Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.[1][2][3][4] In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

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.[5]

Starting as early as 1989 with the first documented ransomware known as the AIDS trojan, the use of ransomware scams has grown internationally.[6][7][8] There were 181.5 million ransomware attacks in the first six months of 2018. This record marks a 229% increase over this same time frame in 2017.[9] In June 2014, vendor 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 of the previous year.[10] CryptoLocker was particularly successful, procuring an estimated US$3 million before it was taken down by authorities,[11] and CryptoWall was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over US$18 million by June 2015.[12] In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. The losses could be more than that, according to the FBI.[13] According to a report by SonicWall, there were around 623 million ransomware attacks in 2021.[14]

Contents

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*.[15] 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, 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.[16][17][18]

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,[19] or even modifying the master boot record and/or partition table to prevent the operating system from booting until it is repaired.[20] 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][21][22]

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,[23] pre-paid voucher services such as paysafecard,[6][24][25] and the Bitcoin cryptocurrency.[26][27][28]

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.[29]

History

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.[30]

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.[31] 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][15]

Examples of extortionate ransomware became prominent in May 2005.[32] 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.[33] 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.[34][35][36][37]

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.[38] 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),[27][39][40][41] and the August 2014 discovery of a Trojan specifically targeting network-attached storage devices produced by Synology.[42] 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.[43][44][45]

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.[46] In 2016, PowerShell was found to be involved in nearly 40% of endpoint security incidents,[47]

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.[48][49] Furthermore, dark web vendors have increasingly 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.[49][50][51]

Symantec has classified ransomware to be the most dangerous cyber threat.[52]

On 28 September 2020, the computer systems at US' biggest healthcare provider the Universal Health Services, was hit by a ransomware attack. The UHS chain from different locations reported noticing problems, with some locations reporting locked computers and phone systems from early Sunday (27 September).[53][52]

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 (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.[18][54]

In 2011, a ransomware Trojan surfaced that imitated the 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 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 charges.[16]

In February 2013, a ransomware Trojan based on the Stamp.EK exploit kit surfaced; the malware was distributed via sites hosted on the project hosting services SourceForge and GitHub that claimed to offer "fake nude pics" of celebrities.[55] In July 2013, an 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 to frustrate attempts to close the page through normal means.[56]

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 accusing him of possessing child pornography. An investigation discovered the incriminating files, and the man was charged with child sexual abuse and possession of child pornography.[57]

Exfiltration (Leakware / Doxware)

The converse of ransomware is a 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.[58] 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 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".[59] 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.

Common targets for exfiltration include:

- third party information stored by the primary victim (such as customer account information or health records);
- information proprietary to the victim (such as trade secrets and product information)
- embarrassing information (such as the victim's health information or information about the victim's personal past)

Exfiltration attacks are usually targeted, with a curated victim list, and often preliminary surveillance of the victim's systems to find potential data targets and weaknesses.[60][61]

Mobile ransomware

With the increased popularity of ransomware on PC platforms, ransomware targeting mobile operating systems 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.[62] Mobile ransomware typically targets the Android platform, as it allows applications to be installed from third-party sources.[62][63] The payload is typically distributed as an APK file installed by an unsuspecting user; it may attempt to display a blocking message over top of all other applications,[63] while another used a form of clickjacking to cause the user to give it "device administrator" privileges to achieve deeper access to the system.[64]

Different tactics have been used on iOS devices, such as exploiting iCloud accounts and using the Find My iPhone system to lock access to the device.[65] On iOS 10.3, Apple patched a bug in the handling of JavaScript pop-up windows in Safari that had been exploited by ransomware websites.[66] 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.[67]

In August 2019 researchers demonstrated it's possible to infect DSLR cameras with ransomware.[68] Digital cameras often use 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 security conference in Las Vegas as a proof of concept attack (not as actual armed malware).

Notable attack targets

Notable software packages

Reveton

In 2012, a major ransomware Trojan known as Reveton began to spread. Based on the Citadel Trojan (which, itself, is based on the Zeus Trojan), its payload displays a warning purportedly from a law enforcement agency claiming that the computer has been used for illegal activities, such as downloading unlicensed software or child pornography. Due to this behaviour, it is commonly referred to as the "Police Trojan".[69][70][71] The warning informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as Ukash or paysafecard. To increase the illusion that the computer is being tracked by law enforcement, the screen also displays the computer's IP address, while some versions display footage from a victim's webcam to give the illusion that the user is being recorded.[6][72]

Reveton initially began spreading in various European countries in early 2012.[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 and the Police National E-Crime Unit. Another version contained the logo of the royalty collection society PRS for Music, which specifically accused the user of illegally downloading music.[73] 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][17]

A Reveton payload, fraudulently claiming that the user must pay a fine to the Metropolitan Police Service

In May 2012, Trend Micro threat researchers discovered templates for variations for the United States and Canada, suggesting that its authors may have been planning to target users in North America.[74] By August 2012, a new variant of Reveton began to spread in the United States, claiming to require the payment of a $200 fine to the FBI using a MoneyPak card.[7][8][72] In February 2013, a Russian citizen was arrested in Dubai by Spanish authorities for his connection to a crime ring that had been using Reveton; ten other individuals were arrested on money laundering charges.[75] In August 2014, Avast Software reported that it had found new variants of Reveton that also distribute password-stealing malware as part of its payload.[76]

CryptoLocker

Encrypting ransomware reappeared in September 2013 with a Trojan known as *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 of specific file extensions. The malware threatened to delete the private key if a payment of Bitcoin or a pre-paid cash voucher was not made within 3 days of the infection. Due to the extremely large key size it uses, analysts and those affected by the Trojan considered CryptoLocker extremely difficult to repair.[26][77][78][79] 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.[80][81]

CryptoLocker was isolated by the seizure of the Gameover ZeuS botnet as part of Operation Tovar, as officially announced by the U.S. Department of Justice on 2 June 2014. The Department of Justice also publicly issued an indictment against the Russian hacker Evgeniy Bogachev for his alleged involvement in the botnet.[82][83] It was estimated that at least US$3 million was extorted with the malware before the shutdown.[11]

CryptoLocker.F and TorrentLocker

In September 2014, a wave of ransomware Trojans surfaced that first targeted users in Australia, under the names *CryptoWall* and *CryptoLocker* (which is, as with CryptoLocker 2.0, unrelated to the original CryptoLocker). The Trojans spread via fraudulent e-mails claiming to be failed parcel delivery notices from Australia Post; to evade detection by automatic e-mail scanners that follow all links on a page to scan for malware, this variant was designed to require users to visit a web page and enter a CAPTCHA code before the payload is actually downloaded, preventing such automated processes from being able to scan the payload. Symantec determined that these new variants, which it identified as *CryptoLocker.F*, were again, unrelated to the original CryptoLocker due to differences in their

operation.[84][85] A notable victim of the Trojans was the Australian Broadcasting Corporation; live programming on its television news channel ABC News 24 was disrupted for half an hour and shifted to Melbourne studios due to a CryptoWall infection on computers at its Sydney studio.[86][87][88]

