Agility Network Services, Inc

Founded 1994 - (877) Agility

e-Newsletter!

June 2014

Rich Snippets

- Cryptolocker Virus
- Safe Computing

The Cryptolocker Ransonware virus is a virus that encrypts all of the data on an infected PC (Windows XP – Windows 8). Once this data is encrypted the end user must pay a ransom to obtain the key to decrypt the files. At this time there is no way to decrypt the files without paying for the key.

What Does this mean? It means, if your PC is infected with this virus, you will lose all files located on that PC that are not backed up.

What can I do to prevent my PC from being infected? The virus is most commonly spread using email and is usually delivered as a .ZIP attachment. If you practice safe computing you already know not to open files from unknown sources. There are also configuration changes that can made to the Windows system to help guard against this type of infection. Please talk to your Agility Consultant for more information and to plan to implement the safeguards listed below.

Additional Info on Cryptolocker

The original Cryptolocker “BotNet” has been seized and is under the control of the FBI. For the most part this is good news, however this also means that if you are infected with this variant of the virus there is no way to get your data back as you can no longer pay the ransom to get the key. If you do not have a good backup, all of the files on the local system will be lost.

Many edge protection devices (Firewalls and spam filters) will block this type of virus or email attachment from entering your network or inbox. However there are no security devices that catch everything. Keeping your firewall subscriptions and firmware up to date and continuing to perform regular maintenance and reviews of your network system is critical.

AMP AntiVirus (AVG) and anti-Malware (MalWareBytes) will detect and quarantine all known variants of this virus. However, the virus infects PC’s when the end user opens the infected attachment. At this point AVG and MalwareBytes will detect the infection but in most cases it will be too late. The virus will run and encrypt all files and neither program will be able to decrypt the files for you.

What can I do if my PC is infected?

- Disconnect from any network (wired and wireless) and shut down the PC. Call your Agility Consultant or the Agility Support Desk and work with them to determine how you will go about dealing with this issue.
- Pay the ransom and hope the encryption key works to decrypt the files. If you choose this option please work with your Agility Consultant before doing so. Your Consultant will make sure to take all the necessary precautions before making payment.
- Don’t pay the ransom and work with your Agility Consultant to restore Windows and your data.If you are using AMP (Agility Management Platform) to create image based backups this should take very little time and leave you with very little or even no lost data. If you are not doing this, please talk to your Agility Consultant about doing so to help prevent these types of issues in the future.

Safe Computing Part I

- Never open emails or email attachments that are from unknown or untrusted sources.
- Be careful as to what links you click on when searching the web. The “bad-guys” will often seed links to virus and malware infections current headlines. When someone searches the Internet for information those infected links show up with the regular search results. Read the URL you for the links you are going to click on. In most cases the URL will be a dead give-away as to whether the link is valid for your search.
- Keep your security software (Anti-virus, anti-Malware, firewall, Windows Updates, etc..) up to date.
- Use standard/limited user accounts for web surfing (not admin accounts). Standard user accounts do not have the required PC permissions to run many of the virus/malware infection programs and will help block the infection.

Questions, comments, feature requests? Call us at (877) AGILITY
Would you like to change your subscription? Email 'opt-out' to webmaster@agilitynetworks.com