Ransomware is a type of malware that encrypts the victim's personal data until a ransom is paid.[1][2][3][4][5] Difficult-to-trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are commonly used for the ransoms, making tracing and prosecuting the perpetrators difficult. Sometimes the original files can be retrieved without paying the ransom due to implementation mistakes, leaked cryptographic keys or a complete lack of encryption in the ransomware.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.[6]

Starting as early as 1989 with the first documented ransomware known as the AIDS trojan, the use of ransomware scams grew internationally.[7][8][9] There were 181.5 million ransomware attacks worldwide in the first six months of 2018, 229% more than the first six months of 2017.[10] In June 2014, security software company McAfee released data showing that it had collected more than double the number of ransomware samples that quarter than it had in the same quarter the previous year.[11] CryptoLocker was particularly successful, procuring an estimated US$3 million before it was taken down by authorities,[12] and CryptoWall was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over US$18 million by June 2015.[13] In 2020, the US Internet Crime Complaint Center (IC3) received 2,474 complaints identified as ransomware, with adjusted losses of over $29.1 million. The losses could exceed this amount, according to the FBI.[14] Globally, according to Statista, there were about 623 million ransomware attacks in 2021, and 493 million in 2022.[15]

Ransomware payments were estimated at $1.1bn in 2019,[16] $999m in 2020, a record $1.25bn in 2023, and a sharp drop to $813m in 2024,[17] attributed to non-payment by victims and action by law enforcement.

Operation

The concept of file-encrypting ransomware was invented and implemented by Young and Yung at 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*.[18] Cryptoviral extortion is the following three-round protocol carried out between the attacker and the victim.[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 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 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, entering a system through, for example, a malicious attachment, an embedded link in a phishing email, or a vulnerability in a network service. The program then runs a payload, which locks the system in some fashion, or claims to lock the system but does not (e.g., a scareware program). Payloads may display a fake warning purportedly by an entity such as a law enforcement agency, falsely claiming that the system has been used for illegal activities, contains content such as pornography and "pirated" media.[19][20][21]

Some payloads consist simply of an application designed to lock or restrict the system until payment is made, typically by setting the Windows Shell to itself,[22] or even modifying the master boot record and/or partition table to prevent the operating system from booting until it is repaired.[23] The most sophisticated payloads encrypt files, with many using strong encryption to encrypt the victim's files in such a way that only the malware author has the needed decryption key.[1][24][25]

Payment is virtually always the goal, and the victim is coerced 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, premium-rate text messages,[26] pre-paid voucher services such as paysafecard,[7][27][28] and the Bitcoin cryptocurrency.[29][30][31]

In May 2020, vendor Sophos reported that the global average cost to remediate a ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity and ransom paid) was $761,106. Ninety-five percent of organizations that paid the ransom had their data restored.[32]

History

See also: History of computer viruses and History of malware

Encrypting ransomware

The first known malware extortion attack, the "AIDS Trojan" written by 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, 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$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 to stand trial for his actions, but he promised to donate the profits from the malware to fund AIDS research.[33]

The idea of abusing anonymous cash systems to safely collect ransom from human kidnapping was introduced in 1992 by Sebastiaan von Solms and David Naccache.[34] This electronic money collection method was also proposed for cryptoviral extortion attacks.[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. Young and Yung critiqued the failed AIDS Information Trojan that relied on symmetric cryptography 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 that used RSA and the Tiny Encryption Algorithm (TEA) to hybrid encrypt the victim's data. Since public key cryptography is used, the virus 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 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] They referred to these attacks as being "cryptoviral extortion", an overt attack that is part of a larger class of attacks in a field called cryptovirology, which encompasses both overt and covert attacks.[1] The cryptoviral extortion protocol was inspired by the parasitic relationship between H. R. Giger's facehugger and its host in the movie *Alien*.[1][18]

Examples of extortionate ransomware became prominent in May 2005.[35] By mid-2006, Trojans such as Gpcode, TROJ.RANSOM.A, 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.[36] 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 effort.[37][38][39][40]

Encrypting ransomware returned to prominence in late 2013 with the propagation of CryptoLocker—using the Bitcoin digital currency platform to collect ransom money. In December 2013, 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.[41] The CryptoLocker technique was widely copied 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, due to its use of Windows' built-in encryption APIs),[30][42][43][44] and the August 2014 discovery of a Trojan specifically targeting network-attached storage devices produced by Synology.[45] In January 2015, it was reported that ransomware-styled attacks have occurred against individual websites via hacking, and through ransomware designed to target Linux-based web servers.[46][47][48]

In 2022, Costa Rica received widespread Conti ransomware attacks affecting government, healthcare and industry.[49] This led President Rodrigo Chaves to declare a state of emergency and announce that Costa Rica is "at war" with its ransomware hackers.[50]

In some infections, there is a two-stage payload, common in many malware systems. The user is tricked into running a script, which downloads the main virus and executes it. In early versions of the dual-payload system, the script was contained in a Microsoft Office document with an attached VBScript macro, or in a windows scripting facility (WSF) file. As detection systems started blocking these first stage payloads, the Microsoft Malware Protection Center identified a trend away toward LNK files with self-contained Microsoft Windows PowerShell scripts.[51] In 2016, PowerShell was found to be involved in nearly 40% of endpoint security incidents.[52]

Some ransomware strains have used proxies tied to Tor hidden services to connect to their command and control servers, increasing the difficulty of tracing the exact location of the criminals.[53][54] Furthermore, dark web vendors have increasingly[*when?*] started to offer the technology as a service, wherein ransomware is sold, ready for deployment on victims' machines, on a subscription basis, similarly to Adobe Creative Cloud or Office 365.[54][55][56]

Symantec has classified ransomware to be the most dangerous cyber threat.[57]