Ransomware Handbook

Franklin Regional Retirement System
www.FRRSma.com

It used to be that all you had to do to defeat ransomware was to have a good backup – but not anymore! Now ransomware will post your stolen data to the internet, and will sell it to hackers if there's useful personal data. (Names and social security numbers are all someone needs to pull off identity theft (bank accounts, loans, maxed credit cards). What follows are our notes on the matter, including what do in the moment, and what to do to prevent. There are also snippets from good information sources for your further self-education. Dale

Ransomware

From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Ransomware

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Some forms of ransomware systematically encrypt files on the system's hard drive (**cryptoviral extortion,** a threat originally envisioned by Adam Young and Moti Yung) using a large key that may be technologically infeasible to breach without paying the ransom, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file.

While initially popular in Russia, the use of ransomware scams has grown internationally;[1][2][3] in June 2013, security software vendor McAfee released data showing that it had collected over 250,000 unique samples of ransomware in the first quarter of 2013—more than double the number it had obtained in the first quarter of 2012.[4]

Wide-ranging attacks involving encryption-based ransomware began to increase through trojans such as CryptoLocker, which had procured an estimated US$3 million before it was taken down by authorities,[5] and Cryptowall, which has procured an estimated $15 million as of June 2015.[6]

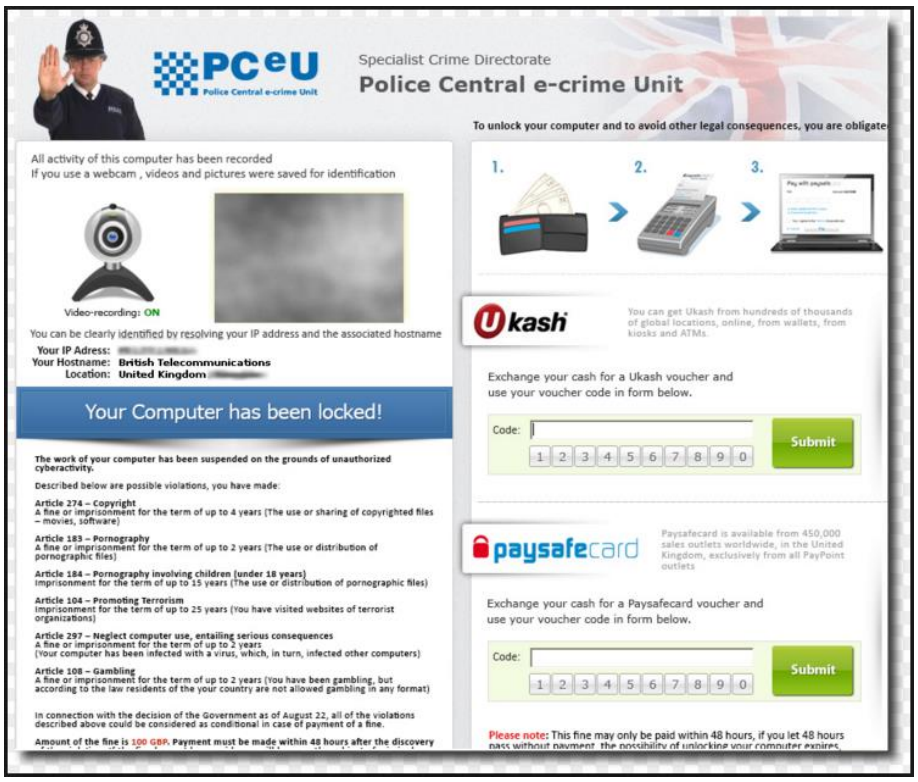
If you see the following screens, immediately unplug your computer and don't turn it on again until you get expert help to deal with the situation. They will start your computer with a clean install disk and then work to remove the virus(es).

Also, it wouldn't hurt to unplug the internet and network cables at your modem and router so you stop any outgoing

traffic, and so you don't cross infect your server or other computers on your network.

Do some advance prep and make your computer's power plug readily accessible. Maybe label the appropriate cables on your modem and router.


Your personal files are encrypted.
Your personal files are encrypted.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' to connect to the secret server and follow instructions.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
71:59:07
Next >>
can open it and use copy-paste for address and key.

