Computer Bytes – April 2016 – The Cryptolocker Bug

Provided By: Harv Oliver, HANDS-ON Consultations

Hello friends and associates. The old saying goes “April showers bring May flowers.” Let’s hope that old adage holds up and we get some adequate rains to SoCal! This session I want to visit an issue that’s currently on the front pages, IT speaking, right now. We provide our information we share from experience, web site/tech site references, etc.

In September 2013 the Cryptolocker threat/bug began to be seen more widely (HOC in fact had a client infected during that timeframe). Since then, Ransomware has received a lot of news coverage which has decreased the number of uninformed victims and lowered the impact the malware Cyber criminals present along with decreasing the percentage of return to the criminal.

Due to this increased public awareness, cybercriminals have targeted a new type of extortion: **Cryptolocker** - and its picking up steam. We assisted a client a couple of months back and another just last week who had been compromised. Many of you may also have heard of a number of law enforcement offices, just as examples, whose entire systems have been infected.

This threat preys on a victim's biggest fear: losing their valuable data. Unlike previous Ransomware that locked operating systems and left data files alone and usually recoverable, Cryptolocker makes extortion of victims more effective because there is no way to retrieve locked files without the attacker's private key. YES – this statement is correct!

How do you get it? The normal process is victims receive spam email that use tactics to try and get you to open the attached ZIP or sometimes PDF file. If you open the file attached to the email, you will find an executable file disguised to look like an invoice report or some other similar ploy, depending on the email theme. Cryptolocker Trojans then encrypt and lock individual files, focused on Microsoft Office files (excel, word, etc.). It also jumps across network shares so it can infect files on the Server the local computer is networked with.

Let me get out this answer as I know some of you are thinking the question. I’ve had clients ask, “don’t we have antivirus?”. My answer always stays the same. Even if you do a user can always find a way to open an email attachment, even if your tools flag it, which in these types of cases may not as it’s embedded.

The severity of this bug is high. If files are encrypted by Cryptolocker and you do not have a backup of the file, it is likely that the file is lost. YES – again, this statement is correct!

Once infected, you may be presented a screen with a ransom demand. ALSO, infected files will often have extensions on them. Variables I’ve personally experienced are “LOL!” and “LOCKY”.

The common rule of thumb is you should never pay a ransom. Payment to cybercriminals only encourages more malware campaigns. Anyway, they’re crooks! There’s no guarantee that payment will lead to the decryption of your files.

Decryption without the key from your attackers is not possible at this time, however, there are solutions to get you back in business. A scan with new Antivirus definitions will be able to help detect and remove the executable file and prevent any further damage or a restore**.** You also delete all the encrypted files and restore them from their last known-good backup**.**

This issue goes to my always expounding on backups – I even close my articles with “until next time, don’t forget your backups!” Always backup your files! Keep your systems up to date with the latest virus definitions and software patches. Refrain from opening any suspicious unsolicited emails. Again, HOC’s slogan; when in doubt – delete!

NOTE: Our sharing of information within articles includes suggestions and tips. USE AND/OR APPLY AT YOUR OWN RISK. If you have any questions or concerns, please contact our offices for professional service/guidance.

Until next time, don’t forget your backups! For more information, contact Harv Oliver, HANDS-ON Consultations, (805) 524-5278, www.hocsupport.com