Operation

The concept of file-encrypting ransomware was invented and implemented by Young and [Yung](https://en.wikipedia.org/wiki/Moti_Yung) at [Columbia University](https://en.wikipedia.org/wiki/Columbia_University) and was presented at the 1996 IEEE Security & Privacy conference. It is called *cryptoviral extortion* and it was inspired by the fictional facehugger in the movie [*Alien*](https://en.wikipedia.org/wiki/Alien_(film)).[[13]](https://en.wikipedia.org/wiki/Ransomware#cite_note-yycacm-13) Cryptoviral extortion is the following three-round protocol carried out between the attacker and the victim.[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1)

1. [attacker**→**victim] The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.
2. [victim**→**attacker] To carry out the cryptoviral extortion attack, the malware generates a random symmetric key and encrypts the victim's data with it. It uses the public key in the malware to encrypt the symmetric key. This is known as [hybrid encryption](https://en.wikipedia.org/wiki/Hybrid_encryption) and it results in a small asymmetric ciphertext as well as the symmetric ciphertext of the victim's data. It zeroizes the symmetric key and the original plaintext data to prevent recovery. It puts up a message to the user that includes the asymmetric ciphertext and how to pay the ransom. The victim sends the asymmetric ciphertext and e-money to the attacker.
3. [attacker**→**victim] The attacker receives the payment, deciphers the asymmetric ciphertext with the attacker's private key, and sends the symmetric key to the victim. The victim deciphers the encrypted data with the needed symmetric key thereby completing the cryptovirology attack.

The [symmetric key](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) is randomly generated and will not assist other victims. At no point is the attacker's private key exposed to victims and the victim need only send a very small ciphertext (the encrypted symmetric-cipher key) to the attacker.

Ransomware attacks are typically carried out using a [Trojan](https://en.wikipedia.org/wiki/Trojan_horse_(computing)), entering a system through, for example, a malicious attachment, embedded link in a [Phishing](https://en.wikipedia.org/wiki/Phishing) email, or a vulnerability in a network service. The program then runs a [payload](https://en.wikipedia.org/wiki/Payload_(computing)), which locks the system in some fashion, or claims to lock the system but does not (e.g., a [scareware](https://en.wikipedia.org/wiki/Scareware) program). Payloads may display a fake warning purportedly by an entity such as a [law enforcement agency](https://en.wikipedia.org/wiki/Law_enforcement_agency), falsely claiming that the system has been used for illegal activities, contains content such as [pornography](https://en.wikipedia.org/wiki/Pornography) and ["pirated" media](https://en.wikipedia.org/wiki/Piracy_(media)).[[14]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cw-ranactivate-14)[[15]](https://en.wikipedia.org/wiki/Ransomware#cite_note-hsfi-ransom-15)[[16]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-russia-16)

Some payloads consist simply of an application designed to lock or restrict the system until payment is made, typically by setting the [Windows Shell](https://en.wikipedia.org/wiki/Windows_Shell) to itself,[[17]](https://en.wikipedia.org/wiki/Ransomware#cite_note-kaspersky-german-17) or even modifying the [master boot record](https://en.wikipedia.org/wiki/Master_boot_record) and/or [partition table](https://en.wikipedia.org/wiki/Partition_table) to prevent the operating to the system from booting until it is repaired.[[18]](https://en.wikipedia.org/wiki/Ransomware#cite_note-kaspersky-mbr-18) The most sophisticated payloads [encrypt](https://en.wikipedia.org/wiki/Cryptography) files, with many using [strong encryption](https://en.wikipedia.org/wiki/Strong_encryption) to [encrypt](https://en.wikipedia.org/wiki/Hybrid_cryptosystem) the victim's files in such a way that only the malware author has the needed decryption key.[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1)[[19]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-2-19)[[20]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-3-20)

Payment is virtually always the goal, and the victim is [coerced](https://en.wikipedia.org/wiki/Coercion) into paying for the ransomware to be removed either by supplying a program that can decrypt the files, or by sending an unlock code that undoes the payload's changes. While the attacker may simply take the money without returning the victim's files, it is in the attacker's best interest to perform the decryption as agreed, since victims will stop sending payments if it becomes known that they serve no purpose. A key element in making ransomware work for the attacker is a convenient payment system that is hard to trace. A range of such payment methods have been used, including [wire transfers](https://en.wikipedia.org/wiki/Wire_transfer), [premium-rate text messages](https://en.wikipedia.org/wiki/Premium_SMS),[[21]](https://en.wikipedia.org/wiki/Ransomware#cite_note-zdnet-21) pre-paid [voucher](https://en.wikipedia.org/wiki/Voucher) services such as [paysafecard](https://en.wikipedia.org/wiki/Paysafecard),[[6]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-russia-6)[[22]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cw-pirated-22)[[23]](https://en.wikipedia.org/wiki/Ransomware#cite_note-arstechnica-23) and the [digital currency bitcoin](https://en.wikipedia.org/wiki/Bitcoin).[[24]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-cryptolocker-24)[[25]](https://en.wikipedia.org/wiki/Ransomware#cite_note-computerworld-cryptodefense-25)[[26]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tm-cryptodefense-26)

History

**Encrypting ransomware**

The first known malware extortion attack, the ["AIDS Trojan"](https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)) written by [Joseph Popp](https://en.wikipedia.org/wiki/Joseph_Popp) in 1989, had a design failure so severe it was not necessary to pay the extortionist at all. Its payload hid the files on the hard drive and encrypted only their [names](https://en.wikipedia.org/wiki/Filename), and displayed a message claiming that the user's license to use a certain piece of software had expired. The user was asked to pay [US$](https://en.wikipedia.org/wiki/United_States_dollar)189 to "PC Cyborg Corporation" in order to obtain a repair tool even though the decryption key could be extracted from the code of the Trojan. The Trojan was also known as "PC Cyborg". Popp was declared [mentally unfit](https://en.wikipedia.org/wiki/Insanity_defense) to stand trial for his actions, but he promised to donate the profits from the malware to fund [AIDS](https://en.wikipedia.org/wiki/HIV/AIDS) research.[[27]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tr-extortion-27)

The idea of abusing anonymous cash systems to safely collect ransom from human [kidnapping](https://en.wikipedia.org/wiki/Kidnapping) was introduced in 1992 by Sebastiaan von Solms and [David Naccache](https://en.wikipedia.org/wiki/David_Naccache).[[28]](https://en.wikipedia.org/wiki/Ransomware#cite_note-28) This electronic money collection method was also proposed for cryptoviral extortion attacks.[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1) In the von Solms-Naccache scenario a newspaper publication was used (since bitcoin ledgers did not exist at the time the paper was written).