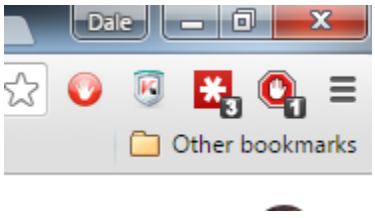

PCeU
Police Central e-crime Unit
Specialist Crime Directorate
Police Central e-crime Unit
All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification
Video-recording: ON
You can be clearly identified by resolving your IP address and the associated hostname
Your IP Adress:
Your Hostname: British Telecommunications
Location: United Kingdom
Your Computer has been locked!
The work of your computer has been suspended on the grounds of unauthorized cyberactivity.
Described below are possible violations, you have made:
Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)
Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)
Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)
Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)
Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years
(Your computer has been infected with a virus, which, in turn, infected other computers)
Article 108 – Gambling
A fine or imprisonment for the term of up to 2 years (You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)
In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.
Amount of the fine is 100 GBP. Payment must be made within 48 hours after the discovery
To unlock your computer and to avoid other legal consequences, you are obligate
1.
2.
3.
ukash
You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.
Exchange your cash for a Ukash voucher and use your voucher code in form below.
Code:
1 2 3 4 5 6 7 8 9 0
Submit
paysafecard
Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets
Exchange your cash for a Paysafecard voucher and use your voucher code in form below.
Code:
1 2 3 4 5 6 7 8 9 0
Submit
Please note: This fine may only be paid within 48 hours, if you let 48 hours

How to prevent infection:

Use ad blockers - Ads are being used to transmit viruses with or without you clicking on anything - we use an extension in Google Chrome (our browser).

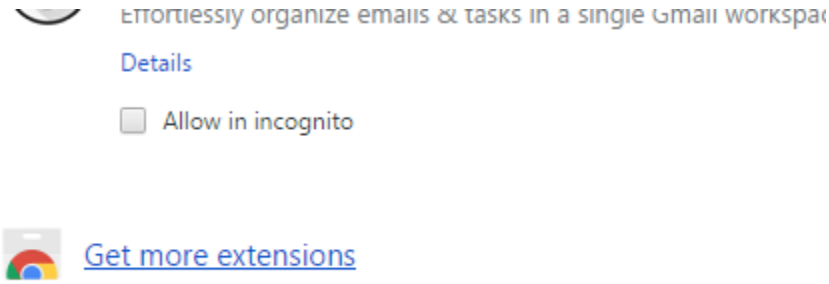
Here's how:

Click the settings symbol (affectionately referred to as the "hamburger" because it's a stack of 3 lines that look like a burger and bun:

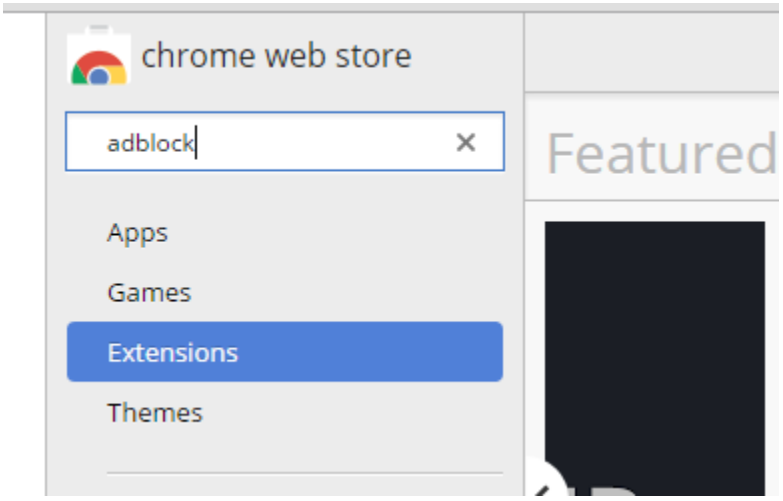


Click "More Tools"

