**Ransomware** is a type of [malicious software](https://en.wikipedia.org/wiki/Malicious_software) that blocks access to the victim's data or threatens to publish or delete it until a [ransom](https://en.wikipedia.org/wiki/Ransom) is paid. It holds a computer or system’s files and functionality hostage in exchange for a ransom

The genesis of Ransomware is likely when Dr. Joseph Popp, an evolutionary biologist, created the AIDS Trojan, which was handed out by Popp via floppy disk to tens of thousands of attendees to a World Health Organization AIDS conference. When inserted and the program executed, it took over the machine, encrypted the files via symmetric encryption, and demanded $189 be sent to the “PC Cyborg Corporation”. Popp was eventually caught and a workaround was found due to the fact that the encryption was symmetric, but his actions sowed the seeds for hackers to use more sophisticated iterations of encryption and demand more ludicrous sums of money.

While Popp’s actions are the first documented case of Ransomware, it’s popularity amongst hackers is likely also based in its relationship to other forms of malware. Indeed, demanding money for protection is also prevalent in “scareware”, albeit in a subtler way. Scareware is a class of programs that tend to pop up on a user’s screen with an appearance emulating an alert from the user’s operating system or anti-virus software telling the user that they need to install software or run a scan to detect or destroy malware. By doing so, they entice the user to download software that is, in fact, malware in and of itself4 . Generic pop-ups on or from untrusted websites work in similar ways: They entice users to click something which then installs malware on the system. Even if hackers had never heard of Dr. Popp, they certainly could have drawn on pop-ups and scareware and stretched the limits of what malware can do by asking for money.



Any action is possible once a device or system is infected and there is no guarantee that paying the ransom will return access or not delete the data. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse.

More advanced malware uses a technique called [cryptoviral extortion](https://en.wikipedia.org/wiki/Cryptoviral_extortion), in which it [encrypts](https://en.wikipedia.org/wiki/Encrypts) the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

The ransomware may also encrypt the computer's [Master File Table](https://en.wikipedia.org/wiki/Master_File_Table) (MFT) or the entire hard drive. Thus, ransomware is a [denial-of-access attack](https://en.wikipedia.org/wiki/Denial-of-access_attack) that prevents computer users from accessing files since it is [intractable](https://en.wikipedia.org/wiki/Computational_complexity_theory#Intractability) to decrypt the files without the decryption [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29). Ransomware attacks are typically carried out using a [Trojan](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) that has a payload disguised as a legitimate file.

Ransomware attack



.

**Technical aspect of how ransomware happens**

The user of a computer or system unwitting executes or downloads a program that then takes over the terminal of the user and simultaneously begins encrypting all of the files on the system. In order to cover the files and system functionality, the user must follow instructions given by the program, which generally involves wiring money somewhere. Generally speaking, the sum of money is not small. If this program infects the system of an enterprise, millions of dollars-worth of information can be held hostage, and thus, demand millions of dollars

Ransom demand



**Ransomware belongs to the Anonymous group of hackers**

Anonymous is a decentralized open online creation group known most for its hacking and Guy Fawkes masks. Reports posit Anonymous is comprised of thousands of “hacktivists.” The group has compromised government, religious and corporate websites.

**Attacks related to Ransomware attack include**

**Spoofing**

A person or program falsifies information to masquerade as someone else or another application. An example is email address spoofing whereby the sender information, i.e. the ‘From’ field, is spoofed to hide the true origins of the email, whilst also imitating another email address. Email address spoofing is widely used in phishing attacks whereby someone fraudulently sends out an email to acquire sensitive information, such as usernames, passwords and credit card details, by impersonating a trustworthy entity, i.e. a bank.

### Man in the middle

An attacker manages to infiltrate a communication system to impersonate each endpoint to the satisfaction of each other. This can be done very easily if an attacker connects to an unencrypted wireless access point. The attacker can then intercept the information sent from an unsuspecting victim as well as the information they would be expecting to receive. This can be particularly critical should the unsuspecting victim be using online banking. Not only could the attacker view all the information being transferred to and from you and your bank they could spoof the bank website to siphon your private details or to divert all payments made to their own account.

### Spyware/viruses and trojans

These are malicious programs that attackers will bundle into other legitimate programs, or will try and trick their target into running. Spyware, when run, will spy on you to track predetermined bits of information, i.e. your keystrokes or websites visited.

A Trojan is a piece of software that can have similar functionality to spyware, however, it gives the attacker more control, i.e. remote access or control of the victim’s system.

A virus is similar to a Trojan with the added functionality that, when run on your system, it will try and autonomously proliferate and infect other systems.

**Ethical Aspects**

It is wrong on the basis that it compromises the security of the organisation, this scam, which exploits a vulnerability in Windows operating systems, locks up users' data files, then offers a "key" or code to unlock them for a ransom payment in hard-to-trace digital Bitcoins. Ransomware is a “Hit and Run” business, crooks use social engineering tricks to induce victims in rapidly pay up of the ransom. The pay up request time normally limited to less than 24 hours. In this way, criminal organizations try to maximize their efforts in a limited period of time by limiting their exposure to law enforcement agencies.