The notion of using public key cryptography for data kidnapping attacks was introduced in 1996 by Adam L. Young and [Moti Yung](https://en.wikipedia.org/wiki/Moti_Yung). Young and Yung critiqued the failed AIDS Information Trojan that relied on [symmetric cryptography](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) alone, the fatal flaw being that the decryption key could be extracted from the Trojan, and implemented an experimental proof-of-concept cryptovirus on a [Macintosh SE/30](https://en.wikipedia.org/wiki/Macintosh_SE/30) that used [RSA](https://en.wikipedia.org/wiki/RSA_(algorithm)) and the [Tiny Encryption Algorithm](https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm) (TEA) to [hybrid encrypt](https://en.wikipedia.org/wiki/Hybrid_encryption) the victim's data. Since public key crypto is used, the cryptovirus only contains the *encryption* key. The attacker keeps the corresponding *private* decryption key private. Young and Yung's original experimental cryptovirus had the victim send the asymmetric ciphertext to the attacker who deciphers it and returns the symmetric decryption key it contains to the victim for a fee. Long before [electronic money](https://en.wikipedia.org/wiki/Electronic_money) existed Young and Yung proposed that electronic money could be extorted through encryption as well, stating that "the virus writer can effectively hold all of the money ransom until half of it is given to him. Even if the e-money was previously encrypted by the user, it is of no use to the user if it gets encrypted by a cryptovirus".[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1) They referred to these attacks as being "[cryptoviral](https://en.wikipedia.org/wiki/Cryptovirology) extortion", an overt attack that is part of a larger class of attacks in a field called [cryptovirology](https://en.wikipedia.org/wiki/Cryptovirology), which encompasses both overt and covert attacks.[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1) The cryptoviral extortion protocol was inspired by the parasitic relationship between H. R. Giger's facehugger and its host in the movie [*Alien*](https://en.wikipedia.org/wiki/Alien_(film)).[[1]](https://en.wikipedia.org/wiki/Ransomware#cite_note-young-1)[[13]](https://en.wikipedia.org/wiki/Ransomware#cite_note-yycacm-13)

Examples of extortionate ransomware became prominent in May 2005.[[29]](https://en.wikipedia.org/wiki/Ransomware#cite_note-29) By mid-2006, Trojans such as [Gpcode](https://en.wikipedia.org/wiki/Gpcode), TROJ.RANSOM.A, [Archiveus](https://en.wikipedia.org/wiki/Archiveus), Krotten, Cryzip, and MayArchive began utilizing more sophisticated RSA encryption schemes, with ever-increasing key-sizes. Gpcode.AG, which was detected in June 2006, was encrypted with a 660-bit RSA public key.[[30]](https://en.wikipedia.org/wiki/Ransomware#cite_note-30) In June 2008, a variant known as Gpcode.AK was detected. Using a 1024-bit RSA key, it was believed large enough to be computationally infeasible to break without a concerted [distributed](https://en.wikipedia.org/wiki/Distributed_computing) effort.[[31]](https://en.wikipedia.org/wiki/Ransomware#cite_note-zdnet-2-31)[[32]](https://en.wikipedia.org/wiki/Ransomware#cite_note-securityfocus-32)[[33]](https://en.wikipedia.org/wiki/Ransomware#cite_note-washingtonpost-33)[[34]](https://en.wikipedia.org/wiki/Ransomware#cite_note-kapersky-34)

Encrypting ransomware returned to prominence in late 2013 with the propagation of [CryptoLocker](https://en.wikipedia.org/wiki/CryptoLocker)—using the [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) [digital currency](https://en.wikipedia.org/wiki/Digital_currency) platform to collect ransom money. In December 2013, [ZDNet](https://en.wikipedia.org/wiki/ZDNet) estimated based on Bitcoin transaction information that between 15 October and 18 December, the operators of CryptoLocker had procured about US$27 million from infected users.[[35]](https://en.wikipedia.org/wiki/Ransomware#cite_note-zdnet-bitcoinprice-35) The CryptoLocker technique was [widely copied](https://en.wikipedia.org/wiki/Copycat_crime) in the months following, including CryptoLocker 2.0 (thought not to be related to CryptoLocker), CryptoDefense (which initially contained a major design flaw that stored the private key on the infected system in a [user-retrievable location](https://en.wikipedia.org/wiki/Application_Data), due to its use of Windows' built-in encryption APIs),[[25]](https://en.wikipedia.org/wiki/Ransomware#cite_note-computerworld-cryptodefense-25)[[36]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcworld-torrentlocker-36)[[37]](https://en.wikipedia.org/wiki/Ransomware#cite_note-eset-cl2-37)[[38]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tm-newcl-38) and the August 2014 discovery of a Trojan specifically targeting [network-attached storage](https://en.wikipedia.org/wiki/Network-attached_storage) devices produced by [Synology](https://en.wikipedia.org/wiki/Synology).[[39]](https://en.wikipedia.org/wiki/Ransomware#cite_note-extech-synologycrypto-39) In January 2015, it was reported that ransomware-styled attacks have occurred against individual websites via hacking, and through ransomware designed to target [Linux](https://en.wikipedia.org/wiki/Linux)-based [web servers](https://en.wikipedia.org/wiki/Web_server).[[40]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcworld-linuxrw-40)[[41]](https://en.wikipedia.org/wiki/Ransomware#cite_note-sw-ransomweb-41)[[42]](https://en.wikipedia.org/wiki/Ransomware#cite_note-guardian-ransomweb-42)

The Microsoft Malware Protection Center identified a trend away from WSF files in favour of LNK files and PowerShell scripting.[[43]](https://en.wikipedia.org/wiki/Ransomware#cite_note-43) These LNK shortcut files install Locky ransomware by automating infection operations rather than relying on traditional user downloads of WSF files—all of which is made possible by the universal [PowerShell Windows application](https://en.wikipedia.org/wiki/PowerShell). Unfortunately, cybercriminals have been able to leverage PowerShell for their attacks for years. In a recent report, the application was found to be involved in nearly 40% of endpoint security incidents.[[44]](https://en.wikipedia.org/wiki/Ransomware#cite_note-44) While attackers have been finding weaknesses in the Windows operating system for years, it's clear that there's something problematic with PowerShell scripting.[[45]](https://en.wikipedia.org/wiki/Ransomware#cite_note-45)

Some ransomware strains have used [proxies](https://en.wikipedia.org/wiki/Proxy_server) tied to [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)) [hidden services](https://en.wikipedia.org/wiki/Hidden_service) to connect to their command and control servers, increasing the difficulty of tracing the exact location of the criminals.[[46]](https://en.wikipedia.org/wiki/Ransomware#cite_note-guardian-tor-46)[[47]](https://en.wikipedia.org/wiki/Ransomware#cite_note-sophos-ctblocker-47) Furthermore, [dark web](https://en.wikipedia.org/wiki/Dark_web) vendors have increasingly started to offer the technology [as a service](https://en.wikipedia.org/wiki/Software_as_a_service).[[47]](https://en.wikipedia.org/wiki/Ransomware#cite_note-sophos-ctblocker-47)[[48]](https://en.wikipedia.org/wiki/Ransomware#cite_note-48)[[49]](https://en.wikipedia.org/wiki/Ransomware#cite_note-49)

Symantec has classified ransomware to be the most dangerous cyber threat.[[50]](https://en.wikipedia.org/wiki/Ransomware#cite_note-50)

**Non-encrypting ransomware**

In August 2010, Russian authorities arrested nine individuals connected to a ransomware Trojan known as WinLock. Unlike the previous Gpcode Trojan, WinLock did not use encryption. Instead, WinLock trivially restricted access to the system by displaying pornographic images and asked users to send a [premium-rate SMS](https://en.wikipedia.org/wiki/Short_Message_Service#Premium-rated_short_messages) (costing around US$10) to receive a code that could be used to unlock their machines. The scam hit numerous users across Russia and neighbouring countries—reportedly earning the group over US$16 million.[[16]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-russia-16)[[51]](https://en.wikipedia.org/wiki/Ransomware#cite_note-51)

In 2011, a ransomware Trojan surfaced that imitated the [Windows Product Activation](https://en.wikipedia.org/wiki/Windows_Product_Activation) notice, and informed users that a system's Windows installation had to be re-activated due to "[being a] victim of fraud". An online activation option was offered (like the actual Windows activation process), but was unavailable, requiring the user to call one of six [international numbers](https://en.wikipedia.org/wiki/International_call) to input a 6-digit code. While the malware claimed that this call would be free, it was routed through a rogue operator in a country with high international phone rates, who placed the call on hold, causing the user to incur large international [long distance](https://en.wikipedia.org/wiki/Long_distance_calling) charges.[[14]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cw-ranactivate-14)