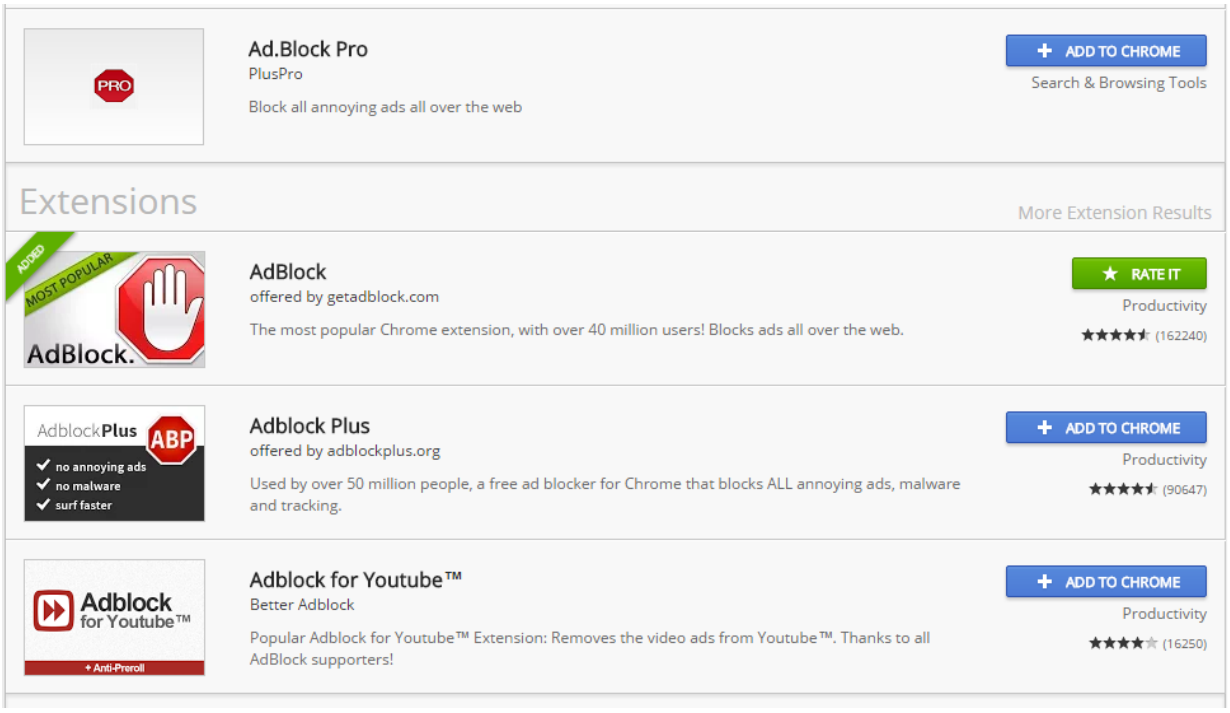
Click “Extensions”
Scroll to the bottom and click “Get More Extensions”



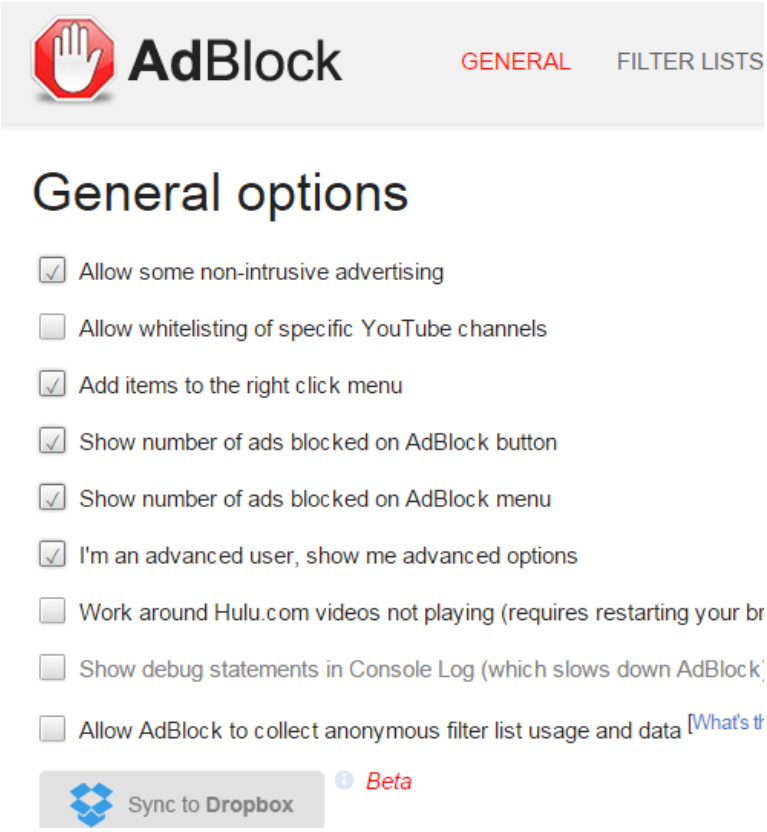
Search for “AdBlock”

