CMIT Solutions®
Your Technology Team

4 WAYS TO FEND OFF CRYPTOWALL, THE LATEST RANSOMWARE VIRUS THREAT

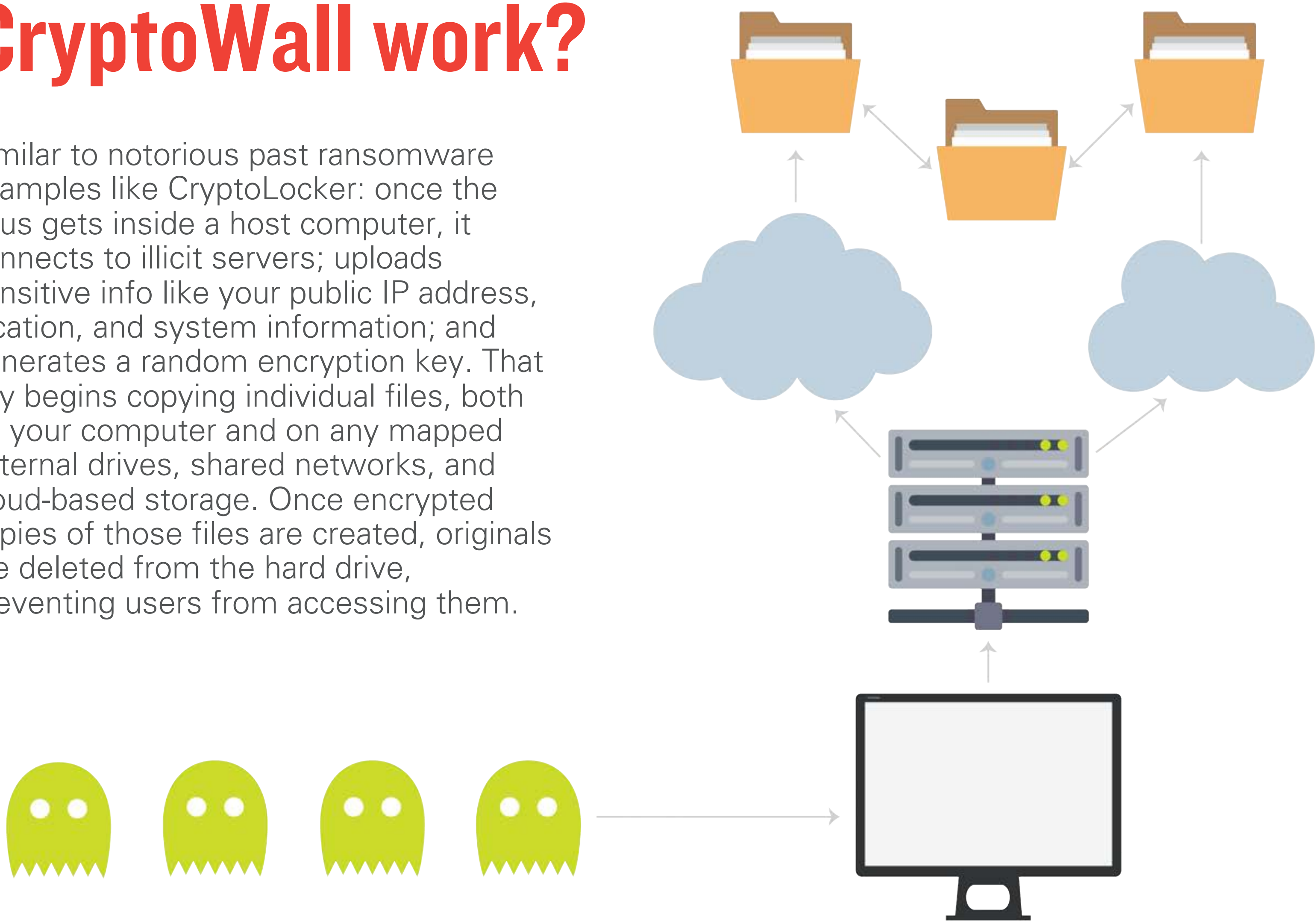
A White Paper by CMIT Solutions

SPREADS THROUGH COMPROMISED BANNER ADS ON LEGITIMATE WEBSITES

A new virus is flexing its corrupting muscle on computers and users worldwide. CryptoWall first appeared in February, but attention surrounding the ransomware spiked this summer, when researches at Dell SecureWorks reported on it. In October, the UK Register revealed that 830,000 victims had been infected — a 25% increase since August. The scariest aspect of CryptoWall is that it's spreading via "malvertising," or compromised banner ads on legitimate websites like Yahoo, AOL, and MSN. The infection is transmitted via Flash, so if a user simply visits an affected website with Flash enabled in their browsers, the user's PC can be infected without even clicking on anything malicious. This means most anti-virus programs are unable to prevent CryptoWall, leaving any computer and user vulnerable.

How does CryptoWall work?

Similar to notorious past ransomware examples like CryptoLocker: once the virus gets inside a host computer, it connects to illicit servers; uploads sensitive info like your public IP address, location, and system information; and generates a random encryption key. That key begins copying individual files, both on your computer and on any mapped external drives, shared networks, and cloud-based storage. Once encrypted copies of those files are created, originals are deleted from the hard drive, preventing users from accessing them.



How do I know if I've been infected?

Two telltale signs:

1) If you attempt to open a file and the data is jumbled or not displaying properly (example below), and

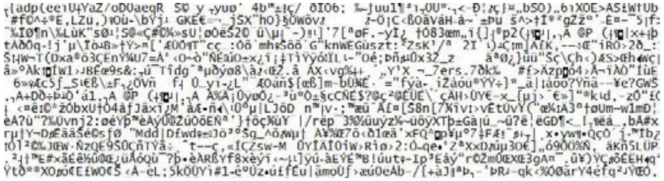


Image Source: http://www.teachscience.net/wp-content/uploads/2014/04/uncorrupted.jpg

2) If you attempt to open a file and get something like "DECRYPT_INSTRUCTION" instead. This will provide instructions for paying a ransom (usually $500 to $1,000) and obtaining a decryption key, which sometimes works to retrieve data and sometimes doesn't. Even when it does, it's a time-consuming task.

DECRYPT INSTRUCTION

So what can you do to AVOID INFECTION?

Have a trusted IT professional assess the security of your systems.

1