In February 2013, a ransomware Trojan based on the Stamp.EK [exploit kit](https://en.wikipedia.org/wiki/Exploit_kit) surfaced; the malware was distributed via sites hosted on the project hosting services [SourceForge](https://en.wikipedia.org/wiki/SourceForge) and [GitHub](https://en.wikipedia.org/wiki/GitHub) that claimed to offer "fake nude pics" of celebrities.[[52]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tnw-fakenudepics-52) In July 2013, an [OS X](https://en.wikipedia.org/wiki/OS_X)-specific ransomware Trojan surfaced, which displays a web page that accuses the user of downloading pornography. Unlike its Windows-based counterparts, it does not block the entire computer, but simply [exploits the behaviour of the web browser itself](https://en.wikipedia.org/wiki/Clickjacking) to frustrate attempts to close the page through normal means.[[53]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tnw-osxransom-53)

In July 2013, a 21-year-old man from Virginia, whose computer coincidentally did contain pornographic photographs of underage girls with whom he had conducted sexualized communications, turned himself in to police after receiving and being deceived by [FBI MoneyPak Ransomware](https://en.wikipedia.org/wiki/FBI_MoneyPak_Ransomware) accusing him of possessing child pornography. An investigation discovered the incriminating files, and the man was charged with [child sexual abuse](https://en.wikipedia.org/wiki/Child_sexual_abuse) and possession of child pornography.[[54]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-cpvirginia-54)

**Leakware (also called Doxware)**

The converse of ransomware is a [cryptovirology](https://en.wikipedia.org/wiki/Cryptovirology) attack invented by Adam L. Young that threatens to publish stolen information from the victim's computer system rather than deny the victim access to it.[[55]](https://en.wikipedia.org/wiki/Ransomware#cite_note-iaw2003-55) In a leakware attack, malware exfiltrates sensitive host data either to the attacker or alternatively, to remote instances of the malware, and the attacker threatens to publish the victim's data unless a ransom is paid. The attack was presented at [West Point](https://en.wikipedia.org/wiki/West_Point) in 2003 and was summarized in the book *Malicious Cryptography* as follows, "The attack differs from the extortion attack in the following way. In the extortion attack, the victim is denied access to its own valuable information and has to pay to get it back, where in the attack that is presented here the victim retains access to the information but its disclosure is at the discretion of the computer virus".[[56]](https://en.wikipedia.org/wiki/Ransomware#cite_note-maliciouscrypto-56) The attack is rooted in game theory and was originally dubbed "non-zero sum games and survivable malware". The attack can yield monetary gain in cases where the malware acquires access to information that may damage the victim user or organization, e.g., the reputational damage that could result from publishing proof that the attack itself was a success.

**Mobile ransomware**

With the increased popularity of ransomware on PC platforms, ransomware targeting [mobile operating systems](https://en.wikipedia.org/wiki/Mobile_operating_system) has also proliferated. Typically, mobile ransomware payloads are blockers, as there is little incentive to encrypt data since it can be easily restored via online synchronization.[[57]](https://en.wikipedia.org/wiki/Ransomware#cite_note-kapersky-androidrw-57) Mobile ransomware typically targets the [Android](https://en.wikipedia.org/wiki/Android_(operating_system)) platform, as it allows applications to be installed from third-party sources.[[57]](https://en.wikipedia.org/wiki/Ransomware#cite_note-kapersky-androidrw-57)[[58]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-androidransomware-58) The payload is typically distributed as an [APK file](https://en.wikipedia.org/wiki/APK_file) installed by an unsuspecting user; it may attempt to display a blocking message over top of all other applications,[[58]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-androidransomware-58) while another used a form of [clickjacking](https://en.wikipedia.org/wiki/Clickjacking) to cause the user to give it "device administrator" privileges to achieve deeper access to the system.[[59]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-ransomwaredeviceadmin-59)

Different tactics have been used on [iOS](https://en.wikipedia.org/wiki/IOS) devices, such as exploiting [iCloud](https://en.wikipedia.org/wiki/ICloud) accounts and using the [Find My iPhone](https://en.wikipedia.org/wiki/Find_My_iPhone) system to lock access to the device.[[60]](https://en.wikipedia.org/wiki/Ransomware#cite_note-fortune-findmyiphonerw-60) On [iOS 10.3](https://en.wikipedia.org/wiki/IOS_10.3), Apple patched a bug in the handling of JavaScript pop-up windows in [Safari](https://en.wikipedia.org/wiki/Safari_(web_browser)) that had been exploited by ransomware websites.[[61]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-iosransom-61) It recently has been shown that ransomware may also target ARM architectures like those that can be found in various Internet-of-Things (IoT) devices, such as Industrial IoT edge devices.[[62]](https://en.wikipedia.org/wiki/Ransomware#cite_note-62)

In August 2019 researchers demonstrated it's possible to infect [DSLR cameras](https://en.wikipedia.org/wiki/DSLR_camera) with ransomware.[[63]](https://en.wikipedia.org/wiki/Ransomware#cite_note-63) Digital cameras often use [Picture Transfer Protocol](https://en.wikipedia.org/wiki/Picture_Transfer_Protocol) (PTP - standard protocol used to transfer files.) Researchers found that it was possible to exploit vulnerabilities in the protocol to infect target camera(s) with ransomware (or execute any arbitrary code). This attack was presented at the [Defcon](https://en.wikipedia.org/wiki/DEF_CON) security conference in Las Vegas as a proof of concept attack (not as actual armed malware).

Notable examples

**Reveton**

[](https://en.wikipedia.org/wiki/File:Metropolitan_Police_ransomware_scam.jpg)

A Reveton payload, fraudulently claiming that the user must pay a fine to the [Metropolitan Police Service](https://en.wikipedia.org/wiki/Metropolitan_Police_Service)

In 2012, a major ransomware Trojan known as Reveton began to spread. Based on the Citadel [Trojan](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) (which itself, is based on the [Zeus](https://en.wikipedia.org/wiki/Zeus_(Trojan_horse)) Trojan), its payload displays a warning purportedly from a law enforcement agency claiming that the computer has been used for illegal activities, such as downloading [unlicensed software](https://en.wikipedia.org/wiki/Copyright_infringement#%22Piracy%22) or [child pornography](https://en.wikipedia.org/wiki/Child_pornography). Due to this behaviour, it is commonly referred to as the "Police Trojan".[[64]](https://en.wikipedia.org/wiki/Ransomware#cite_note-thejournal-policetrojam-64)[[65]](https://en.wikipedia.org/wiki/Ransomware#cite_note-65)[[66]](https://en.wikipedia.org/wiki/Ransomware#cite_note-reg-reve-66) 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](https://en.wikipedia.org/wiki/Ukash) or [paysafecard](https://en.wikipedia.org/wiki/Paysafecard). To increase the illusion that the computer is being tracked by law enforcement, the screen also displays the computer's [IP address](https://en.wikipedia.org/wiki/IP_address), while some versions display footage from a victim's [webcam](https://en.wikipedia.org/wiki/Webcam) to give the illusion that the user is being recorded.[[6]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-russia-6)[[67]](https://en.wikipedia.org/wiki/Ransomware#cite_note-iw-fbi-67)