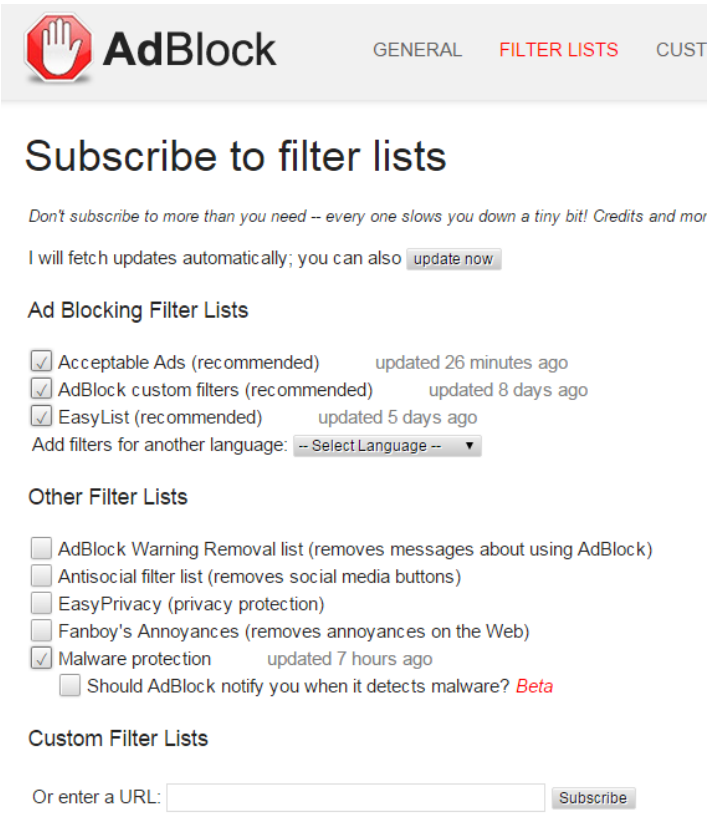


Don’t get ad.block Pro, or Adblock Plus (different companies).
Get AdBlock (by getadblock.com)



Play with the settings to suit yourself, but here's what ours look like (I think it's default settings are strong):





Do not accept or open attachments – have people use Sharefile. Use Sharefile to send and receive all attachments.

Use Gmail because it does a great job of detecting infected emails and warning you.

and Google Chrome as your browser because it more rapidly updated when new viruses are detected.

Read URLs before opening (know how to read them), and when sending links, send the raw URL so the recipient can read it.

Keep all software updated. Windows, Adobe Reader, Java, Flash (disable Reader, Flash, and Java use as much as you can).

Here are recent articles:
Chimera Ransomware Promises to Publish Encrypted Data Online

- See more at: https://threatpost.com/chimera-ransomware-promises-to-publish-encrypted-data-online/115293/#sthash.iMSmuNbU.dpuf

by Michael Mimoso November 6, 2015
Threat Post - The Kaspersky Lab Security News Service

Ransomware continues to elevate itself as perhaps the most worrisome crossover threat affecting consumers and businesses.
Already this week, we've had an update to the dangerous Cryptowall family of malware that includes new encryption features making that strain of ransomware harder to decrypt. This news came on the heels of a summer-long adoption of Cryptowall in particular by the virulent Angler exploit kit and other less prevalent malware toolkits.

Now comes another expansion of the ransomware threat from Chimera, malware that's primarily targeting companies in Germany, not only encrypting files and network drives, but also making veiled threats to publish encrypted data online if the extortion demands are not met.

The Anti-Botnet Advisory Centre, or Botfrei, published a note about the Chimera update this week. Chimera has been in circulation for two months, spreading via links in business-related emails.
"Several variants of sender addresses try to target specific employees within a company and they have one thing in common: within the email, a link points to a source at Dropbox, claiming that additional information has been stored there," Botfrei's report said. "The users get asked to download these files from there."

If the user clicks on the link, the Chimera malware downloads and begins encrypting locally stored data and seeks out network drives connected to the compromised computer. All the file extensions are then changed to .crypt.

Once the victim reboots, they're greeted with the customary ransom note demanding £630 (about $685 USD) to be paid in Bitcoin. The note also promises to publish the personal data and photographs stored on the computer online if the ransom isn't paid.

"At this point, there is no evidence whether personal data has been published on the internet or not – same as we haven't heard of a case where the cybercriminals have released the data after paying the 630 EUR in Bitcoins," the Botfrei report said.

This is a new twist for ransomware campaigns, most of which just encrypt data locally and promise to deliver the private encryption key unlocking the captive data. It's rarely stolen, or copied elsewhere.

Clearly, ransomware authors aren't sitting still. This week's Cryptowall update, dubbed Cryptowall 4.0 by researchers at Bleeping Computer, has gone a step beyond where its predecessor had by encrypting not only locally stored data but also file names. "I'm surprised more don't it; this makes it significantly harder to recover files except for paying the ransom," said independent researcher Nathan Scott, who analyzed the Cryptowall 4.0 sample with Bleeping Computer. "If you try to do a forensic data recovery, the files show up with these weird names and the user doesn't know what file is what. No one knows any structure in files any more.