The economic impact of Ransomware infection could also be measured evaluating the effort spent to restore the encrypted file and the business opportunity lost during the infection.

**Technical aspects**

Ransomware attacks are typically carried out using a [Trojan](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), entering a system through, for example, a downloaded file or vulnerability in a network service. The program then runs a [payload](https://en.wikipedia.org/wiki/Payload_%28computing%29), 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_%28media%29)

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 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 system from booting until it is repaired 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.

Payment is virtually always the goal, and the victim is coerced into paying for the ransomware to be removed—which may or may not actually occur—either by supplying a program that can decrypt the files, or by sending an unlock code that undoes the payload's changes. 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) pre-paid [voucher](https://en.wikipedia.org/wiki/Voucher) services such as [**Pay safe card**](https://en.wikipedia.org/w/index.php?title=Paysafecard&action=edit&redlink=1), and the [digital currency](https://en.wikipedia.org/wiki/Digital_currency) [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin). A 2016 census commissioned by [Citrix](https://en.wikipedia.org/wiki/Citrix) revealed that larger businesses are holding bitcoin as contingency plans.

It is wrong on the basis that it compromises the security of the organisation, this scam, which exploits a vulnerability in Windows operating systems, locks up users' data files, then offers a "key" or code to unlock them for a ransom payment in hard-to-trace digital Bitcoins

Ransomware is a “Hit and Run” business, crooks use social engineering tricks to induce victims in rapidly pay up of the ransom.

The pay up request time normally limited to less than 24 hours. In this way, criminal organizations try to maximize their efforts in a limited period of time by limiting their exposure to law enforcement agencies.

The economic impact of Ransomware infection could also be measured evaluating the effort spent to restore the encrypted file and the business opportunity lost during the infection.

Many times, they're backed by organized crime or nation states. The black hat operates on the dark side of the Internet, damaging organizations, spreading unsavory content, and threatens governments with cyber terrorism. And they can cripple a victim's financial and well-being. White hat hackers are considered to be the good guys and are "ethical hackers." The white hat hacker has a supportive government and industry and is computer experts.

Many times, they are contract employees hired by security companies and are trained to test systems and attempt to break into them. But they can also be an internal team conducting regular penetration testing as part of an overall security plan. Ethical hackers diligently look for any system vulnerabilities in the computer's defense system, where, once identified, is reported and fixed either by the white hat team or the appropriate IT personnel, with the idea of improving a company's defense posture.

**General principles of hackers**

* Expressed (often written) permission to probe the network and attempt to identify potential security risks.
* You respect the individual's or company's privacy.
* You close out your work, not leaving anything open for you or someone else to exploit at a later time.
* You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware, if not already known by the company.

**Mitigating Ransomware attack**

An overall approach to addressing the threat of ransomware could include the following practices:

* Train and educate personnel on an ongoing basis not click hyperlinks from un-known sources, and without establishing authenticity of link even from known sources. Develop a communication channel and strategy to quickly inform all employees if a virus reaches the company network
* Specifically address and plan for Ransomware in the business’ disaster recovery and business continuity plans, including testing of those plans.
* Ensure that all anti-virus and other security software is properly updated. Many forms of Ransomware can be detected and avoided using this simple step. Back up all digital content to a secure, offsite secret location(s) within the organisation and keep all software (especially the system software) up to date, including operating systems and applications.
* Engage a third-party expert security vendor to assess your organization’s systems and procedures. This expert should also train all the staff using the digital assets including mobile devices connected to network, on cyber security practices, emphasizing not opening attachments or links from unknown sources.
* Prepare an up-to-date inventory of all the “Digital Assets” at various locations/facilities being used by the various departments; this will ease identifying and isolating potentially infected systems.

#### General outlook or impact of such an attack

Ransomware typically targets an organization’s most valued information. But it could reach almost any information, including marketing materials, payroll data, intellectual property, financial transactions, and health records.

Hiring an expert who is able to decrypt the information is often more expensive and time-consuming than paying the ransom to get the information restored. And sometimes data restored by a recovery service is incomplete, with full recovery requiring the decryption key. However, by the time an organization discovers that the recovery is incomplete; the attacker likely has already destroyed the key and moved on, making full recovery impossibility.

If the Ransomware hits certain servers, it may be distributed throughout an organization to all users and potentially to third-party users connecting to those servers or other infected user devices. It can also infect the organization’s backup media, meaning that if the target tries to restore data from its backups, it could re-infect its systems and data.

These attacks can take hostage and threaten to or actually disclose confidential or proprietary information to the public or, even worse, the highest bidder. The fear of such disclosure a motivating factor for victims and gives them little time to think rationally about their options. They are therefore considered terrorist attacks as documented by the various FBI reports.