Reveton initially began spreading in various European countries in early 2012.[[6]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-russia-6) Variants were localized with templates branded with the logos of different law enforcement organizations based on the user's country; for example, variants used in the United Kingdom contained the branding of organizations such as the [Metropolitan Police Service](https://en.wikipedia.org/wiki/Metropolitan_Police_Service) and the [Police National E-Crime Unit](https://en.wikipedia.org/wiki/Police_National_E-Crime_Unit). Another version contained the logo of the [royalty collection society](https://en.wikipedia.org/wiki/Copyright_collective) [PRS for Music](https://en.wikipedia.org/wiki/PRS_for_Music), which specifically accused the user of illegally downloading music.[[68]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-pecu-68) In a statement warning the public about the malware, the Metropolitan Police clarified that they would never lock a computer in such a way as part of an investigation.[[6]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-russia-6)[[15]](https://en.wikipedia.org/wiki/Ransomware#cite_note-hsfi-ransom-15)

In May 2012, [Trend Micro](https://en.wikipedia.org/wiki/Trend_Micro) threat researchers discovered templates for variations for the [United States](https://en.wikipedia.org/wiki/United_States) and [Canada](https://en.wikipedia.org/wiki/Canada), suggesting that its authors may have been planning to target users in North America.[[69]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-canusa-69) By August 2012, a new variant of Reveton began to spread in the United States, claiming to require the payment of a [$](https://en.wikipedia.org/wiki/United_states_dollar)200 fine to the FBI using a [MoneyPak](https://en.wikipedia.org/wiki/MoneyPak) card.[[7]](https://en.wikipedia.org/wiki/Ransomware#cite_note-FBI-7)[[8]](https://en.wikipedia.org/wiki/Ransomware#cite_note-IC3-8)[[67]](https://en.wikipedia.org/wiki/Ransomware#cite_note-iw-fbi-67) In February 2013, a Russian citizen was arrested in [Dubai](https://en.wikipedia.org/wiki/Dubai) by Spanish authorities for his connection to a crime ring that had been using Reveton; ten other individuals were arrested on [money laundering](https://en.wikipedia.org/wiki/Money_laundering) charges.[[70]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tw-revetonarrest-70) In August 2014, [Avast Software](https://en.wikipedia.org/wiki/Avast_Software) reported that it had found new variants of Reveton that also distribute password-stealing malware as part of its payload.[[71]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-revetonupgrade-71)

**CryptoLocker**

*Main article:*[*CryptoLocker*](https://en.wikipedia.org/wiki/CryptoLocker)

Encrypting ransomware reappeared in September 2013 with a Trojan known as [*CryptoLocker*](https://en.wikipedia.org/wiki/CryptoLocker), which generated a 2048-bit RSA key pair and uploaded in turn to a command-and-control server, and used to encrypt files using a [whitelist](https://en.wikipedia.org/wiki/Whitelist) of specific [file extensions](https://en.wikipedia.org/wiki/File_extension). The malware threatened to delete the private key if a payment of [Bitcoin](https://en.wikipedia.org/wiki/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 CryptoLocker extremely difficult to repair.[[24]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-cryptolocker-24)[[72]](https://en.wikipedia.org/wiki/Ransomware#cite_note-geek-cryptolocker-72)[[73]](https://en.wikipedia.org/wiki/Ransomware#cite_note-guardian-cryptolocker-73)[[74]](https://en.wikipedia.org/wiki/Ransomware#cite_note-sophos-cryptolocker-74) Even after the deadline passed, the private key could still be obtained using an online tool, but the price would increase to 10 BTC—which cost approximately US$2300 as of November 2013.[[75]](https://en.wikipedia.org/wiki/Ransomware#cite_note-nw-cryptolockersecondchance-75)[[76]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-moremoney-76)

CryptoLocker was isolated by the seizure of the [Gameover ZeuS](https://en.wikipedia.org/wiki/Gameover_ZeuS) [botnet](https://en.wikipedia.org/wiki/Botnet) as part of [Operation Tovar](https://en.wikipedia.org/wiki/Operation_Tovar), as officially announced by the [U.S. Department of Justice](https://en.wikipedia.org/wiki/U.S._Department_of_Justice) on 2 June 2014. The Department of Justice also publicly issued an [indictment](https://en.wikipedia.org/wiki/Indictment) against the Russian hacker Evgeniy Bogachev for his alleged involvement in the botnet.[[77]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cw-whambam-77)[[78]](https://en.wikipedia.org/wiki/Ransomware#cite_note-doj-takedown-78) It was estimated that at least US$3 million was extorted with the malware before the shutdown.[[11]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cl-takedown-11)

**CryptoLocker.F and TorrentLocker**

In September 2014, a wave of ransomware Trojans surfaced that first targeted users in [Australia](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/CAPTCHA) code before the payload is actually downloaded, preventing such automated processes from being able to scan the payload. [Symantec](https://en.wikipedia.org/wiki/NortonLifeLock) determined that these new variants, which it identified as *CryptoLocker.F*, were again, unrelated to the original CryptoLocker due to differences in their operation.[[79]](https://en.wikipedia.org/wiki/Ransomware#cite_note-symantec-aus-79)[[80]](https://en.wikipedia.org/wiki/Ransomware#cite_note-smh-lockup-80) A notable victim of the Trojans was the [Australian Broadcasting Corporation](https://en.wikipedia.org/wiki/Australian_Broadcasting_Corporation); live programming on its television [news channel](https://en.wikipedia.org/wiki/News_channel) [ABC News 24](https://en.wikipedia.org/wiki/ABC_News_24) was disrupted for half an hour and shifted to [Melbourne](https://en.wikipedia.org/wiki/Melbourne) studios due to a CryptoWall infection on computers at its [Sydney](https://en.wikipedia.org/wiki/Sydney) studio.[[81]](https://en.wikipedia.org/wiki/Ransomware#cite_note-arn-cryptolockerf-81)[[82]](https://en.wikipedia.org/wiki/Ransomware#cite_note-smh-cryptowall-82)[[83]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cso-abcnews24-83)

Another Trojan in this wave, [TorrentLocker](https://en.wikipedia.org/wiki/TorrentLocker), initially contained a design flaw comparable to CryptoDefense; it used the same [keystream](https://en.wikipedia.org/wiki/Keystream) for every infected computer, making the encryption trivial to overcome. However, this flaw was later fixed.[[36]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcworld-torrentlocker-36) By late-November 2014, it was estimated that over 9,000 users had been infected by TorrentLocker in Australia alone, trailing only Turkey with 11,700 infections.[[84]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cso-torrentlocker-84)

**CryptoWall**

Another major ransomware Trojan targeting Windows, CryptoWall, first appeared in 2014. One strain of CryptoWall was distributed as part of a [malvertising](https://en.wikipedia.org/wiki/Malvertising) campaign on the [Zedo](https://en.wikipedia.org/wiki/Zedo) ad network in late-September 2014 that targeted several major websites; the ads redirected to rogue websites that used browser plugin exploits to download the payload. A [Barracuda Networks](https://en.wikipedia.org/wiki/Barracuda_Networks) researcher also noted that the payload was signed with a [digital signature](https://en.wikipedia.org/wiki/Digital_signature) in an effort to appear trustworthy to security software.[[85]](https://en.wikipedia.org/wiki/Ransomware#cite_note-pcw-signedcryptowall-85) CryptoWall 3.0 used a payload written in [JavaScript](https://en.wikipedia.org/wiki/JavaScript) as part of an email attachment, which downloads executables disguised as [JPG](https://en.wikipedia.org/wiki/JPG) images. To further evade detection, the malware creates new instances of [explorer.exe](https://en.wikipedia.org/wiki/Explorer.exe) and [svchost.exe](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Bitcoin_wallet).[[86]](https://en.wikipedia.org/wiki/Ransomware#cite_note-tm-cw3-86)

