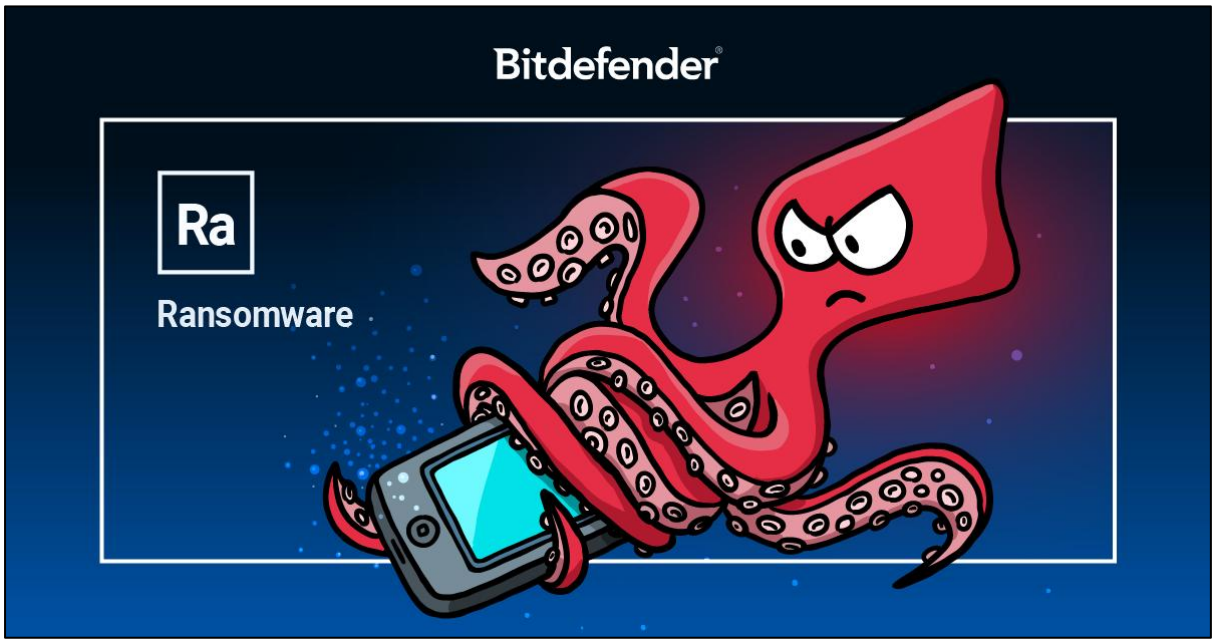
What is Ransomware? Prevention & Data Recovery

While there may be more than 1 billion malicious programs (malware) prowling the Internet for a chance to infect victims, one class of malware has been inflicting financial losses and security concerns for years: Ransomware. Its sole purpose is to block access to computer systems or files until the victim pays a ransom. These ransom demands fluctuate wildly, from the equivalent of a couple of hundred dollars to several hundred thousand.

What is Ransomware?

Ransomware is a category of malicious software designed to block access to a computer system until a sum of money is paid. Payment is usually demanded in cryptocurrencies such as Bitcoin or Monero. Victims are told to purchase these digital assets and then transfer them to the attackers. Ransomware has evolved over the past decade to target more victims, generate huge profits for cybercriminals, and make it nearly impossible to recover data unless the victim pays the ransom note or recovers it from backups.



While encryption is considered a powerful tool for ensuring online privacy, by allowing everyone to communicate without fearing that others are eavesdropping, ransomware developers have used it to make sure affected files cannot be used. Some encryption mechanisms make it impossible to recover data unless attackers agree to send victims the decryption key, unlocking access to the affected system after the ransom is paid. Imagine someone breaking into your home, finding your jewellery, locking it in an impenetrable chest in the middle of your home, then leaving with the key after placing a ransom note. If you contact the burglar and pay the ransom note, he will give you the key to unlock the chest and get to your jewellery. Otherwise, good luck breaking the chest. You know all your valuables are there, but you simply can't use them. Ransomware acts in a similar way, except that it goes after your files and data.

Three different types of ransomwares are out there so far:

1. **Screen lockers**

The “mildest” of all ransomwares are screen-lockers: they only prevent the user from accessing their device by blocking access to the desktop or home screen in the case of smartphones. While annoying, screen lockers can be bypassed without paying the attacker, provided you have enough technical experience.

2. **Crypto ransomware**

While early less malignant ransomware strains proved ineffective at making money as they focused on preventing users from accessing their devices by using screen lockers (no data was encrypted), later versions started using encryption known as crypto-ransomware. Crypto-ransomware is extremely effective as it encrypts specific locally stored information and sometimes cloud backups too and offers to decrypt it in exchange for a fee ranging from $300 to $900. Because crypto-ransomware uses the same technology that protects our online conversations, banking transactions and military communication, encrypted files can’t be retrieved without paying the ransom. Crypto-ransomware families are responsible for extorting more than one billion dollars a year from victims. Some crypto-ransomware families such as GandCrab have even generated the equivalent of more than 2 billion dollars in paid ransom in less than two years of activity.

