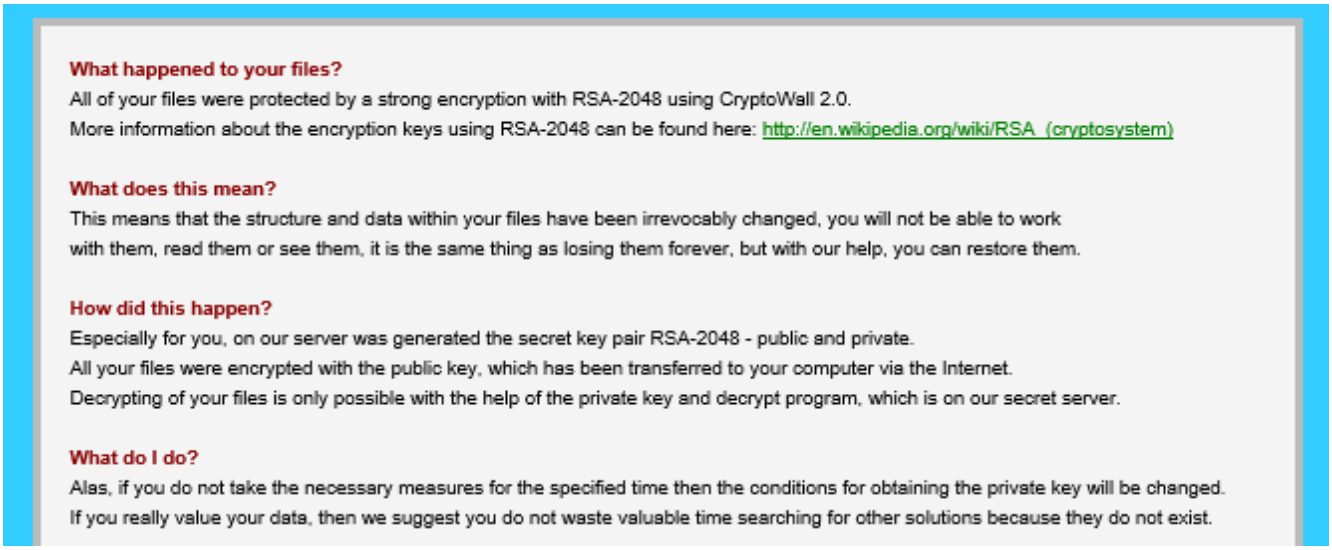
Alert: CryptoWall 2.0, CryptoLocker, WinLock, and Assorted Ransomware

Some of these new threats to documents on computers have made the network news, others will get there eventually. The short version: There is malware showing up in emails (as fake receipts and documents) and on websites (as fake 'you must update your system' messages), that will sit quietly in the background while it encrypts all your documents, and then will present an unapologetic ransom message on your screen.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

First thing we're asked about these ransoms is "Do they actually decrypt your files?" Well, the payment is untraceable, made by Bitcoin or by money orders entered by number into a hidden web site with an untrackable physical location. There's no way to pull back those payments. The reports in the repair community say that most machines are decrypted after payment (or else word would get around and their source of income would fall away), but the international law enforcement agencies are working to break these systems, and if you've paid a ransom, and that server goes down, no decryption can happen.

The second question: Can you recover the files? So far, the answers are: Yes, if you have backups that the malware could not see, in any form. No, not if you're relying on any backups built into Windows.

We have removed CryptoWall 2.0, and can add these points to the news reports:

• CryptoWall 2.0 encrypts everything it finds that looks like a document. What is lost includes photographs, web shortcuts & history and cookies and remembered passwords, favorites, email and contacts in Outlook, and so on. The damage is so severe that the only practical repair is to delete the user profile (your login on the computer) and create a new account. A better repair is to restore the computer from an 'image' backup of the entire drive.

• Besides documents from Word, Excel, and so on, encrypted files include text files used for program settings and database files that hold entries in nearly any kind of software. The result is that all specialty database programs need reinstallation. If you run an accounting program, either QuickBooks or Peachtree (now known as Sage), or a specialty business-management product for your industry, CryptoWall will damage it, and it will need reinstallation.

• CryptoWall and CryptoLocker also encrypt files on network drives that you reach by using a 'mapped' drive letter–it's the higher drive letters that point to your network drives and to your external hard drives. It also encrypts files in 'sync' folders, like those that are tied to cloud services, like Carbonite and DropBox. If files on a service

like Carbonite are encrypted, it's possible to get back older versions of files, but recovery may require a manual process of going to every file in your online backup and choosing to restore an older version from a date before the infection and encryption occurred. It's a clumsy approach and will take days–an image backup is the best backup.

Prevention

There are several things you need to do to prevent these infections, and to make recovery from these attacks possible:

1) Educate your staff and family–do not open unexpected attachments.

No bank sends attachments. No government agency sends them, and neither does any lottery. If an email is one line long, and says "You have to see this" plus a link or an attachment, delete it–it's fake and dangerous.

2) Keep all patches up-to-date.

In particular, keep Windows, Adobe Flash and Adobe Reader, and Oracle's Java, completely up-to-date at all times. Remember that these three companies generally release patches in bunches, on the second Tuesday of each month. Watch for them, and allow them to install. Java and Reader will add update icons to the system tray. If you don't actually need Java, and most users don't, uninstall it–less to update, fewer security holes to infect.

3) In Windows' folder options, turn off the feature "Hide extensions for known file types."

Here's why: Most malware infections that arrive by email are fake documents, receipts, reports, and so on. They arrive with a filename like "Bank-statement.pdf.scr" That's not a PDF file–it's an SCR file, which is a screensaver script, which has the ability to change Windows settings and install other software. By default, Windows hides the last "extension" on the name, '.scr' in order to provide a "helpful and unconfusing Windows experience." So the filename looks like "Bank-statement.pdf", which is a lie. Turning off that feature means that you will always see the entire filename, and be able to see if it really is a PDF or a DOC, and not an EXE (program) or an SCR or BAT or VBS (script file).

4) Work as a Standard User

Don't download files, read emails, or surf the 'net as an Administrator. Over 90% of all malware is stopped by using a limited or standard account–it can't install anything. Use a separate Administrator account for updating software, and for nothing else.

5) Keep an Antivirus program installed and updated.

6) Use automated full-drive 'image' backups.

The best backups are to drives that are invisible to CryptoWall, such as drives with only network paths, and no drive letters. Keep multiple copies–last night's file backup is probably partially encrypted, and a proper repair may have to go back to an earlier backup. If you're using a cloud backup, make sure it keeps file history.

Post-Infection

Disconnect the network cable of the infected computer, or disconnect from wireless. Turn off the computer. Then call us at 410-871-2877.

Check other computers on the network for copies of the ransom note; they're generally placed in most folders that have encrypted files.

Important: If your system is infected with ransomware, stop your backups. It's easy to restore a full-image backup, and fix your system in one step, if the backup isn't also encrypted. Stopping the backup software keeps your computer from backing up encrypted files. Revised for Cryptowall 2.0, Dec. 2014, recommendations subject to change..