Another Trojan in this wave, TorrentLocker, initially contained a design flaw comparable to CryptoDefense; it used the same keystream for every infected computer, making the encryption trivial to overcome. However, this flaw was later fixed.[39] 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.[89]

CryptoWall

Another major ransomware Trojan targeting Windows, CryptoWall, first appeared in 2014. One strain of CryptoWall was distributed as part of a malvertising campaign on the Zedo ad network in late-September 2014 that targeted several major websites; the ads redirected to rogue websites that used browser plugin exploits to download the payload. A Barracuda Networks researcher also noted that the payload was signed with a digital signature in an effort to appear trustworthy to security software.[90] CryptoWall 3.0 used a payload written in JavaScript as part of an email attachment, which downloads executables disguised as JPG images. To further evade detection, the malware creates new instances of explorer.exe and svchost.exe to communicate with its servers. When encrypting files, the malware also deletes volume shadow copies and installs spyware that steals passwords and Bitcoin wallets.[91]

The FBI reported in June 2015 that nearly 1,000 victims had contacted the bureau's Internet Crime Complaint Center to report CryptoWall infections, and estimated losses of at least $18 million.[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.[92]

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.[93]

Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom.[94] The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 USD 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 as a pornographic video player. Thus, victims, thinking it is harmless, unwittingly download Fusob.[95]

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

In May 2017, the WannaCry ransomware attack spread through the Internet, using an exploit vector named EternalBlue, which was allegedly leaked from the U.S. National Security Agency. The ransomware attack, unprecedented in scale,[96] infected more than 230,000 computers in over 150 countries,[97] using 20 different languages to demand money from users using Bitcoin cryptocurrency. WannaCry demanded US$300 per computer.[98] The attack affected Telefónica and several other large companies in Spain, as well as parts of the British National Health Service (NHS), where at least 16 hospitals had to turn away patients or cancel scheduled operations,[99] FedEx, Deutsche Bahn, Honda,[100] Renault, as well as the Russian Interior Ministry and Russian telecom MegaFon.[101] The attackers gave their victims a 7-day deadline from the day their computers got infected, after which the encrypted files would be deleted.[102]

Petya

Petya was first discovered in March 2016; unlike other forms of encrypting ransomware, the malware aimed to infect the master boot record, installing a payload which encrypts the file tables of the 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 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.[103]

On 27 June 2017, a heavily modified version of Petya was used for a global cyberattack primarily targeting Ukraine (but affecting many countries[104]). 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.[105][106]

Bad Rabbit

On 24 October 2017, some users in 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 believed the ransomware to have been distributed by a bogus update to Adobe Flash software.[107] Among agencies that were affected by the ransomware were: Interfax, Odesa International Airport, Kyiv Metro, and the Ministry of Infrastructure of Ukraine.[108] 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.[109] 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,[110] appending to CrowdStrike Bad Rabbit and NotPetya's DLL (dynamic link library) share 67 percent of the same code[111]) though the only identity to the culprits are the names of characters from the *Game of Thrones* series embedded within the code.[109]

Security experts found that the ransomware did not use the EternalBlue exploit to spread, and a simple method to inoculate an unaffected machine running older Windows versions was found by 24 October 2017.[112][113] 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.[109]

SamSam

In 2016, a new strain of ransomware emerged that was targeting JBoss servers.[114] This strain, named "SamSam", was found to bypass the process of phishing or illicit downloads in favor of exploiting vulnerabilities on weak servers.[115] The malware uses a Remote Desktop Protocol 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, the Colorado Department of Transportation, Davidson County, North Carolina, and most recently, a ransomware attack on the infrastructure of Atlanta.[115]

Mohammad Mehdi Shah Mansouri (born in Qom, Iran in 1991) and Faramarz Shahi Savandi (born in Shiraz, Iran, in 1984) are wanted by the FBI for allegedly launching SamSam ransomware.[116] The two have allegedly made $6 million from extortion and caused over $30 million in damages using the malware.[117]

DarkSide

On May 7, 2021 a cyberattack was executed on the US Colonial Pipeline. The Federal Bureau of Investigation identified DarkSide as the perpetrator of the Colonial Pipeline ransomware attack, perpetrated by malicious code, that led to a voluntary shutdown of the main pipeline supplying 45% of fuel to the East Coast of the United States. The attack was described as the worst cyberattack to date on U.S. critical infrastructure. DarkSide successfully extorted about 75 Bitcoin (almost US$5 million) from Colonial Pipeline. U.S. officials are investigating whether the attack was purely criminal or took place with the involvement of the Russian government or another state sponsor. Following the attack, DarkSide posted a statement claiming that "We are apolitical, we do not participate in geopolitics...Our goal is to make money and not creating problems for society."

On May 10, SentinelOne published an analysis (https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/) of the DarkSide Ransomware attack.

In May 2021, the FBI and Cybersecurity and Infrastructure Security Agency issued a joint alert urging the owners and operators of critical infrastructure to take certain steps to reduce their vulnerability to DarkSide ransomware and ransomware in general.

Syskey

Syskey is a utility that was included with Windows NT-based operating systems to encrypt the user account database, optionally with a password. The tool has sometimes been effectively used as ransomware during technical support scams—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.[118] Syskey was removed from later versions of Windows 10 and Windows Server in 2017, due to being obsolete and "known to be used by hackers as part of ransomware scams".[119][120]

Ransomware-as-a-service

Ransomware-as-a-service (RaaS) became a notable method after the Russia-based[121] or Russian-speaking[122] group REvil staged operations against several targets, including the Brazil-based JBS S.A. in May 2021, and the US-based Kaseya Limited in July 2021.[123] After a July 9, 2021 phone call between United States president Joe Biden and Russian president Vladimir Putin, Biden told the press, "I made it very clear to him that the United States expects when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is." Biden later added that the United States would take the group's servers down if Putin did not.[124][125] Four days later, REvil websites and other infrastructure vanished from the internet.[126]

Mitigation

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.[127][128]

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[26][129] As such, having a proper 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, it's also critical to maintain "offline" backups of data stored in locations inaccessible from any potentially infected computer, such as external storage drives or devices that do not have any access to any network (including the Internet), prevents them from being accessed by the ransomware. Moreover, if using a NAS or Cloud storage, then the computer should have append-only permission to the destination storage, such that it cannot delete or overwrite previous backups. According to comodo, applying two Attack Surface Reduction on OS/Kernel provides a materially-reduced attack surface which results in a heightened security posture.[130][131][132]

Installing security updates issued by software vendors can mitigate the vulnerabilities leveraged by certain strains to propagate.[133][134][135][136][137] Other measures include cyber hygiene – exercising caution when opening e-mail attachments and links, network segmentation, and keeping critical computers isolated from networks.[138][139] Furthermore, to mitigate the spread of ransomware measures of infection control can be applied.[140] Such may include disconnecting infected machines from all networks, educational programs,[141] effective communication channels, malware surveillance and ways of collective participation[140]

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 does not disable it.