"The only way to regain your data is a complete backup," Scott said. "If you don't backup, the only way to get the data back is to pay the ransom."

- See more at: https://threatpost.com/chimera-ransomware-promises-to-publish-encrypted-data-online/115293/#sthash.iMSmuNbU.dpuf

UPDATED CRYPTOWALL ENCRYPTS FILE NAMES, MOCKS VICTIMS

by Michael Mimoso November 5, 2015
Threat Post - The Kaspersky Lab Security News Service

Cryptowall has gotten a minor, but important facelift that might make it more difficult for researchers to tear apart and for victims to recover their encrypted data without paying a ransom.

Spotted two days ago, the latest update to the ransomware has begun not only encrypting data on victims' machines, but also file names, a first according to independent researcher Nathan Scott, who examined the code along with researchers from Bleeping Computer. "I'm surprised more don't it; this makes it significantly harder to recover files except for paying the ransom," Scott said. "If you try to do a forensic data recovery, the files show up with these weird names and the user doesn't know what file is what. No one knows any structure in files any more.

"The only way to regain your data is a complete backup," Scott said. "If you don't backup, the only way to get the data back is to pay the ransom."

The attackers behind Cryptowall have also updated the ransom note that victims are presented with. The note contains new mocking language, congratulating the victim for becoming part of the Cryptowall community, and the attackers have also assigned themselves a hashtag #CryptowallProject. The use of the hashtag, Scott speculates, is that victims may use it to commiserate on social media and if there is any kind of volume, it may lead them toward paying the ransom that much quicker.

Cryptowall is by far the most profitable of the ransomware families. A recent report from the Cyber Threat Alliance, a consortium of security vendors, concluded that Cryptowall 3.0 has caused an estimated $325 million in damages. It's unclear whether this most recent version of the crypto-ransomware is indeed Cryptowall 4.0, as Bleeping Computer has called it, or a point release as others have labeled it.
Regardless, this version of Cryptowall spreads via infected email attachments as its predecessors have. The attachments are disguised as a Word document (usually pretending to be an invoice or business document), but are instead a JavaScript executable that launches the malware.

This version also includes a nasty little feature where a compromised machine is less likely to have its restore points intact, making recovery that much harder. Restore points are system snapshots taken by Windows every time programs are installed or Windows is updated.

"Sometimes with ransomware, the user is lucky and the malware does not remove restore points or fails to and you can restore the system to a date before the ransomware infection and restore it as if it never happened," Scott said. "4.0 ensures this isn't an option."

Scott said that most victims who choose to pay the ransom in order to restore their data are sent the private key from the attackers, which isn't always the case with every ransomware operation.

“They run their model like a business and it’s very straightforward how it works. They know if they screw over too many people, they’re not getting paid,” Scott said. “They go out of their way make sure victims get files back.”

The FBI has also suggested that victims might want to consider just paying the ransom, especially for Cryptowall infections. The FBI’s estimates of Cryptowall damages were much lower than the CTA’s ($18 million).
“These guys have been around the longest,” Scott said, “and have learned from their mistakes.”

- See more at: https://threatpost.com/updated-cryptowall-encrypts-file-names-mocks-victims/115285/#sthash.NnZQsZko.dpuf

Here are some information resources:

https://business.kaspersky.com/practical-guide/4752/

http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/

11 things you can do to protect against ransomware, including Cryptolocker

BY LYSA MYERS POSTED 12 DEC 2013 - 06:42PM

Ransomware is malicious software that cyber criminals use to hold your computer or computer files for ransom, demanding payment from you to get them back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike. There is a variety of ransomware can get onto a person's machine, but as always, those techniques either boil down to social engineering tactics or using software vulnerabilities to silently install on a victim's machine.

Why is Cryptolocker so noteworthy?

One specific ransomware threat that has been in the news a lot lately is Cryptolocker (detected by ESET as Win32/Filecoder). The perpetrators of Cryptolocker have been emailing it to huge numbers of people, targeting particularly the US and UK. Like a notorious criminal, this malware has been associated with a variety of other bad actors – backdoor Trojans, downloaders, spammers, password-stealers, ad-clickers and the like. Cryptolocker may come on its own (often by email) or by way of a backdoor or downloader, brought along as an additional component.

You may wonder why the big fuss over this one particular ransomware family – in essence, it is because Cryptolocker's authors have been both nimble and persistent. There has been a concerted effort to pump out new variants, keeping up with changes in protection technology, and targeting different groups over time.