Other ransomware families have started adopting extortion as another intimidation tactic to scare victims into paying. For instance, before attackers encrypt sensitive data, they steal it from victims and threaten to expose it online as part of a public shaming campaign if the ransom demand is not met.

3. **Disk encryptors**

Finally, the most disruptive forms of ransomware are known as disk-encryptors. Unlike file encryptors, disk encryptors prevent users from booting their entire operating system, as the ransomware holds the entire disk drive “hostage”.

How does Ransomware spread?

Emails are one of the most-used mechanisms for spreading ransomware. Either tricking victims into clicking on links and downloading ransomware-infected files, or attaching tainted documents that pose as CVs, invoices, and other types of files, spam emails account for many ransomware infections. If the user opens the message and clicks the attachment, the encryption process starts. When all the information is encrypted, the user sees a warning message directly on the desktop, along with instructions on how to pay the ransom and get the decryption key.

Another technique that attackers use is to buy advertising on high-traffic websites and then leverage them to exploit unpatched vulnerabilities in browsers or plugins. When such a vulnerability is exploited, the browser or plugin crashes and the ransomware payload is automatically installed. Many users have grown reluctant to open

attachments or click on email links, so this method removes any user interaction or social engineering component by relying on unpatched vulnerabilities.

Finally, cybercriminals sneak ransomware into illegal, pirated content that is available for download on torrent or “warez” websites. Unsuspecting victims download ransomware disguised as cracks, key generators, and other types of software onto their systems, execute them, and consequently install ransomware.

How to protect your PC against Ransomware Attacks

Ransomware is a highly lucrative business for cybercriminals, and they are constantly investing in new ways to infect victims and make it difficult for security solutions to fend off. The best way to protect against ransomware attacks is to not get infected in the first place. Ransomware infection can be limited and sometimes prevented with a few best practices:

1. **Use an updated security solution**

Use an anti-malware solution with anti-exploit, anti-malware, and anti-spam modules that is constantly updated and able to perform active scanning. Make sure you don’t override the optimal settings of your security solution and that you update it daily.

2. **Schedule file backups**

Performing regular backups of your important files and documents in the cloud or locally is also recommended. Keeping those backups on storage devices not directly connected to your computer or discoverable on your network is also required, as ransomware infections usually seek out connected storage devices and encrypt those as well. By doing this, even if you get infected and lose your locally stored files, you can always recover from a backup without paying the ransom note.

3. **Keep Windows up to date**

Keep your Windows operating system and your vulnerable software – especially the browser and the browser plug-ins – up to date with the latest security patches. Exploit kits use vulnerabilities in these components to automatically install malware.

4. **Keep UAC enabled**

UAC (User Account Control) notifies you when changes are going to be made to your computer that require administrator-level permission. Keep UAC enabled to decrease or block the impact of malware.

5. **Follow safe internet practices**

Follow safe Internet practices by not visiting questionable websites, not clicking links or opening attachments in emails from uncertain sources. Avoid downloading apps from unfamiliar sites — only install software from trusted sources. Do not provide personally identifiable information on public chat rooms or forums.

6. **Enable adblockers**

Enable ad-blocking and privacy extensions (such as Adblock Plus) to reduce malicious ads. Increase your online protection by adjusting your web browser security settings. Alternatively, you might want to consider a browser extension that blocks JavaScript (such as NoScript).

7. **Use anti-spam filters**

Implement and use an anti-spam filter to reduce the number of infected spam emails that reach your Inbox.