- On Windows, the 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.[142] It is advised to add backup and other important directories to Controlled Folder Access.
- Unless malware gains root on the ZFS host system in deploying an attack coded to issue ZFS administrative commands, file servers running ZFS are broadly 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.[143] 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][144] 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 in the jargon of 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.[145] 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, Jigsaw, LambdaLocker, Legion, NoobCrypt, Stampado, SZFLocker, TeslaCrypt, XData.[146] The No More Ransom Project is an initiative by the Netherlands' police's National High Tech Crime Unit, Europol's European Cybercrime Centre, Kaspersky Lab and McAfee to help ransomware victims recover their data without paying a ransom.[147] They offer a free CryptoSheriff tool to analyze encrypted files and search for decryption tools.[148]

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.

Growth

Ransomware malicious software was first confined to one or two countries in Eastern Europe and subsequently spread across the Atlantic to the United States and Canada.[149] The number of cyberattacks during 2020 was double that of 2019.[150] The first versions of this type of malware used various techniques to disable the computers[149] by locking the victims system machine (Locker Ransomware) [133]. Ransomware uses different tactics to extort victims. One of the most common methods is locking the device's screen by displaying a message from a branch of local law enforcement alleging that the victim must pay a fine for illegal activity. The ransomware may request a payment by sending an SMS message to a premium rate number. Some similar variants of the malware display pornographic image content and demanded payment for the removal of it.[149]

In 2016, a significant uptick in ransomware attacks on hospitals was noted. According to the 2017 Internet Security Threat Report from Symantec Corp, ransomware affected not only IT systems but also patient care, clinical operations, and billing. Online criminals may be motivated by the money available and sense of urgency within the healthcare system.[151]

Ransomware is growing rapidly across the internet users but also for the IoT environment.[149] 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.[152]

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.[153] The common distribution method today is based on email campaigns.

The first reported death following a ransomware attack was at a German hospital in October 2020.[154]

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.

Criminal arrests and convictions

Zain Qaiser

A British student, Zain Qaiser, from Barking, London was jailed for more than six years at Kingston Crown Court for his ransomware attacks in 2019.[155] 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 Ransomware strain of the malicious Angler Exploit Kit (AEK)[156] 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 vouchers, and enter the code in the Reveton panel displayed on the screen. This money entered a MoneyPak account managed by Qaiser, who would then deposit the voucher payments into an American co-conspirator's debit card—that of Raymond Odigie Uadiale, who was then a student at Florida International University during 2012 and 2013 and later worked for Microsoft. Uadiale would convert the money into Liberty Reserve digital currency and deposit it into Qaiser's Liberty Reserve account.[157]

A breakthrough in this case occurred in May 2013 when authorities from several countries seized the Liberty Reserve servers, obtaining access to all its transactions and account history. Qaiser was running encrypted virtual machines on his Macbook Pro with both Mac and Windows operating systems.[158] 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 Wi-Fi to access his advertising

sites.) His lawyer claimed that Qaiser had suffered from mental illness.[155] Russian police arrested 50 members of the Lurk malware gang in June 2016.[159] Uadiale, a naturalized US citizen of Nigerian descent, was jailed for 18 months.[160]

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.[161] However, this provision was removed from the final version of the bill.[162] A minor in Japan was arrested for creating and distributing ransomware code.[163] Young and Yung have had the ANSI C source code to a ransomware cryptotrojan on-line, at cryptovirology.com, since 2005 as part of a 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.[164]

See also

- Colonial Pipeline ransomware attack – Ransomware attack on American oil pipeline system
- BlueKeep (security vulnerability)
- Hitler-Ransomware – Form of ransomware
- Jigsaw (ransomware)
- Append-only – Property of computer data storage
- Riskware
- Ryuk (ransomware) – Type of ransomware
- Reliability engineering – Sub-discipline of systems engineering that emphasizes dependability
- Air gap (networking) – Network security measure
- Data redundancy
- Double switching
- Fault tolerance – Resilience of systems to component failures or errors
- Reliability (computer networking)
- Unidirectional network – Network device that permits data flow in only one direction
- fault-tolerant computer system
- ZFS – File system
- Byzantine fault – Fault in a computer system that presents different symptoms to different observers
- Quantum Byzantine agreement
- Two Generals' Problem – Thought experiment

References

1. Young, A.; M. Yung (1996). *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676 (https://doi.org/10.1109%2FSECPRI.1996.502676). ISBN 0-8186-7417-2.

2. Schofield, Jack (28 July 2016). "How can I remove a ransomware infection?" (https://www.theguardian.com/technology/askjack/2016/jul/28/how-can-i-remove-ransomware-infection). *The Guardian*. Retrieved 28 July 2016.
3. Mimoso, Michael (28 March 2016). "Petya Ransomware Master File Table Encryption" (https://threatpost.com/petya-ransomware-encrypts-master-file-table/117024/). *threatpost.com*. Retrieved 28 July 2016.
4. Justin Luna (21 September 2016). "Mamba ransomware encrypts your hard drive, manipulates the boot process" (https://www.neowin.net/news/mamba-ransomware-encrypts-your-hard-drive-manipulates-the-boot-process). *Neowin*. Retrieved 5 November 2016.
5. Cameron, Dell (13 May 2017). "Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It" (https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/). *Gizmodo*. Retrieved 13 May 2017.
6. Dunn, John E. "Ransom Trojans spreading beyond Russian heartland" (https://web.archive.org/web/20140702211354/http://news.techworld.com/security/3343528/ransom-trojans-spreading-beyond-russian-heartland/). TechWorld. Archived from the original (http://news.techworld.com/security/3343528/ransom-trojans-spreading-beyond-russian-heartland/) on 2 July 2014. Retrieved 10 March 2012.
7. "New Internet scam: Ransomware..." (https://www.fbi.gov/news/stories/2012/august/new-internet-scam/new-internet-scam) FBI. 9 August 2012.
8. "Citadel malware continues to deliver Reveton ransomware..." (https://www.ic3.gov/media/2012/121130.aspx) Internet Crime Complaint Center (IC3). 30 November 2012.
9. "Ransomware back in big way, 181.5 million attacks since January" (https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/). *Help Net Security*. 11 July 2018. Retrieved 20 October 2018.
10. "Update: McAfee: Cyber criminals using Android malware and ransomware the most" (http://www.infoworld.com/t/security/mcafee-cyber-criminals-using-android-malware-and-ransomware-the-most-219916). *InfoWorld*. 3 June 2013. Retrieved 16 September 2013.
11. "Cryptolocker victims to get files back for free" (https://www.bbc.co.uk/news/technology-28661463). BBC News. 6 August 2014. Retrieved 18 August 2014.
12. "FBI says crypto ransomware has raked in >$18 million for cybercriminals" (https://arstechnica.com/security/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/). *Ars Technica*. 25 June 2015. Retrieved 25 June 2015.
13. "Internet Crime Report 2020" (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf) (PDF). *Ic3.gov*. Retrieved 1 March 2022.
14. "Ransomware's savage reign continues as attacks increase 105%" (https://www.helpnetsecurity.com/2022/02/18/rise-ransomware-attacks/). *Help Net Security*. 18 February 2022. Retrieved 20 April 2022.
15. Young, Adam L.; Yung, Moti (2017). "Cryptovirology: The Birth, Neglect, and Explosion of Ransomware" (https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext). **60** (7). Communications of the ACM: 24–26. Retrieved 27 June 2017.
16. "Ransomware squeezes users with bogus Windows activation demand" (http://www.computerworld.com/s/article/9215711/Ransomware_squeezes_users_with_bogus_Windows_activation_demand). *Computerworld*. 11 April 2011. Retrieved 9 March 2012.
17. "Police warn of extortion messages sent in their name" (http://www.hs.fi/english/article/Police+warn+of+extortion+messages+sent+in+their+name/1329103586716). *Helsingin Sanomat*. Retrieved 9 March 2012.