The FBI reported in June 2015 that nearly 1,000 victims had contacted the bureau's [Internet Crime Complaint Center](https://en.wikipedia.org/wiki/Internet_Crime_Complaint_Center) to report CryptoWall infections, and estimated losses of at least $18 million.[[12]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-fbicryptowall-12)

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.[[87]](https://en.wikipedia.org/wiki/Ransomware#cite_note-heimdal-87)

**Fusob**

Fusob is one of the major mobile ransomware families. Between April 2015 and March 2016, about 56 percent of accounted mobile ransomware was Fusob.[[88]](https://en.wikipedia.org/wiki/Ransomware#cite_note-88)

Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom.[[89]](https://en.wikipedia.org/wiki/Ransomware#cite_note-89) The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 [USD](https://en.wikipedia.org/wiki/United_States_Dollar) or otherwise face a fictitious charge. Rather surprisingly, Fusob suggests using iTunes gift cards for payment. Also, a timer clicking down on the screen adds to the users’ anxiety as well.

In order to infect devices, Fusob [masquerades](https://en.wikipedia.org/wiki/Trojan_(computing)) as a pornographic video player. Thus, victims, thinking it is harmless, unwittingly download Fusob.[[90]](https://en.wikipedia.org/wiki/Ransomware#cite_note-90)

When Fusob is installed, it first checks the language used in the device. If it uses Russian or certain Eastern European languages, Fusob does nothing. Otherwise, it proceeds on to lock the device and demand ransom. Among victims, about 40% of them are in Germany with the United Kingdom and the United States following with 14.5% and 11.4% respectively.

Fusob has lots in common with Small, which is another major family of mobile ransomware. They represented over 93% of mobile ransomware between 2015 and 2016.

**WannaCry**

*Main article:*[*WannaCry ransomware attack*](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

In May 2017, the [WannaCry ransomware attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) spread through the Internet, using an exploit vector named [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue), which was allegedly leaked from the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency). The ransomware attack, unprecedented in scale,[[91]](https://en.wikipedia.org/wiki/Ransomware#cite_note-:3-91) infected more than 230,000 computers in over 150 countries,[[92]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cnbc1-92) using 20 different languages to demand money from users using [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) cryptocurrency. WannaCry demanded US$300 per computer.[[93]](https://en.wikipedia.org/wiki/Ransomware#cite_note-93) The attack affected [Telefónica](https://en.wikipedia.org/wiki/Telef%C3%B3nica) and several other large companies in Spain, as well as parts of the British [National Health Service](https://en.wikipedia.org/wiki/National_Health_Service) (NHS), where at least 16 hospitals had to turn away patients or cancel scheduled operations,[[94]](https://en.wikipedia.org/wiki/Ransomware#cite_note-94) [FedEx](https://en.wikipedia.org/wiki/FedEx), [Deutsche Bahn](https://en.wikipedia.org/wiki/Deutsche_Bahn), [Honda](https://en.wikipedia.org/wiki/Honda),[[95]](https://en.wikipedia.org/wiki/Ransomware#cite_note-95) [Renault](https://en.wikipedia.org/wiki/Renault), as well as the [Russian Interior Ministry](https://en.wikipedia.org/wiki/Ministry_of_Internal_Affairs_(Russia)) and Russian telecom [MegaFon](https://en.wikipedia.org/wiki/MegaFon).[[96]](https://en.wikipedia.org/wiki/Ransomware#cite_note-:2-96) The attackers gave their victims a 7-day deadline from the day their computers got infected, after which the encrypted files would be deleted.[[97]](https://en.wikipedia.org/wiki/Ransomware#cite_note-97)

**Petya**

*Main article:*[*Petya (malware)*](https://en.wikipedia.org/wiki/Petya_(malware))

*See also:*[*2017 cyberattacks on Ukraine*](https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine)

Petya was first discovered in March 2016; unlike other forms of encrypting ransomware, the malware aimed to infect the [master boot record](https://en.wikipedia.org/wiki/Master_boot_record), installing a payload which encrypts the file tables of the [NTFS](https://en.wikipedia.org/wiki/NTFS) file system the next time that the infected system boots, blocking the system from booting into Windows at all until the ransom is paid. [Check Point](https://en.wikipedia.org/wiki/Check_Point) reported that despite what it believed to be an innovative evolution in ransomware design, it had resulted in relatively-fewer infections than other ransomware active around the same time frame.[[98]](https://en.wikipedia.org/wiki/Ransomware#cite_note-nw-petyadouble-98)

On 27 June 2017, a heavily modified version of Petya was used for a global cyberattack primarily targeting [Ukraine](https://en.wikipedia.org/wiki/Ukraine) (but affecting many countries[[99]](https://en.wikipedia.org/wiki/Ransomware#cite_note-99)). This version had been modified to propagate using the same EternalBlue exploit that was used by WannaCry. Due to another design change, it is also unable to actually unlock a system after the ransom is paid; this led to security analysts speculating that the attack was not meant to generate illicit profit, but to simply cause disruption.[[100]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-wiper-100)[[101]](https://en.wikipedia.org/wiki/Ransomware#cite_note-BBCPMdc-101)

**Bad Rabbit**

On 24 October 2017, some users in [Russia](https://en.wikipedia.org/wiki/Russia) and Ukraine reported a new ransomware attack, named "Bad Rabbit", which follows a similar pattern to WannaCry and Petya by encrypting the user's file tables and then demands a Bitcoin payment to decrypt them. [ESET](https://en.wikipedia.org/wiki/ESET) believed the ransomware to have been distributed by a bogus update to [Adobe Flash](https://en.wikipedia.org/wiki/Adobe_Flash) software.[[102]](https://en.wikipedia.org/wiki/Ransomware#cite_note-102) Among agencies that were affected by the ransomware were: [Interfax](https://en.wikipedia.org/wiki/Interfax), [Odessa International Airport](https://en.wikipedia.org/wiki/Odessa_International_Airport), [Kiev Metro](https://en.wikipedia.org/wiki/Kiev_Metro), and the Ministry of Infrastructure of Ukraine.[[103]](https://en.wikipedia.org/wiki/Ransomware#cite_note-103) As it used corporate network structures to spread, the ransomware was also discovered in other countries, including Turkey, Germany, Poland, Japan, South Korea, and the United States.[[104]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cnn_badrabbit-104) Experts believed the ransomware attack was tied to the Petya attack in Ukraine (especially because Bad Rabbit's code has many overlapping and analogical elements to the code of Petya/NotPetya,[[105]](https://en.wikipedia.org/wiki/Ransomware#cite_note-105) appending to CrowdStrike Bad Rabbit and NotPetya's DLL (dynamic link library) share 67 percent of the same code[[106]](https://en.wikipedia.org/wiki/Ransomware#cite_note-106)) though the only identity to the culprits are the names of characters from the [*Game of Thrones*](https://en.wikipedia.org/wiki/Game_of_Thrones) series embedded within the code.[[104]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cnn_badrabbit-104)