8. **Disable Flash**

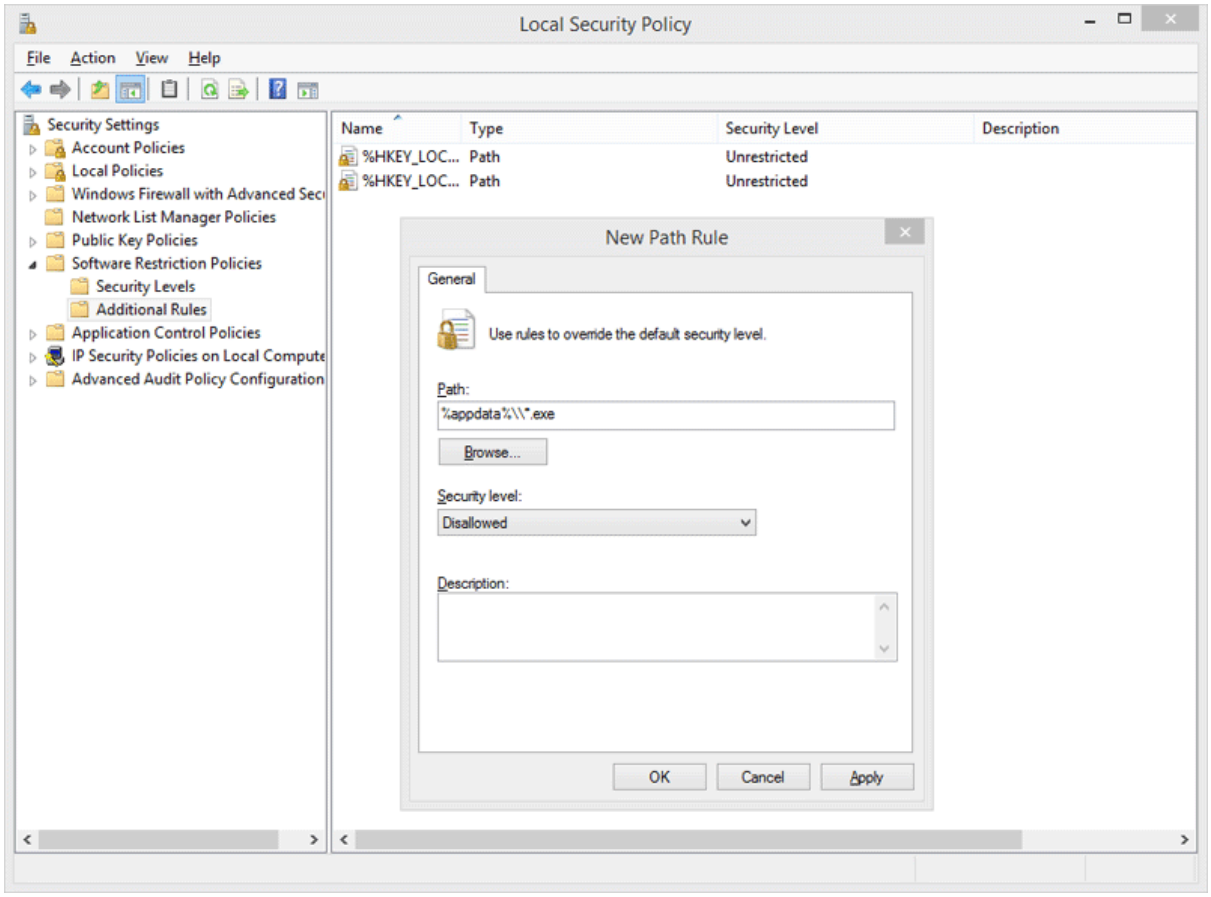
When possible, virtualize or completely disable Adobe Flash, as it has been repeatedly used as an infection vector.

9. **Enable software restriction policies**

If your computer runs a Windows Professional or Windows Server edition or if you are a decision maker in the company's IT team, enable software restriction policies. System administrators can enforce group policy objects into the registry to block executables from specific locations.

This can only be achieved when running a Windows Professional or Windows Server edition. The 'Software Restriction Policies' option can be found in the 'Local Security Policy' editor. After clicking the 'New Software Restriction Policies' button under 'Additional Rules', the following Path Rules should be used with the 'Disallowed' Security level:

"%username%\\Appdata\\Roaming*.exe"
"%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\\.*exe"
C:*.exe
"%temp%*.exe"
"%userprofile%\\Start Menu\\Programs\\Startup*.exe"
"%userprofile%*.exe"
"%username%\\Appdata*.exe"
"%username%\\Appdata\\Local*.exe"
"%username%\\Application Data*.exe"
"%username%\\Application Data\\Microsoft*.exe"
"%username%\\Local Settings\\Application Data*.exe"



What to do if Ransomware encrypts your files

Usually, in the case of encrypting ransomware, local files are encrypted using a randomly generated key pair that's associated with the infected computer. While the public key is copied on the infected computer, the private key can only be obtained by paying for it within an allocated amount of time. If the payment is not delivered, the private key is threatened to be deleted, leaving no possible decrypting method for recovering the locked files.

Authorities recommend not giving in to ransom demands. Paying a ransom does not guarantee you will get your files back and only serves to financially fuel the development of new and more sophisticated ransomware families, helps finance other cybercriminal activities, and ultimately legitimizes the ransomware business by making it profitable for hackers. Defeating ransomware attacks is difficult, but not impossible. Law enforcement and security companies have been working together for years to help victims recover their files.

Tips to recover ransomware encrypted data:

1. If Bitdefender's Ransomware Remediation module is enabled at the time of a ransomware attack, your files will be automatically restored.
2. It is also possible to recover encrypted ransomware files by restoring original files from an external or cloud backup.
3. Initiatives such as the nomoreransom.org website can help ransomware victims recover their data, in cases where law enforcement or security vendors have found a way to decrypt files for specific ransomware families.
4. FBI has the following recommendations for victims of ransomware:
    - Submit a tip online or contact your local FBI field office to request assistance.
    - File a report with the FBI's Internet Crime Complaint Center (IC3).

Remember! It's important to frequently backup your data, keep an eye out for unsolicited emails, constantly update all your software and operating systems, install a security solution that features multiple layers of protection against ransomware, and not give in to extortion.