18. McMillian, Robert (31 August 2010). "Alleged Ransomware Gang Investigated by Moscow Police" (https://www.pcworld.com/article/204577/alleged_ransomware_gang_investigated_by_moscow_police.html). *PC World*. Retrieved 10 March 2012.
19. "Ransomware: Fake Federal German Police (BKA) notice" (http://www.securelist.com/en/blog/6155/Ransomware_Fake_Federal_German_Police_BKA_notice). SecureList (Kaspersky Lab). Retrieved 10 March 2012.
20. "And Now, an MBR Ransomware" (http://www.securelist.com/en/blog/208188032/And_Now_an_MBR_Ransomware). SecureList (Kaspersky Lab). Retrieved 10 March 2012.
21. Adam Young (2005). Zhou, Jianying; Lopez, Javier (eds.). "Building a Cryptovirus Using Microsoft's Cryptographic API". *Information Security: 8th International Conference, ISC 2005*. Springer-Verlag. pp. 389–401.
22. Young, Adam (2006). "Cryptoviral Extortion Using Microsoft's Crypto API: Can Crypto APIs Help the Enemy?". *International Journal of Information Security*. **5** (2): 67–76. doi:10.1007/s10207-006-0082-7 (https://doi.org/10.1007%2Fs10207-006-0082-7). S2CID 12990192 (https://api.semanticscholar.org/CorpusID:12990192).
23. Danchev, Dancho (22 April 2009). "New ransomware locks PCs, demands premium SMS for removal" (https://web.archive.org/web/20090426055732/http://blogs.zdnet.com/security/?p=3197). *ZDNet*. Archived from the original (http://blogs.zdnet.com/security/?p=3197) on 26 April 2009. Retrieved 2 May 2009.
24. "Ransomware plays pirated Windows card, demands $143" (http://www.computerworld.com/s/article/9219745/Ransomware_plays_pirated_Windows_card_demands_143). *Computerworld*. 6 September 2011. Retrieved 9 March 2012.
25. Cheng, Jacqui (18 July 2007). "New Trojans: give us $300, or the data gets it!" (https://arstechnica.com/security/news/2007/07/new-trojans-give-us-300-or-the-data-gets-it.ars). *Ars Technica*. Retrieved 16 April 2009.
26. "You're infected—if you want to see your data again, pay us $300 in Bitcoins" (https://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/). *Ars Technica*. 17 October 2013. Retrieved 23 October 2013.
27. "CryptoDefense ransomware leaves decryption key accessible" (http://www.computerworld.com/s/article/9247348/CryptoDefense_ransomware_leaves_decryption_key_accessible). *Computerworld*. IDG. April 2014. Retrieved 7 April 2014.
28. "What to do if Ransomware Attacks on your Windows Computer?" (https://archive.today/20160523092754/https://www.techiemotto.com/ransomware-attacks-windows-computer/75/). *Techie Motto*. Archived from the original (https://www.techiemotto.com/ransomware-attacks-windows-computer/75/) on 23 May 2016. Retrieved 25 April 2016.
29. Adam, Sally (12 May 2020). "The state of ransomware 2020" (https://news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/). *Sophos News*. Retrieved 18 September 2020.
30. Kassner, Michael. "Ransomware: Extortion via the Internet" (https://www.techrepublic.com/blog/security/ransomware-extortion-via-the-internet/2976). *TechRepublic*. Retrieved 10 March 2012.
31. Sebastiaan von Solms; David Naccache (1992). "On Blind 'Signatures and Perfect Crimes" (https://web.archive.org/web/20171026002327/https://pdfs.semanticscholar.org/67bb/82e6981239270d644e60e8f868b4f0752126.pdf) (PDF). *Computers & Security*. **11** (6): 581–583. doi:10.1016/0167-4048(92)90193-U (https://doi.org/10.1016%2F0167-4048%2892%2990193-U). S2CID 23153906 (https://api.semanticscholar.org/CorpusID:23153906). Archived from the original (https://pdfs.semanticscholar.org/67bb/82e6981239270d644e60e8f868b4f0752126.pdf) (PDF) on 26 October 2017. Retrieved 25 October 2017.
32. Schaibly, Susan (26 September 2005). "Files for ransom" (http://www.networkworld.com/buzz/2005/092605-ransom.html?page=3). Network World. Retrieved 17 April 2009.

