HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

ALERT

Issued 4/26/17

Ransomware Hiding inside Microsoft Word - Protect Yourself

Malware spreading through Microsoft Word macros is making a comeback, and an old strain of ransomware has taken advantage of the trend. Locky, a particularly nasty piece of ransomware that has no easy fix, is back, and it's taking advantage of your favorite word processor. Spotting it is fairly simple, but if you don't practice commonsense online security, you can kiss your files goodbye — probably forever.

The researchers at Abingdon, England-based security firm Sophos discovered the ransomware making the rounds by email, hidden deep within a string of files, and detailed their findings in a blog post. The website MyOnlineSecurity had a similar warning. Sophos' description referred to "a macro hidden inside a Word document that is in turn nested within a PDF," all contained within a single malicious email attachment. The scam begins with an email with "Receipt" or "Payment Receipt," followed by a random number, as the subject line. Attached is a PDF documenting your purported purchases that it contains a prompt to open a document in Microsoft Word. The unsolicited, nonspecific receipt email, the attachment, and the PDF trying to open another program should all raise red flags. Should you follow the steps anyway, then Microsoft Word will open and prompt you to run macros.

This is where the average user could run into trouble: If Word macros are enabled by default, then the Locky ransomware will infect your computer. If not, you'll get a prompt as to whether or not you want to let a Word macro run. While the Locky ransomware is as disastrous as Sophos makes it sound — unlike with some other encrypting ransomware strains, there's no effective decryption tool available — the average user has no fewer than five opportunities to stop it. First, delete any suspicious emails. Failing that, then at least don't open any suspicious attachments. Should you disregard that advice, don't let a PDF launch another application. Even if you've gone that far, you can still (probably) disallow Microsoft Word from running macros.

As an absolute last line of defense, the Sophos antivirus program will stop this variant Locky from installing on your computer; some other AV programs will as well, but there's no comprehensive list of which ones just yet. If you haven't tinkered too much with your Microsoft Word settings, you won't need to worry about the program running macros without permission. Macros are a big security risk, so they're disabled in Word by default. Still, if you want to double-check (or if you've enabled macros, and want to disable them), open Microsoft Word, then go to File, Options, Trust Center and then Trust Center Settings, and make sure one of the "disable" settings is checked. If you're curious about what Locky does, it's not pretty, but it's pretty standard encrypting ransomware. The malware encrypts all of your files in an unreadable .OSIRIS format, then demands money in Bitcoin for a decryption key. In theory, it's not a good idea to comply with the instructions; not all ransomware distributors keep their word to decrypt the files after payment, and exchanging information with cybercriminals can give them further personal details to leverage against you.

After Locky infects your machine, you can't do much except wait and hope that security researchers eventually devise a decryption method someday.

Back up your data regularly, keep your system patched, run a reliable antivirus program and don’t open strange emails. This won’t prevent 100 percent of cyberattacks, but it will prevent about 99 percent of them, and those are pretty good odds.