Security experts found that the ransomware did not use the EternalBlue exploit to spread, and a simple method to vaccinate an unaffected machine running older Windows versions was found by 24 October 2017.[[107]](https://en.wikipedia.org/wiki/Ransomware#cite_note-107)[[108]](https://en.wikipedia.org/wiki/Ransomware#cite_note-108) Further, the sites that had been used to spread the bogus Flash updating have gone offline or removed the problematic files within a few days of its discovery, effectively killing off the spread of Bad Rabbit.[[104]](https://en.wikipedia.org/wiki/Ransomware#cite_note-cnn_badrabbit-104)

**SamSam**

In 2016, a new strain of ransomware emerged that was targeting [JBoss](https://en.wikipedia.org/wiki/WildFly) servers.[[109]](https://en.wikipedia.org/wiki/Ransomware#cite_note-109) This strain, named "[SamSam](https://en.wikipedia.org/w/index.php?title=SamSam_(malware)&action=edit&redlink=1)", was found to bypass the process of phishing or illicit downloads in favor of exploiting vulnerabilities on weak servers.[[110]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Barkley-110) The malware uses a [Remote Desktop Protocol](https://en.wikipedia.org/wiki/Remote_Desktop_Protocol) [brute-force attack](https://en.wikipedia.org/wiki/Brute-force_attack) to guess weak passwords until one is broken. The virus has been behind attacks on government and healthcare targets, with notable hacks occurring against the town of [Farmington, New Mexico](https://en.wikipedia.org/wiki/Farmington,_New_Mexico), the [Colorado Department of Transportation](https://en.wikipedia.org/wiki/Colorado_Department_of_Transportation), [Davidson County, North Carolina](https://en.wikipedia.org/wiki/Davidson_County,_North_Carolina), and most recently, a [major breach of security](https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack) on the infrastructure of [Atlanta](https://en.wikipedia.org/wiki/Atlanta).[[110]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Barkley-110)

Mohammad Mehdi Shah Mansouri (born in [Qom](https://en.wikipedia.org/wiki/Qom), [Iran](https://en.wikipedia.org/wiki/Iran) in 1991) and Faramarz Shahi Savandi (born in [Shiraz](https://en.wikipedia.org/wiki/Shiraz), [Iran](https://en.wikipedia.org/wiki/Iran), in 1984) are wanted by the [FBI](https://en.wikipedia.org/wiki/FBI) for allegedly launching SamSam ransomware.[[111]](https://en.wikipedia.org/wiki/Ransomware#cite_note-111) The two have allegedly made $6 million from extortion and caused over $30 million in damages using the malware.[[112]](https://en.wikipedia.org/wiki/Ransomware#cite_note-SamSam_DOJ_release-112)

**Syskey**

[Syskey](https://en.wikipedia.org/wiki/Syskey) is a utility that was included with [Windows NT](https://en.wikipedia.org/wiki/Windows_NT)-based operating systems to encrypt the [user account database](https://en.wikipedia.org/wiki/Security_Account_Manager), optionally with a password. The tool has sometimes been effectively used as ransomware during [technical support scams](https://en.wikipedia.org/wiki/Technical_support_scam)—where a caller with remote access to the computer may use the tool to lock the user out of their computer with a password known only to them.[[113]](https://en.wikipedia.org/wiki/Ransomware#cite_note-113) Syskey was removed from later versions of [Windows 10](https://en.wikipedia.org/wiki/Windows_10) and [Windows Server](https://en.wikipedia.org/wiki/Windows_Server) in 2017, due to being obsolete and "known to be used by hackers as part of ransomware scams".[[114]](https://en.wikipedia.org/wiki/Ransomware#cite_note-114)[[115]](https://en.wikipedia.org/wiki/Ransomware#cite_note-115)

Mitigation

As with other forms of malware, security software ([antivirus software](https://en.wikipedia.org/wiki/Antivirus_software)) might not detect a ransomware payload, or, especially in the case of encrypting payloads, only after encryption is under way or complete, particularly if a [new version unknown to the protective software](https://en.wikipedia.org/wiki/Zero-day_exploit) is distributed.[[116]](https://en.wikipedia.org/wiki/Ransomware#cite_note-yumasun-cryptolocker-116) If an attack is suspected or detected in its early stages, it takes some time for encryption to take place; immediate removal of the malware (a relatively simple process) before it has completed would stop further damage to data, without salvaging any already lost.[[117]](https://en.wikipedia.org/wiki/Ransomware#cite_note-malwarebytes-117)[[118]](https://en.wikipedia.org/wiki/Ransomware#cite_note-register-118)

Security experts have suggested precautionary measures for dealing with ransomware. Using software or other security policies to block known payloads from launching will help to prevent infection, but will not protect against all attacks[[24]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ars-cryptolocker-24)[[119]](https://en.wikipedia.org/wiki/Ransomware#cite_note-securityweek131119-119) As such, having a proper [backup](https://en.wikipedia.org/wiki/Backup) solution is a critical component to defending against ransomware. Note that, because many ransomware attackers will not only encrypt the victim's live machine but it will also attempt to delete any hot backups stored locally or on accessible over the network on a [NAS](https://en.wikipedia.org/wiki/Network-attached_storage), it's also critical to maintain "offline" [backups](https://en.wikipedia.org/wiki/Backup) of data [stored in locations inaccessible from any potentially infected computer](https://en.wikipedia.org/wiki/Storage_security), such as external storage drives or devices that [do not have any access to any network (including the Internet)](https://en.wikipedia.org/wiki/Air_gap_(networking)), prevents them from being accessed by the ransomware. Moreover, if using a NAS or [Cloud storage](https://en.wikipedia.org/wiki/Cloud_storage), then the computer should have [append-only](https://en.wikipedia.org/wiki/Append-only) permission to the destination storage, such that it cannot delete or overwrite previous backups.

Installing security [updates](https://en.wikipedia.org/wiki/Patch_(computing)) issued by software vendors can mitigate the [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) leveraged by certain strains to propagate.[[120]](https://en.wikipedia.org/wiki/Ransomware#cite_note-120)[[121]](https://en.wikipedia.org/wiki/Ransomware#cite_note-121)[[122]](https://en.wikipedia.org/wiki/Ransomware#cite_note-122)[[123]](https://en.wikipedia.org/wiki/Ransomware#cite_note-123)[[124]](https://en.wikipedia.org/wiki/Ransomware#cite_note-ecot-124) Other measures include [cyber hygiene](https://en.wikipedia.org/wiki/Cyber_hygiene) − exercising caution when opening [e-mail attachments](https://en.wikipedia.org/wiki/E-mail_attachment) and links, [network segmentation](https://en.wikipedia.org/wiki/Network_segmentation), and keeping critical computers isolated from networks.[[125]](https://en.wikipedia.org/wiki/Ransomware#cite_note-125)[[126]](https://en.wikipedia.org/wiki/Ransomware#cite_note-126) Furthermore, to mitigate the spread of ransomware measures of [infection control](https://en.wikipedia.org/wiki/Infection_control) can be applied.[[127]](https://en.wikipedia.org/wiki/Ransomware#cite_note-chang-127) Such may include disconnecting infected machines from all networks, educational programs,[[128]](https://en.wikipedia.org/wiki/Ransomware#cite_note-128) effective communication channels, malware surveillance[[*original research?*](https://en.wikipedia.org/wiki/Wikipedia:No_original_research)] and ways of collective participation[[127]](https://en.wikipedia.org/wiki/Ransomware#cite_note-chang-127)

**File system defenses against ransomware**

A number of file systems keep snapshots of the data they hold, which can be used to recover the contents of files from a time prior to the ransomware attack in the event the ransomware doesn't disable it.