Due to the slippery "malvertising" aspect of CryptoWall, stopping it requires more than just anti-virus and a firewall. Limiting admin rights for user PCs, applying DNS filters, implementing strict browser settings, and employing constantly updated behavioral anti-spyware can help. But these are complicated measures that most business owners don't have the time or ability to keep up with. Only nonstop vigilance can properly address the CryptoWall threat — and that kind of 24/7 service is what an IT professional like CMIT Solutions specializes in.

2

Implement regular, remote backups and a sound disaster recovery plan.

Businesses should be creating comprehensive image-based off-site backups multiple times a day. If a virus like CryptoWall hits a 20-person firm at 4:00 PM, and that firm has to rely on an encrypted backup from the night before to get up and running again, those employees will lose an entire day of work. Remember, a local backup plugged in to a computer will still be susceptible if CryptoWall infects your system!

Do not open ANY email or attachment from ANY sender you don’t recognize.

3

Although CryptoWall has morphed into a Flash-based “malvertising” approach, email security is still paramount. Never open attachments you aren’t expecting, even if they appear to come from legitimate looking email accounts.

4

Validate ANY link in ANY unfamiliar email before clicking on it.

Malicious links arrive in spam emails — many disguised as FedEx, UPS, or USPS shipping updates — every day. Make sure you hover over all links and look for legitimate IP addresses, not long strings of random characters, before clicking. All it takes is one click on one bad link by one employee to compromise the data of your entire company. Avoiding the threat of viruses like CryptoWall is possible with diligent and continuously updated security measures. But accidents can happen, which makes a strong backup solution critical to the success of your business. Want to know whether your systems and data secure? Contact CMIT Solutions today.

At CMIT Solutions, we worry about IT so you don't have to.

That means you can concentrate on doing your job and effectively manage your time while we take care of the tech issues. If you're looking for more ways to increase your productivity and efficiency, contact us today.

CONTACT US

CMIT Solutions®
Your Technology Team