Since the beginning of September, the malware authors have sent waves of spam emails targeting different groups. Most of the targeted groups have been in the US and the UK, but there is no geographical limit on who can be affected, and plenty of people outside of either country have been hit. Initially emails were targeting home users, then small to medium businesses, and now they are going for enterprises as well.

The malware also spreads via RDP ports that have been left open to the Internet, as well as by email. Cryptolocker can also affect a user's files that are on drives that are "mapped", which is to say, they have been given a drive letter (e.g. D:, E:, F:). This could be an external hard-drive including USB thumb drives, or it could be a folder on the network or in the Cloud. If you have, say, your Dropbox folder mapped locally, it can encrypt those files as well.
At this point, tens of thousands of machines have been affected, though it is estimated that the criminals have sent millions of emails. Hopefully the remainder of recipients simply deleted the malicious emails without opening them, rather than them sitting unopened, waiting to unleash more pain.

Those people that have been affected have had a large number of their files encrypted. These files are primarily popular data formats, files you would open with a program (like Microsoft Office, Adobe programs, iTunes or other music players, or photo viewers). The malware authors use two types of encryption: The files themselves are protected with 256-bit AES encryption. The keys generated by this first encryption process are then protected with 2048-bit RSA encryption, and the malware author keeps the private key that would allow both the keys on the user's machine and the files they protect, to be decrypted. The decryption key cannot be brute-forced, or gathered from the affected computer's memory. The criminals are the only ones who ostensibly have the private key.

What can you do about it?

On the one hand, ransomware can be very scary – the encrypted files can essentially be considered damaged beyond repair. But if you have properly prepared your system, it is really nothing more than a nuisance. Here are a few tips that will help you keep ransomware from wrecking your day:

1. Back up your data
The **single biggest thing** that will defeat ransomware is **having a regularly updated backup**. If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy. Remember that Cryptolocker will also encrypt files on drives that are mapped. This includes any external drives such as a USB thumb drive, as well as any network or cloud file stores that you have assigned a drive letter. So, what you need is a regular backup regimen, to an external drive or backup service, one that is not assigned a drive letter or is disconnected when it is not doing backup.
The next three tips are meant to deal with how Cryptolocker has been behaving – this may not be the case forever, but these tips can help increase your overall security in small ways that help prevent against a number of different common malware techniques.

2. Show hidden file-extensions

One way that Cryptolocker frequently arrives is in a file that is named with the extension ".PDF.EXE", counting on Window's default behavior of hiding known file-extensions. If you re-enable the ability to see the full file-extension, it can be easier to spot suspicious files.

3. Filter EXEs in email

If your gateway mail scanner has the ability to filter files by extension, you may wish to deny mails sent with ".EXE" files, or to deny mails sent with files that have two file extensions, the last one being executable ("*.*.EXE" files, in filter-speak). If you do legitimately need to exchange executable files within your environment and are denying emails with ".EXE" files, you can do so with ZIP files (password-protected, of course) or via cloud services.

4. Disable files running from AppData/LocalAppData folders

You can create rules within Windows or with Intrusion Prevention Software, to disallow a particular, notable behavior used by Cryptolocker, which is to run its executable from the App Data or Local App Data folders. If (for some reason) you have legitimate software that you know is set to run not from the usual Program Files area but the App Data area, you will need to exclude it from this rule.

5. Use the Cryptolocker Prevention Kit

The Cryptolocker Prevention Kit is a tool created by Third Tier that automates the process of making a Group Policy to disable files running from the App Data and Local App Data folders, as well as disabling executable files from running from the Temp directory of various unzipping utilities. This tool is updated as new techniques are discovered for Cryptolocker, so you will want to check in periodically to make sure you have the latest version. If you need to create exemptions to these rules, they provide this document that explains that process.

6. Disable RDP

The Cryptolocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If you do not require the use of RDP, you can disable RDP to protect your machine from Filecoder and other RDP exploits. For instructions to do so, visit the appropriate Microsoft Knowledge Base article below:

- Windows XP RDP disable
- Windows 7 RDP disable
- Windows 8 RDP disable

7. Patch or Update your software

These next two tips are more general malware-related advice, which applies equally to Cryptolocker as to any malware threat. Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto your system. It can significantly decrease the potential for ransomware-pain if you make a practice of updating your software often. Some vendors release security updates on a regular basis (Microsoft and Adobe both use the second Tuesday of the month), but there are often "out-of-band" or unscheduled updates in case of emergency. Enable automatic updates if you can, or go directly to the software vendor's website, as malware authors like to disguise their creations as software update notifications too.