33. Leyden, John (24 July 2006). "Ransomware getting harder to break" (http://theregister.co.uk/2006/07/24/ransomware/). *The Register*. Retrieved 18 April 2009.
34. Naraine, Ryan (6 June 2008). "Blackmail ransomware returns with 1024-bit encryption key" (https://web.archive.org/web/20080803000014/http://blogs.zdnet.com/security/?p=1251). *ZDNet*. Archived from the original (http://blogs.zdnet.com/security/?p=1251) on 3 August 2008. Retrieved 3 May 2009.
35. Lemos, Robert (13 June 2008). "Ransomware resisting crypto cracking efforts" (http://www.securityfocus.com/news/11523). SecurityFocus. Retrieved 18 April 2009.
36. Krebs, Brian (9 June 2008). "Ransomware Encrypts Victim Files with 1,024-Bit Key" (http://voices.washingtonpost.com/securityfix/2008/06/ransomware_encrypts_victim_fil.html). *The Washington Post*. Retrieved 16 April 2009.
37. "Kaspersky Lab reports a new and dangerous blackmailing virus" (http://www.kaspersky.com/news?id=207575650). Kaspersky Lab. 5 June 2008. Retrieved 11 June 2008.
38. Violet Blue (22 December 2013). "CryptoLocker's crimewave: A trail of millions in laundered Bitcoin" (https://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/). *ZDNet*. Retrieved 23 December 2013.
39. "Encryption goof fixed in TorrentLocker file-locking malware" (http://www.pcworld.com/article/2685432/encryption-goof-fixed-in-torrentlocker-filelocking-malware.html). *PC World*. 17 September 2014. Retrieved 15 October 2014.
40. "Cryptolocker 2.0 – new version, or copycat?" (http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/). *WeLiveSecurity*. ESET. 19 December 2013. Retrieved 18 January 2014.
41. "New CryptoLocker Spreads via Removable Drives" (https://web.archive.org/web/20161104095631/http://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/). Trend Micro. 26 December 2013. Archived from the original (http://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/) on 4 November 2016. Retrieved 18 January 2014.
42. "Synology NAS devices targeted by hackers, demand Bitcoin ransom to decrypt files" (https://web.archive.org/web/20140819084648/http://www.extremetech.com/extreme/187518-synology-nas-devices-targeted-by-hackers-demand-bitcoin-ransom-to-decrypt-files). *ExtremeTech*. Ziff Davis Media. Archived from the original (http://www.extremetech.com/extreme/187518-synology-nas-devices-targeted-by-hackers-demand-bitcoin-ransom-to-decrypt-files) on 19 August 2014. Retrieved 18 August 2014.
43. "File-encrypting ransomware starts targeting Linux web servers" (http://www.pcworld.com/article/3003098/business-security/file-encrypting-ransomware-starts-targeting-linux-web-servers.html). *PC World*. IDG. 9 November 2015. Retrieved 31 May 2016.
44. "Cybercriminals Encrypt Website Databases in "RansomWeb" Attacks" (http://www.securityweek.com/cybercriminals-encrypt-website-databases-%E2%80%9Cransomweb%E2%80%9D-attacks). *SecurityWeek*. Retrieved 31 May 2016.
45. "Hackers holding websites to ransom by switching their encryption keys" (https://www.theguardian.com/technology/2015/feb/03/hackers-websites-ransom-switching-encryption-keys). *The Guardian*. Retrieved 31 May 2016.
46. "The new .LNK between spam and Locky infection" (https://blogs.technet.microsoft.com/mmpc/2016/10/19/the-new-lnk-between-spam-and-locky-infection/). *Blogs.technet.microsoft.com*. 19 October 2016. Retrieved 25 October 2017.
47. Muncaster, Phil (13 April 2016). "PowerShell Exploits Spotted in Over a Third of Attacks" (https://www.infosecurity-magazine.com/news/powershell-exploits-spotted-over/).

48. "New ransomware employs Tor to stay hidden from security" (https://www.theguardian.com/technology/2014/jul/25/new-ransomware-employs-tor-onion-malware). *The Guardian*. Retrieved 31 May 2016.
49. "The current state of ransomware: CTB-Locker" (https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker/). *Sophos Blog*. Sophos. 31 December 2015. Retrieved 31 May 2016.
50. Brook, Chris (4 June 2015). "Author Behind Ransomware Tox Calls it Quits, Sells Platform" (https://threatpost.com/author-behind-ransomware-tox-calls-it-quits-sells-platform/113151). Retrieved 6 August 2015.
51. Dela Paz, Roland (29 July 2015). "Encryptor RaaS: Yet another new Ransomware-as-a-Service on the Block" (https://web.archive.org/web/20150802013442/http://blog.fortinet.com/post/encryptor-raas-yet-another-new-ransomware-as-a-service-on-the-block). Archived from the original (http://blog.fortinet.com/post/encryptor-raas-yet-another-new-ransomware-as-a-service-on-the-block) on 2 August 2015. Retrieved 6 August 2015.
52. "Symantec classifies ransomware as the most dangerous cyber threat – Tech2" (http://tech.firstpost.com/news-analysis/symantec-classifies-ransomware-as-the-most-dangerous-cyber-threat-336688.html). 22 September 2016. Retrieved 22 September 2016.
53. "Ransomware reportedly to blame for outage at US hospital chain" (https://www.theverge.com/2020/9/28/21482304/ransomware-outage-hospital-chain-cybersecurity). *The Verge*. 28 September 2020. Retrieved 28 September 2020.
54. Leyden, John. "Russian cops cuff 10 ransomware Trojan suspects" (https://www.theregister.co.uk/2010/09/01/ransomware_trojan_suspects_cuffed/). *The Register*. Retrieved 10 March 2012.
55. "Criminals push ransomware hosted on GitHub and SourceForge pages by spamming 'fake nude pics' of celebrities" (https://thenextweb.com/insider/2013/02/07/criminals-push-ransomware-hosted-on-github-and-sourceforge-pages-by-spamming-fake-nude-pics-of-celebrities/). *TheNextWeb*. 7 February 2013. Retrieved 17 July 2013.
56. "New OS X malware holds Macs for ransom, demands $300 fine to the FBI for 'viewing or distributing' porn" (https://thenextweb.com/apple/2013/07/16/new-os-x-malware-holds-macs-for-ransom-demands-300-fine-to-the-fbi-for-viewing-or-distributing-porn/). *TheNextWeb*. 15 July 2013. Retrieved 17 July 2013.
57. "Man gets ransomware porn pop-up, goes to cops, gets arrested on child porn charges" (https://arstechnica.com/tech-policy/2013/07/man-gets-ransomware-porn-pop-up-turns-self-in-on-child-porn-charges/). *Ars Technica*. 26 July 2013. Retrieved 31 July 2013.
58. Young, A. (2003). *Non-Zero Sum Games and Survivable Malware*. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop. pp. 24–29.
59. A. Young, M. Yung (2004). *Malicious Cryptography: Exposing Cryptovirology*. Wiley. ISBN 978-0-7645-4975-5.
60. Arntz, Pieter (10 July 2020). "Threat spotlight: WastedLocker, customized ransomware" (https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/). *Malwarebytes Labs*. Retrieved 27 July 2020.
61. Ricker, Thomas (27 July 2020). "Garmin confirms cyber attack as fitness tracking systems come back online" (https://www.theverge.com/2020/7/27/21339910/garmin-back-online-recovery-ransomeware). *The Verge*. Retrieved 27 July 2020.
62. "Ransomware on mobile devices: knock-knock-block" (https://blog.kaspersky.com/mobile-ransomware-2016/12491/). *Kaspersky Lab*. Retrieved 6 December 2016.
63. "Your Android phone viewed illegal porn. To unlock it, pay a $300 fine" (https://arstechnica.com/security/2014/05/your-android-phone-viewed-illegal-porn-to-unlock-it-pay-a-300-fine/). *Ars Technica*. 6 May 2014. Retrieved 9 April 2017.