* On Windows, the [Volume shadow copy](https://en.wikipedia.org/wiki/Volume_shadow_copy) (VSS) is often used to store backups of data; ransomware often targets these snapshots to prevent recovery and therefore it is often advisable to disable user access to the user tool *VSSadmin.exe* to reduce the risk that ransomware can disable or delete past copies.
* On Windows 10, users can add specific directories or files to Controlled Folder Access in Windows Defender to protect them from ransomware.[[129]](https://en.wikipedia.org/wiki/Ransomware#cite_note-129) It is advised to add backup and other important directories to Controlled Folder Access.
* File servers running [ZFS](https://en.wikipedia.org/wiki/ZFS) are almost universally immune to ransomware, because ZFS is capable of snapshotting even a large file system many times an hour, and these snapshots are immutable (read only) and easily rolled back or files recovered in the event of data corruption.[[130]](https://en.wikipedia.org/wiki/Ransomware#cite_note-130) In general, only an administrator can delete (but cannot modify) snapshots.

**File decryption and recovery**

There are a number of tools intended specifically to decrypt files locked by ransomware, although successful recovery may not be possible.[[2]](https://en.wikipedia.org/wiki/Ransomware#cite_note-schofield-2)[[131]](https://en.wikipedia.org/wiki/Ransomware#cite_note-131) If the same encryption key is used for all files, decryption tools use files for which there are both uncorrupted backups and encrypted copies (a [known-plaintext attack](https://en.wikipedia.org/wiki/Known-plaintext_attack) in the jargon of [cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis). But, it only works when the cipher the attacker used was weak to begin with, being vulnerable to known-plaintext attack); recovery of the key, if it is possible, may take several days.[[132]](https://en.wikipedia.org/wiki/Ransomware#cite_note-132) Free ransomware decryption tools can help decrypt files encrypted by the following forms of ransomware: AES\_NI, Alcatraz Locker, Apocalypse, BadBlock, Bart, BTCWare, Crypt888, CryptoMix, CrySiS, EncrypTile, FindZip, Globe, [Hidden Tear](https://en.wikipedia.org/wiki/Hidden_Tear), Jigsaw, LambdaLocker, Legion, NoobCrypt, Stampado, SZFLocker, [TeslaCrypt](https://en.wikipedia.org/wiki/TeslaCrypt), XData.[[133]](https://en.wikipedia.org/wiki/Ransomware#cite_note-133)

In addition, old copies of files may exist on the disk, which has been previously deleted. In some cases, these deleted versions may still be recoverable using software designed for that purpose.

The growing threat of malware

|  |  |
| --- | --- |
|  | This section **is written like a**[**personal reflection, personal essay, or argumentative essay**](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#Wikipedia_is_not_a_publisher_of_original_thought) that states a Wikipedia editor's personal feelings or presents an original argument about a topic. Please [help improve it](https://en.wikipedia.org/w/index.php?title=Ransomware&action=edit) by rewriting it in an [encyclopedic style](https://en.wikipedia.org/wiki/Wikipedia:Writing_better_articles#Information_style_and_tone). *(February 2020) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

Ransomware malicious software has evolved since its beginnings when it was confined to one or two countries in Eastern Europe which then spread across the Atlantic to the United States and Canada.[[134]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Gorman&McDonald-134) The first versions of this type of malware used various techniques to disable the computers[[134]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Gorman&McDonald-134) by locking the victims system machine (Locker Ransomware) [133]. Some examples of how this ransomware works, include; locking the screen by displaying a message from a branch of local law enforcement indicating the user's lines like “You have browsed illicit materials and must pay a fine”. They were first seen in Russia by year 2009 claiming to be a message from Microsoft. They also used to request a payment by sending an SMS message to a premium rate number. The next variant displayed pornographic image content and demanded payment for the removal of it.[[134]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Gorman&McDonald-134)

In 2011 the tactics changed, the attackers started to use electronic payment methods and they added more languages to the messages which also changed based on the user's location which was obtained by geo-locating the user's IP addresses.[[134]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Gorman&McDonald-134)

Not only end users are affected by these attacks. Corporations, private entities, government, and even hospitals are also affected. For example, in healthcare (although 2015 was the year in which the largest ePHI data breaches occurred according to the ONC) 2016 was the year that ransomware started to increase exponentially in this market. According to the 2017 Internet Security Threat Report from Symantec Corp, ransomware affects not only IT systems but also patient care, clinical operations, and billing. Online criminals have found “there was easy money to be made in healthcare,” according to the Symantec report, which was developed with data from insurance claims and the U.S. Department of Health and Human Services (HHS).[[135]](https://en.wikipedia.org/wiki/Ransomware#cite_note-135)

Ransomware is growing rapidly across the internet users but also for the IoT environment[[134]](https://en.wikipedia.org/wiki/Ransomware#cite_note-Gorman&McDonald-134) which creates a challenging problem to the INFOSEC while increasing the attack surface area. They are evolving into more sophisticated attacks and, they are becoming more resistant; at the same time, they are also more accessible than ever. Today, for a cheap price, the attackers have access to ransomware as a service. The big problem is that millions of dollars are lost by some organizations and industries that have decided to pay, such as the Hollywood Presbyterian Medical Center and the MedStar Health.[[136]](https://en.wikipedia.org/wiki/Ransomware#cite_note-136) At the end, the pressure to offer services to the patients and keep their lives is so critical that they are forced to pay, and the attacker knows that. The problem here is that by paying the ransom, they are funding the cybercrime.

According to Symantec 2019 ISTR report, for the first time since 2013, in 2018 there was an observed decrease in ransomware activity with a drop of 20 percent. Before 2017, consumers were the preferred victims, but in 2017 this changed dramatically, it moved to the enterprises. In 2018 this path accelerated with 81 percent infections which represented a 12 percent increase.[[137]](https://en.wikipedia.org/wiki/Ransomware#cite_note-137) The common distribution method today is based on email campaigns.

Cyber awareness training is crucial to detecting attacks, whereas technology cannot protect against careless or foolish behavior.[[138]](https://en.wikipedia.org/wiki/Ransomware#cite_note-138) It is important for organizations to help their users recognize malicious contact whereas ransomware is typically introduced through email and [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(security)) techniques to either download a file, provide key sensitive information or take some action that will bring harm to the organization.  According to KnowBe4 Osterman report, there are number of approaches to security awareness training that are practiced by organizations and managed by security teams. There is the break room approach which are special meetings periodically held  to talk about security; monthly security videos with short snippets of security information; simulated phishing tests which target users with internal phishing messages; human firewall approach where everyone is subject to simulated phishing and those employees that are prone to attack are identified; and then there is the do-nothing approach where cyber awareness training does not exist in the organization.[[139]](https://en.wikipedia.org/wiki/Ransomware#cite_note-139)

An effective and successful cyber awareness training program must be sponsored from the top of the organization with supporting policies and procedures which effectively outline ramifications of non-compliance, frequency of training and a process for acknowledgement of training. Without sponsorship from the “C-level” executives the training cannot be ignored.  Other factors that are key to a successful Cyber Awareness Training program is to establish a baseline identifying the level of knowledge of the organization to establish where the users are in their knowledge prior to training and after. Whichever approach an organization decides to implement, it is important that the organization has policies and procedures in place that provide training that is up to date, performed frequently and has the backing of the entire organization from the top down.

Investment in technology to detect and stop these threats must be maintained, but along with that we need to remember and focus on our weakest link, which is the user.