8. Use a reputable security suite

It is always a good idea to have both anti-malware software and a software firewall to help you identify threats or suspicious behavior. Malware authors frequently send out new variants, to try to avoid detection, so this is why it is important to have both layers of protection. And at this point, most malware relies on

remote instructions to carry out their misdeeds. If you run across a ransomware variant that is so new that it gets past anti-malware software, it may still be caught by a firewall when it attempts to connect with its Command and Control (C&C) server to receive instructions for encrypting your files.

If you find yourself in a position where you have already run a ransomware file without having performed any of the previous precautions, your options are quite a bit more limited. But all may not be lost. There are a few things you can do that *might* help mitigate the damage, particularly if the ransomware in question is Cryptolocker:

9. Disconnect from WiFi or unplug from the network immediately

If you run a file that you suspect may be ransomware, but you have not yet seen the characteristic ransomware screen, if you act *very* quickly you might be able to stop communication with the C&C server before it finish encrypting your files. If you disconnect yourself from the network *immediately*(have I stressed enough that this must be done *right away*?), you might mitigate the damage. It takes some time to encrypt all your files, so you may be able to stop it before it succeeds in garbling them all. This technique is definitely not foolproof, and you might not be sufficiently lucky or be able to move more quickly than the malware, but disconnecting from the network may be better than doing nothing.

10. Use System Restore to get back to a known-clean state

If you have System Restore enabled on your Windows machine, you might be able to take your system back to a known-clean state. But, again, you have to out-smart the malware. Newer versions of Cryptolocker can have the ability to delete “Shadow” files from System Restore, which means those files will not be there when you try to to replace your malware-damaged versions. Cryptolocker will start the deletion process whenever an executable file is run, so you will need to move very quickly as executables may be started as part of an automated process. That is to say, executable files may be run without you knowing, as a normal part of your Windows system’s operation.

11. Set the BIOS clock back

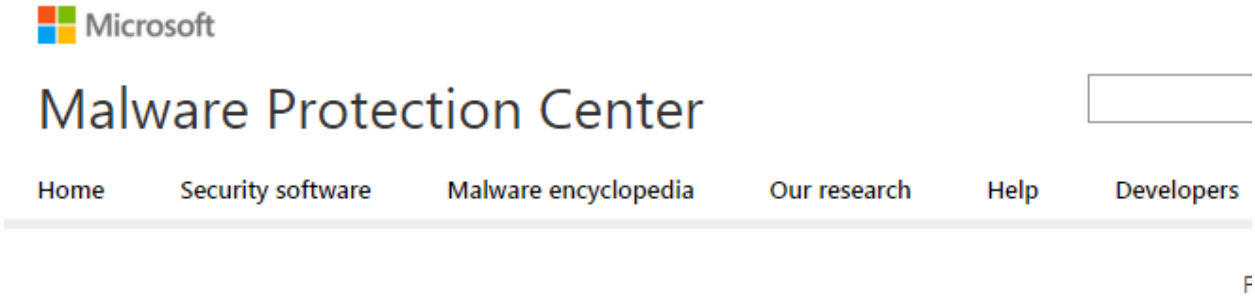
Cryptolocker has a payment timer that is generally set to 72 hours, after which time the price for your decryption key goes up significantly. (The price may vary as Bitcoin has a fairly volatile value. At the time of writing the initial price was .5 Bitcoin or $300, which then goes up to 4 Bitcoin) You can “beat the clock” somewhat, by setting the BIOS clock back to a time before the 72 hour window is up. I give this advice reluctantly, as all it can do is keep you from having to pay the higher price, and**we strongly advise that you do not pay the ransom**. Paying the criminals may get your data back, but there have been plenty of cases where the decryption key never arrived or where it failed to properly decrypt the files. Plus, it encourages criminal behavior! Ransoming *anything* is not a legitimate business practice, and the malware authors are under no obligation to do as promised – they can take your money and provide nothing in return, because there is no backlash if the criminals fail to deliver.

Further information

If you are an ESET customer and are concerned about ransomware protection or think you have been targeted by ransomware, call the customer care number for your country/region. They will have the latest details on how to prevent and remediate ransomware attacks.

In addition, there are several We Live Security articles that provide more information on this threat, see: Filecoder: Holding your data to ransom and Remote Desktop (RDP) Hacking 101: I can see your

desktop from here! For an audio explanation of, and historical perspective on, the topic of ransomware, listen to Aryeh Goretsky's recent podcast on the subject: Ransomware 101.
Finally, it should be noted that the recent rash of ransomware attacks has generated a lot of breathless news coverage, mainly because it is a departure from previous trends in financially motivated malware (which tended to be stealthy and thus not data-damaging). Ransomware can certainly be frightening, but there are many benign problems that can cause just as much destruction. That is why it has always been, and always will be, best practice to protect yourself against data loss with regular backups. That way, no matter what happens, you will be able to restart your digital life quickly. It is my hope that if anything good can come out of this ransomware trend, it is an understanding of an importance of performing regular, frequent backups to protect our valuable data.



https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

Ransomware

What is ransomware?