64. "New Android ransomware uses clickjacking to gain admin privileges" (http://www.pcworld.com/article/3027123/new-android-ransomware-uses-clickjacking-to-gain-admin-privileges.html). *PC World*. 27 January 2016. Retrieved 9 April 2017.
65. "Here's How to Overcome Newly Discovered iPhone Ransomware" (http://fortune.com/2016/08/04/apple-iphone-ransomware/). *Fortune*. Retrieved 9 April 2017.
66. "Ransomware scammers exploited Safari bug to extort porn-viewing iOS users" (https://arstechnica.com/security/2017/03/ransomware-scammers-exploited-safari-bug-to-extort-porn-viewing-ios-users/). *Ars Technica*. 28 March 2017. Retrieved 9 April 2017.
67. Al-Hawawreh, Muna; den Hartog, Frank; Sitnikova, Elena (2019). "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things". *IEEE Internet of Things Journal*. **6** (4): 7137–7151. doi:10.1109/JIOT.2019.2914390 (https://doi.org/10.1109%2FJIOT.2019.2914390). S2CID 155469264 (https://api.semanticscholar.org/CorpusID:155469264).
68. Palmer, Danny. "This is how ransomware could infect your digital camera" (https://www.zdnet.com/article/this-is-how-ransomware-could-infect-your-digital-camera/). *ZDNet*. Retrieved 13 August 2019.
69. "Gardaí warn of 'Police Trojan' computer locking virus" (http://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/). *TheJournal.ie*. Retrieved 31 May 2016.
70. "Barrie computer expert seeing an increase in the effects of the new ransomware" (http://www.thebarrieexaminer.com/2013/03/07/barrie-computer-expert-seeing-an-increase-in-the-effects-of-the-new-ransomware). *Barrie Examiner*. Postmedia Network. Retrieved 31 May 2016.
71. "Fake cop Trojan 'detects offensive materials' on PCs, demands money" (https://www.theregister.co.uk/2012/04/05/police_themed_ransomware/). *The Register*. Retrieved 15 August 2012.
72. "Reveton Malware Freezes PCs, Demands Payment" (http://www.informationweek.com/security/attacks/reveton-malware-freezes-pcs-demands-paym/240005598). *InformationWeek*. Retrieved 16 August 2012.
73. Dunn, John E. "Police alert after ransom Trojan locks up 1,100 PCs" (https://web.archive.org/web/20140702202942/http://news.techworld.com/security/3373656/police-issue-alert-after-ransom-trojan-infects-1100-pcs/). TechWorld. Archived from the original (http://news.techworld.com/security/3373656/police-issue-alert-after-ransom-trojan-infects-1100-pcs/) on 2 July 2014. Retrieved 16 August 2012.
74. Constantian, Lucian (9 May 2012). "Police-themed Ransomware Starts Targeting US and Canadian Users" (https://www.pcworld.com/article/255303/policethemed_ransomware_starts_targeting_us_and_canadian_users.html). *PC World*. Retrieved 11 May 2012.
75. "Reveton 'police ransom' malware gang head arrested in Dubai" (https://web.archive.org/web/20141214021849/http://news.techworld.com/security/3426085/reveton-police-ransom-malware-gang-head-arrested-in-dubai/). *TechWorld*. Archived from the original (http://news.techworld.com/security/3426085/reveton-police-ransom-malware-gang-head-arrested-in-dubai/) on 14 December 2014. Retrieved 18 October 2014.
76. " 'Reveton' ransomware upgraded with powerful password stealer" (http://www.pcworld.com/article/2466980/reveton-ransomware-upgraded-with-powerful-password-stealer.html). *PC World*. 19 August 2014. Retrieved 18 October 2014.
77. "Disk encrypting Cryptolocker malware demands $300 to decrypt your files" (https://web.archive.org/web/20161104045318/http://www.geek.com/apps/disk-encryptiing-cryptolocker-malware-demands-300-to-decrypt-your-files-1570402/). *Geek.com*. 11 September 2013. Archived from the original (http://www.geek.com/apps/disk-encryptiing-cryptolocker-malware-demands-300-to-decrypt-your-files-1570402/) on 4 November 2016. Retrieved 12 September 2013.
78. Ferguson, Donna (19 October 2013). "CryptoLocker attacks that hold your computer to ransom" (https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware). *The Guardian*. Retrieved 23 October 2013.

79. "Destructive malware "CryptoLocker" on the loose – here's what to do" (https://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/). *Naked Security*. Sophos. 12 October 2013. Retrieved 23 October 2013.
80. "CryptoLocker crooks charge 10 Bitcoins for second-chance decryption service" (http://www.networkworld.com/community/node/84174). *NetworkWorld*. 4 November 2013. Retrieved 5 November 2013.
81. "CryptoLocker creators try to extort even more money from victims with new service" (http://www.pcworld.com/article/2060640/cryptolocker-creators-try-to-extort-even-more-money-from-victims-with-new-service.html). *PC World*. 4 November 2013. Retrieved 5 November 2013.
82. "Wham bam: Global Operation Tovar whacks CryptoLocker ransomware & GameOver Zeus botnet" (https://web.archive.org/web/20140703092912/http://blogs.computerworld.com/cybercrime-and-hacking/23980/wham-bam-global-operation-tovar-whacks-cryptolocker-ransomware-gameover-zeus-botnet). *Computerworld*. IDG. Archived from the original (http://blogs.computerworld.com/cybercrime-and-hacking/23980/wham-bam-global-operation-tovar-whacks-cryptolocker-ransomware-gameover-zeus-botnet) on 3 July 2014. Retrieved 18 August 2014.
83. "U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator" (https://www.justice.gov/opa/pr/2014/June/14-crm-584.html). *Justice.gov*. U.S. Department of Justice. Retrieved 18 August 2014.
84. "Australians increasingly hit by global tide of cryptomalware" (http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware). Symantec. Retrieved 15 October 2014.
85. Grubb, Ben (17 September 2014). "Hackers lock up thousands of Australian computers, demand ransom" (https://www.smh.com.au/it-pro/security-it/hackers-lock-up-thousands-of-australian-computers-demand-ransom-20140917-10hyyh.html). *Sydney Morning Herald*. Retrieved 15 October 2014.
86. "Australia specifically targeted by Cryptolocker: Symantec" (http://www.arnnet.com.au/article/556598/australia-specifically-targeted-by-cryptolocker-symantec/). *ARNnet*. 3 October 2014. Retrieved 15 October 2014.
87. "Scammers use Australia Post to mask email attacks" (https://www.smh.com.au/digital-life/consumer-security/scammers-use-australia-post-to-mask-email-attacks-20141015-10ru0s.html). *Sydney Morning Herald*. 15 October 2014. Retrieved 15 October 2014.
88. Steve Ragan (7 October 2014). "Ransomware attack knocks TV station off air" (http://www.csoonline.com/article/2692614/malware-cybercrime/ransomware-attack-knocks-tv-station-off-air.html). *CSO*. Retrieved 15 October 2014.
89. "Over 9,000 PCs in Australia infected by TorrentLocker ransomware" (http://www.cso.com.au/article/562658/over-9-000-pcs-australia-infected-by-torrentlocker-ransomware/). *CSO.com.au*. 17 December 2014. Retrieved 18 December 2014.
90. "Malvertising campaign delivers digitally signed CryptoWall ransomware" (http://www.pcworld.com/article/2688992/malvertising-campaign-delivers-digitally-signed-cryptowall-ransomware.html). *PC World*. 29 September 2014. Retrieved 25 June 2015.
91. "CryptoWall 3.0 Ransomware Partners With FAREIT Spyware" (http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/). Trend Micro. 20 March 2015. Retrieved 25 June 2015.
92. Andra Zaharia (5 November 2015). "Security Alert: CryptoWall 4.0 – new, enhanced and more difficult to detect" (https://heimdalsecurity.com/blog/security-alert-cryptowall-4-0-new-enhanced-and-more-difficult-to-detect/). *HEIMDAL*. Retrieved 5 January 2016.
93. "Ransomware on mobile devices: knock-knock-block" (https://blog.kaspersky.com/mobile-ransomware-2016/12491/). *Kaspersky Lab*. Retrieved 4 December 2016.