Freedom of speech challenges and criminal punishment

The publication of proof-of-concept attack code is common among academic researchers and vulnerability researchers. It teaches the nature of the threat, conveys the gravity of the issues, and enables countermeasures to be devised and put into place. However, lawmakers with the support of law-enforcement bodies are contemplating making the creation of ransomware illegal. In the state of Maryland, the original draft of HB 340 made it a felony to create ransomware, punishable by up to 10 years in prison.[[140]](https://en.wikipedia.org/wiki/Ransomware#cite_note-hb340-140) However, this provision was removed from the final version of the bill.[[141]](https://en.wikipedia.org/wiki/Ransomware#cite_note-marylandbill-141) A minor in Japan was arrested for creating and distributing ransomware code.[[142]](https://en.wikipedia.org/wiki/Ransomware#cite_note-jransomware-142) Young and [Yung](https://en.wikipedia.org/wiki/Moti_Yung) have had the ANSI C source code to a ransomware cryptotrojan on-line, at cryptovirology.com, since 2005 as part of a [cryptovirology](https://en.wikipedia.org/wiki/Cryptovirology) book being written. The source code to the cryptotrojan is still live on the Internet and is associated with a draft of Chapter 2.[[143]](https://en.wikipedia.org/wiki/Ransomware#cite_note-yychp2-143)

Ransomware arrests and convictions

A British student Zain Qaiser (24) from Barking, London was jailed for more than six years at Kingston Crown Court for his ransomware attacks in 2019.[[144]](https://en.wikipedia.org/wiki/Ransomware#cite_note-144). He is said to have been "the most prolific cyber criminal to be sentenced in the UK". He became active when he was only 17. He contacted the Russian controller of one of the most powerful attacks, believed to be the Lurk malware gang, and arranged for a split of his profits. He also contacted online criminals from China and the US to move the money. For about one and a half years, he posed as a legitimate supplier of online promotions of book advertising on some of the world's most visited legal pornography websites. Each of the adverts that was promoted on the websites contained the Reveton strain of the malicious "Angler Exploit Kit (AEK)"[[145]](https://en.wikipedia.org/wiki/Ransomware#cite_note-145) code that seized control of the machine. Investigators discovered about £700,000 of earnings, although his network may have earned more than £4m. He may have hidden some money using cryptocurrencies. The ransomware would instruct victims to buy [GreenDot MoneyPak](https://en.wikipedia.org/wiki/MoneyPak) vouchers, and enter the code in the Reveton panel that being displayed on the screens. This money entered a MoneyPak account managed by Qaiser, who would then deposit the voucher payments into an American co-conspirator's (Raymond Odigie Uadiale Uadiale, who was then a student at [Florida International University](https://en.wikipedia.org/wiki/Florida_International_University) during 2012 and 2013 and later worked for Microsoft) debit card, who would convert the money into Liberty Reserve digital currency and deposit it into Qaiser's Liberty Reserve account.[[146]](https://en.wikipedia.org/wiki/Ransomware#cite_note-146)

A breakthrough in this case came occurred in May 2013 when authorities from several countries seized the [Liberty Reserve](https://en.wikipedia.org/wiki/Liberty_Reserve) servers, obtaining access to all the transactions and account history. Qaiser was running encrypted virtual machines on his Macbook Pro with both Mac and Windows operating systems.[[147]](https://en.wikipedia.org/wiki/Ransomware#cite_note-147) He could not be tried earlier because he was sectioned under the UK Mental Health Act at Goodmayes hospital (where he was found to be using the hospital wifi to access his advertising sites.) His lawyer claimed that Qaiser had suffered from mental illness.[[148]](https://en.wikipedia.org/wiki/Ransomware#cite_note-148) Russian police arrested 50 members of the Lurk malware gang in June 2016.[[149]](https://en.wikipedia.org/wiki/Ransomware#cite_note-149) Raymond Odigie Uadiale, a naturalized US citizen of Nigerian descent, was jailed for 18 months.[[150]](https://en.wikipedia.org/wiki/Ransomware#cite_note-150)

# **Ransomware: Facts, Threats, and Countermeasures**

### Ransomware

Ransomware is a type of malware that has become a significant threat to U.S. businesses and individuals during the past two years. Most of the current ransomware variants encrypt files on the infected system/network (crypto ransomware), although a few variants are known to erase files or block access to the system using other methods (locker ransomware). Once access to the system is blocked, the ransomware demands a ransom in order to unlock the files, frequently $200 - $3,000 in bitcoins, though other currencies and gift cards are occasionally reported. Ransomware variants almost always opportunistically target victims, infecting an array of devices from computers to smartphones.

Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.

### Infection Vectors

The majority of ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website. In other instances, malware is disseminated through malvertising and drive-by downloads, which do not require user engagement for the infection to be successful.

While almost all ransomware infections are opportunistic, disseminated through indiscriminate infection vectors such as those discussed above, in a few very rare instances cyber threat actors specifically target a victim. This may occur after the actors realize that a sensitive entity has been infected or because of specific infection attempts. The Federal Bureau of Investigation (FBI) refers to these instances as extortion, rather than ransomware, as there is almost always a higher ransom amount that coincides with the strategic targeting. This was the case in spring 2016, when several hospitals infected with strategically targeted ransomware made the news.

### Additional Capabilities

In the past year, ransomware variants features have expanded to include data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components. One variant deletes files regardless of whether or not a payment was made. Another variant includes the capability to lock cloud-based backups when systems continuously back up in real-time (a.k.a. during persistent synchronization). Other variants target smartphones and Internet of Things (IoT) devices.

Although not as common, some variants claim to be from a law enforcement agency and that the user owes a “fee” or “fine” for conducting illegal activities, such as viewing pornography. In an effort to appear more legitimate these variants can use techniques to identify the victim’s rough geographic location in order to use the name of a specific law enforcement agency. No U.S. law enforcement agency will ever remotely lock or disable a computer and demand a fine to unlock it.

### How to Mitigate the Risk of Ransomware Infections

These recommendations are not comprehensive but provide general best practices.

#### **Securing Networks and Systems**

* **Have an incident response plan** that includes what to do during a ransomware event.
* **Backups are critical.** Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.
* **Use antivirus and anti-spam solutions.** Enable regular system and network scans with antivirus programs enabled to automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.
* **Disable macros scripts.** Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
* **Keep all systems patched**, including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date. Use a centralized patch management system if possible. Implement application white-listing and software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.
* **Restrict Internet access.** Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.
* **Apply the principles of least privilege and network segmentation.** Categorize and separate data based on organizational value and where possible, implement virtual environments and the physical and logical separation of networks and data. Apply the principle of least privilege.
* **Vet and monitor third parties** that have remote access to the organization’s network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
* **Participate in cybersecurity information sharing** programs and organizations, such as MS-ISAC and InfraGard.

#### **Securing the End User**

* **Provide social engineering and phishing training to employees.** Urge them not to open suspicious emails, not to click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites.
* **Remind users to close their browser** when not in use.
* **Have a reporting plan** that ensures staff knows where and how to report suspicious activity.

#### **Responding to a Compromise/Attack**

* **Immediately** disconnect the infected system from the network to prevent infection propagation.
* **Determine the affected data** as some sensitive data, such as electronic protected health information (ePHI) may require additional reporting and/or mitigation measures.
* **Determine if a decryptor is available.** Online resources such as [No More Ransom!](https://www.nomoreransom.org/) can help.
* **Restore** files from regularly maintained backups.
* R**eport the infection.** It is highly recommended that SLTT government agencies report ransomware incidents to MS-ISAC. Other sectors and home users may report to infections to local Federal Bureau of Investigation (FBI) field offices or to the [Internet Crime Complaint Center (IC3)](http://www.ic3.gov/).