Ransomware stops you from using your PC. It holds your PC or files for ransom.

Some versions of ransomware are called "FBI Moneypak" or the "FBI virus" because they use the FBI's logos.

What does it look like and how does it work?

There are different types of ransomware. However, all of them will prevent you from using your PC normally, and they will all ask you to do something before you can use your PC.

They can:

- Prevent you from accessing Windows.
- Encrypt files so you can't use them.
- Stop certain apps from running (like your web browser).

They will demand that you do something to get access to your PC or files. We have seen them:

- Demand you pay money.

- Make you complete surveys.

Often the ransomware will claim you have done something illegal with your PC, and that you are being fined by a police force or government agency.

These claims are false. It is a scare tactic designed to make you pay the money without telling anyone who might be able to restore your PC.

There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.

- How did ransomware get on my PC?
  In most instances ransomware is automatically downloaded when you visit a malicious website or a website that's been hacked.

  For other ways malware, including ransomware, gets on your PC, see:

  - How malware gets on your PC
- How do I protect myself against ransomware?
  You should:

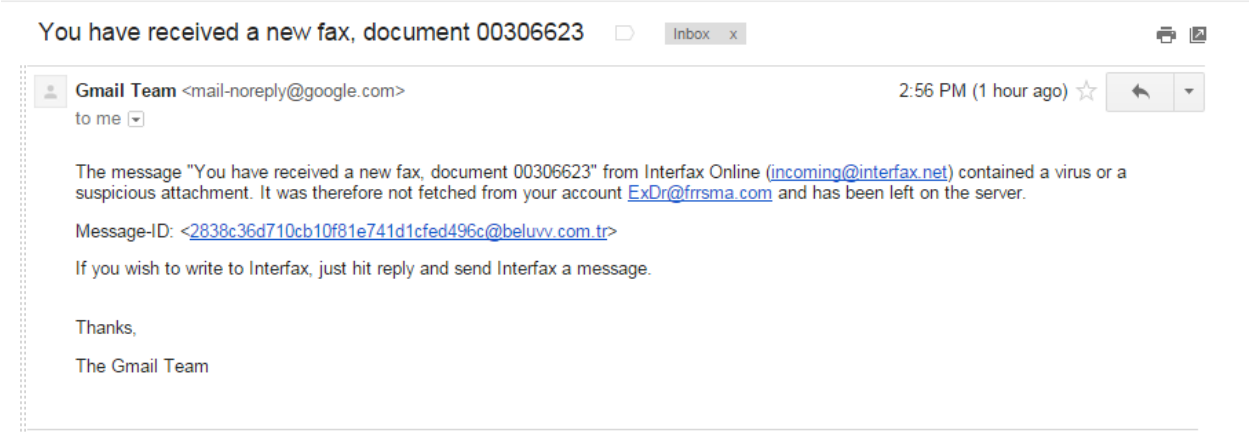
  - Install and use an up-to-date antivirus solution (such as Microsoft Security Essentials).
  - Make sure your software is up-to-date.
  - Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
  - Ensure you have smart screen (in Internet Explorer) turned on.
  - Have a pop-up blocker running in your web browser.
  - Regularly backup your important files.

  You can backup your files with a cloud storage service that keeps a history or archive of your files, such as OneDrive which is now fully integrated into Windows 10 and Windows 8.1, and Microsoft Office.
  After you've removed the ransomware infection from your computer, you can restore previous, unencrypted versions of your Office files using "version history".

  See the question "How do I get my files back?" above for more help on how to use this feature in OneDrive.

  For more tips on preventing malware infections, including ransomware infections, see:

  - Help prevent malware infection on your PC.


You have received a new fax, document 00306623 Inbox x

Gmail Team <mail-noreply@google.com> 2:56 PM (1 hour ago)
to me

The message "You have received a new fax, document 00306623" from Interfax Online (incoming@interfax.net) contained a virus or a suspicious attachment. It was therefore not fetched from your account ExDr@frrsma.com and has been left on the server.

Message-ID: <2838c36d710cb10f81e741d1cfed496c@beluvv.com.tr>

If you wish to write to Interfax, just hit reply and send Interfax a message.

Thanks,

The Gmail Team