94. "The evolution of mobile ransomware" (https://blog.avast.com/the-evolution-of-mobile-ransomware). *Avast*. Retrieved 4 December 2016.
95. "Mobile ransomware use jumps, blocking access to phones" (http://www.pcworld.com/article/3090049/security/mobile-ransomware-use-jumps-blocking-access-to-phones.html). *PCWorld*. IDG Consumer & SMB. 30 June 2016. Retrieved 4 December 2016.
96. "Cyber-attack: Europol says it was unprecedented in scale" (https://www.bbc.com/news/world-europe-39907965). *BBC News*. 13 May 2017. Retrieved 13 May 2017.
97. " 'Unprecedented' cyberattack hits 200,000 in at least 150 countries, and the threat is escalating" (https://www.cnbc.com/2017/05/14/cyber-attack-hits-200000-in-at-least-150-countries-europol.html). CNBC. 14 May 2017. Retrieved 16 May 2017.
98. "The real victim of ransomware: Your local corner store" (https://www.cnet.com/news/wannacry-ransomware-real-victim-small-business-local-corner-store/). *CNET*. Retrieved 22 May 2017.
99. Marsh, Sarah (12 May 2017). "The NHS trusts hit by malware – full list" (https://www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware). *The Guardian*. Retrieved 12 May 2017.
100. "Honda halts Japan car plant after WannaCry virus hits computer network" (https://www.reuters.com/article/us-honda-cyberattack-idUSKBN19C0EI). *Reuters*. 21 June 2017. Retrieved 21 June 2017.
101. "The Latest: Russian Interior Ministry is hit by cyberattack" (https://www.wthr.com/article/news/world/the-latest-russian-interior-ministry-is-hit-by-cyberattack-0/531-887e72b5-1310-48a2-ac46-ec9a3da10515). *WTHR*.
102. Scott, Paul Mozur, Mark; Goel, Vindu (19 May 2017). "Victims Call Hackers' Bluff as Ransomware Deadline Nears" (https://www.nytimes.com/2017/05/19/business/hacking-malware-wanncry-ransomware-deadline.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 22 May 2017.
103. Constantin, Lucian. "Petya ransomware is now double the trouble" (http://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html). *NetworkWorld*. Retrieved 27 June 2017.
104. "Ransomware Statistics for 2018 | Safety Detective" (https://www.safetydetective.com/blog/ransomware-statistics/). *Safety Detective*. 23 October 2018. Retrieved 20 November 2018.
105. "Tuesday's massive ransomware outbreak was, in fact, something much worse" (https://arstechnica.com/security/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/). *Ars Technica*. 28 June 2017. Retrieved 28 June 2017.
106. "Cyber-attack was about data and not money, say experts" (https://www.bbc.com/news/technology-40442578). *BBC News*. 29 June 2017. Retrieved 29 June 2017.
107. " 'Bad Rabbit' ransomware strikes Ukraine and Russia" (https://www.bbc.com/news/technology-41740768). *BBC*. 24 October 2017. Retrieved 24 October 2017.
108. Hern, Alex (25 October 2017). "Bad Rabbit: Game of Thrones-referencing ransomware hits Europe" (https://www.theguardian.com/technology/2017/oct/25/bad-rabbit-game-of-thrones-ransomware-europe-notpetya-bitcoin-decryption-key). *Theguardian.com*. Retrieved 25 October 2017.
109. Larson, Selena (25 October 2017). "New ransomware attack hits Russia and spreads around globe" (https://money.cnn.com/2017/10/24/technology/bad-rabbit-ransomware-attack/index.html). *CNN*. Retrieved 25 October 2017.
110. "BadRabbit: a closer look at the new version of Petya/NotPetya" (https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/). *Malwarebytes Labs*. 24 October 2017. Retrieved 31 July 2019.

111. Palmer, Danny. "Bad Rabbit: Ten things you need to know about the latest ransomware outbreak" (https://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/). *ZDNet*. Retrieved 31 July 2019.
112. Cameron, Dell (24 October 2017). " 'Bad Rabbit' Ransomware Strikes Russia and Ukraine" (https://gizmodo.com/bad-rabbit-ransomware-strikes-russia-and-ukraine-1819814538). *Gizmodo*. Retrieved 24 October 2017.
113. Palmer, Danny (24 October 2017). "Bad Rabbit ransomware: A new variant of Petya is spreading, warn researchers" (https://www.zdnet.com/article/bad-rabbit-ransomware-a-new-variant-of-petya-is-spreading-warn-researchers/). *ZDNet*. Retrieved 24 October 2017.
114. Rashid, Fahmida Y. (19 April 2016). "Patch JBoss now to prevent SamSam ransomware attacks" (https://www.infoworld.com/article/3058254/security/patch-jboss-now-to-prevent-samsam-ransomware-attacks.html). *InfoWorld*. IDG. Retrieved 23 July 2018.
115. Crowe, Jonathan (March 2018). "City of Atlanta Hit with SamSam Ransomware: 5 Key Things to Know" (https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam). *Barkley vs Malware*. Barkley Protects, Inc. Retrieved 18 July 2018.
116. Federal Bureau of Investigation, *Wanted by the FBI: SamSam Subjects* (https://www.fbi.gov/wanted/cyber/samsam-subjects/samsam-subjects-fbi-wanted-8-5x11.pdf) (PDF), U.S. Department of Justice, retrieved 5 October 2019
117. "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses" (https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public) (Press release). United States Department of Justice. 28 November 2018. Retrieved 11 December 2018.
118. Whittaker, Zack. "We talked to Windows tech support scammers. Here's why you shouldn't" (https://www.zdnet.com/article/why-you-should-never-talk-to-windows-tech-support-scammers/). *ZDNet*. Retrieved 6 November 2019.
119. "Windows 10 Fall Creators Update: syskey.exe support dropped" (https://www.ghacks.net/2017/06/26/windows-10-fall-creators-update-no-support-for-syskey-exe/). *gHacks*. 26 June 2017. Retrieved 6 November 2019.
120. "Syskey.exe utility is no longer supported in Windows 10, Windows Server 2016 and Windows Server 2019" (https://support.microsoft.com/en-hk/help/4025993/syskey-exe-utility-is-no-longer-supported-in-windows-10-windows-server). Microsoft. Retrieved 6 November 2019.
121. "Russian-based ransomware group 'REvil' disappears after hitting US businesses" (https://www.independent.co.uk/news/world/americas/us-politics/revil-ransomware-russia-us-latest-b1883490.html). *The Independent*. 13 July 2021.
122. "Prolific ransomware gang suddenly disappears from internet. The timing is noteworthy" (https://www.nbcnews.com/tech/tech-news/russian-speaking-ransomware-gang-goes-offline-rcna1403). *NBC News*.
123. "McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service - The All-Stars" (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/). 2 October 2019.
124. "Biden tells Putin Russia must crack down on cybercriminals" (https://apnews.com/article/joe-biden-europe-technology-government-and-politics-russia-df7ef73f02bcba61ad6e628aa95a9f84). *AP NEWS*. 9 July 2021.
125. Sanger, David E. (13 July 2021). "Russia's most aggressive ransomware group disappeared. It's unclear who disabled them" (https://ghostarchive.org/archive/20211228/https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html). *The New York Times*. Archived from the original (https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html) on 28 December 2021.

