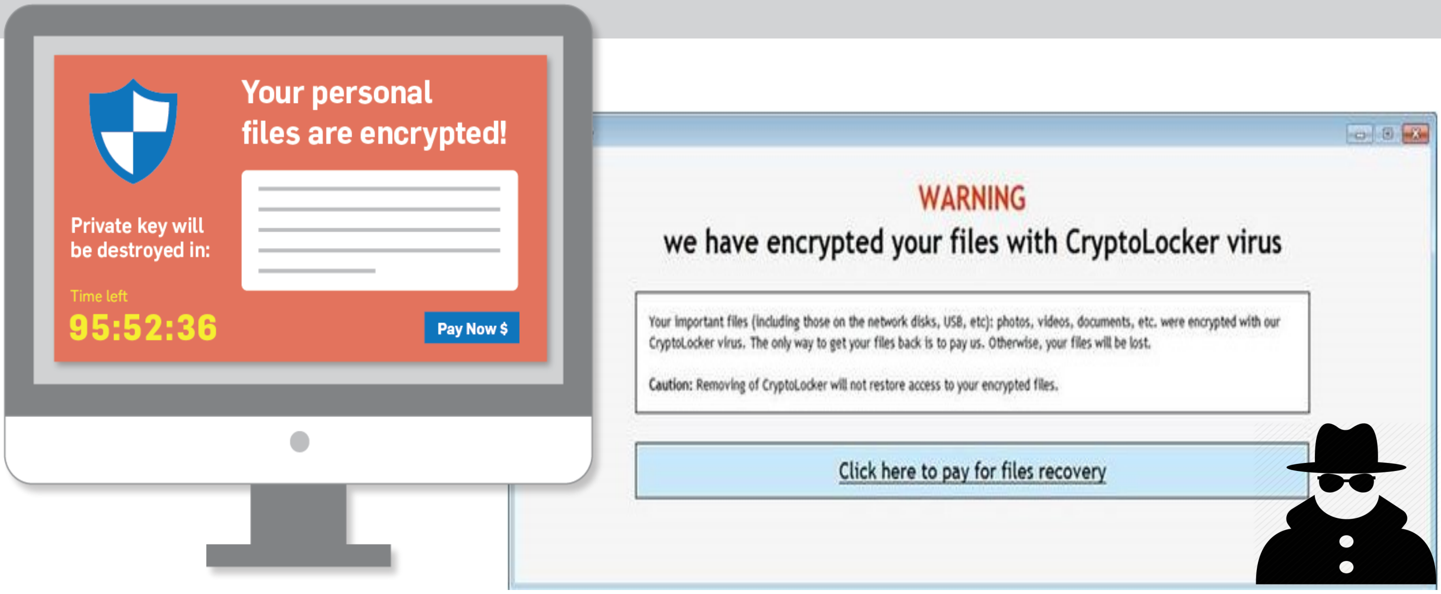
YOU'RE VULNERABLE TO RANSOMWARE IF...

- You use legacy software.
- Your browser and/or OSes are unpatched.
- You operate with outdated equipment.
- You don't have a legitimate backup plan.
- You lack a comprehensive cyber-security strategy.



Your personal files are encrypted!

Private key will be destroyed in:

Time left

95:52:36

WARNING

we have encrypted your files with CryptoLocker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our CryptoLocker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of CryptoLocker will not restore access to your encrypted files.

RANSOMWARE 101: 4 Things You Need to Know

Ransomware is a variant of malware that criminals greatly love, it is easy for them to execute and is financially rewarding. Below are 4 things you should know about ransomware.

1) The Basic Process is a Marvel of Simplicity

Criminals primarily deliver malware through spam or a phishing attack, luring you into clicking on a link that will release a program that will lock up your computer/s and files in just a few minutes. Once everything is nicely locked up, the criminal sends you a ransom demand to unlock your computer, generally asking you to pay a ransom.

3) Sophisticated Ransomware Has Reared Its Head

Ransomware attacks are not only proliferating, they're becoming more sophisticated, noted the FBI in a recent article. The FBI pointed out that because email systems got better at filtering out spam, cybercriminals turned to spearphishing emails that target specific individuals. In some recent instances of ransomware, criminals didn't use emails at all. "These criminals have evolved over time and now bypass the need for an individual to "click on a link, said James Trainor, FBI Cyber Division Assistant Director. " They do this by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers."

2) There Are Two Main Kinds of Ransomware

The file-encrypting version encrypts all the data it finds in the computer it infects. *The screen-locker version* locks the screen of the infected computer and renders it useless. The former is much more popular, probably because the bad guys want their victims to be able to use their computers to pay their ransoms.

4) How to Prevent Ransomware

Deploy advanced antivirus and endpoint protection solutions. They will help you to eliminate the vulnerabilities that enable cybercriminals to hijack your PCs and infect you with ransomware. Learn to understand how ransomware works. Don't click on links or attachments from suspicious or unsolicited emails. Train yourself to be aware of phishing scams. Back up your data. If you can quickly restore your files and access your data even if it is infected, Then you won't have to pay a ransom.

TO LEARN MORE ABOUT HOW TO PROTECT YOUR BUSINESS FROM RANSOMWARE CONTACT US TODAY

Kevin@AYSROC.com or 585-645-6300

AYS | TECHNOLOGIES