126. Business, Brian Fung, Zachary Cohen and Geneva Sands, CNN (13 July 2021). "Ransomware gang that hit meat supplier mysteriously vanishes from the internet" (https://www.cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html). *CNN*.
127. Cannell, Joshua (8 October 2013). "Cryptolocker Ransomware: What You Need To Know, last updated 06/02/2014" (https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/). *Malwarebytes Unpacked*. Archived (https://web.archive.org/web/20210930200636/https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/) from the original on 30 September 2021. Retrieved 19 October 2013.
128. Leyden, Josh. "Fiendish CryptoLocker ransomware: Whatever you do, don't PAY" (https://www.theregister.com/2013/10/18/cryptolocker_ransmware). *The Register*. Archived (https://web.archive.org/web/20210813214911/https://www.theregister.com/2013/10/18/cryptolocker_ransmware) from the original on 13 August 2021. Retrieved 18 October 2013.
129. "Cryptolocker Infections on the Rise; US-CERT Issues Warning" (https://www.securityweek.com/cryptolocker-infections-rise-us-cert-issues-warning). *SecurityWeek*. 19 November 2013. Archived (https://web.archive.org/web/20210527161032/https://www.securityweek.com/cryptolocker-infections-rise-us-cert-issues-warning) from the original on 27 May 2021. Retrieved 18 January 2014.
130. Metin, Ozer. "Applying attack surface reduction" (https://techtalk.comodo.com/2020/10/10/applying-attack-surface-reduction-on-top-of-attack-surface-reduction-asr2/). Comodo Cybersecurity. Archived (https://web.archive.org/web/20211005003825/https://techtalk.comodo.com/2020/10/10/applying-attack-surface-reduction-on-top-of-attack-surface-reduction-asr2/) from the original on 5 October 2021. Retrieved 27 August 2020.
131. "Overview of attack surface reduction capabilities" (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide). Microsoft. Archived (https://web.archive.org/web/20211118052451/https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide) from the original on 18 November 2021. Retrieved 6 February 2020.
132. "Comodo's patented "Kernel API Virtualization" – Under the Hood" (https://techtalk.comodo.com/2020/08/17/comodos-patented-kernel-api-virtualization-under-the-hood/). Comodo Cybersecurity. Archived (https://web.archive.org/web/20211004234110/https://techtalk.comodo.com/2020/08/17/comodos-patented-kernel-api-virtualization-under-the-hood/) from the original on 4 October 2021. Retrieved 27 August 2020.
133. " 'Petya' Ransomware Outbreak Goes Global" (https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/). *krebsonsecurity.com*. Krebs on Security. Retrieved 29 June 2017.
134. "How to protect yourself from Petya malware" (https://www.cnet.com/how-to/petya-goldeneye-malware-ransomware-protect-yourself-against/). *CNET*. Retrieved 29 June 2017.
135. "Petya ransomware attack: What you should do so that your security is not compromised" (http://economictimes.indiatimes.com/tech/internet/petya-ransomware-attack-what-you-should-do-so-that-your-security-is-not-compromised/articleshow/59357161.cms). *The Economic Times*. 29 June 2017. Retrieved 29 June 2017.
136. "New 'Petya' Ransomware Attack Spreads: What to Do" (https://www.tomsguide.com/us/petya-ransomware-attack,news-25389.html). Tom's Guide. 27 June 2017. Retrieved 29 June 2017.
137. "India worst hit by Petya in APAC, 7th globally: Symantec" (http://economictimes.indiatimes.com/tech/internet/india-worst-hit-by-petya-in-apac-7th-globally-symantec/articleshow/59367013.cms). *The Economic Times*. 29 June 2017. Retrieved 29 June 2017.
138. "TRA issues advice to protect against latest ransomware Petya | The National" (http://www.thenational.ae/uae/technology/tra-issues-advice-to-protect-against-latest-ransomware-petya). 29 June 2017. Retrieved 29 June 2017.

139. "Petya Ransomware Spreading Via EternalBlue Exploit « Threat Research Blog" (https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html). FireEye. Retrieved 29 June 2017.
140. Chang, Yao-Chung (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait* (https://books.google.com/books?id=8HsK_QZBIpkC&pg=PR9). Edward Elgar Publishing. ISBN 9780857936684. Retrieved 30 June 2017.
141. "Infection control for your computers: Protecting against cyber crime - GP Practice Management Blog" (https://practiceindex.co.uk/gp/blog/it-technology/infection-control-for-your-computers-protecting-against-cyber-crime/). *GP Practice Management Blog*. 18 May 2017. Retrieved 30 June 2017.
142. "How to Turn On Ransomware Protection in Windows 10" (https://windowsloop.com/turn-on-ransomware-protection-windows-10/). *WindowsLoop*. 8 May 2018. Retrieved 19 December 2018.
143. "Defeating CryptoLocker Attacks with ZFS" (https://www.ixsystems.com/blog/defeating-cryptolocker). *ixsystems.com*. 27 August 2015.
144. "List of free Ransomware Decryptor Tools to unlock files" (https://www.thewindowsclub.com/list-ransomware-decryptor-tools). *Thewindowsclub.com*. Retrieved 28 July 2016.
145. "Emsisoft Decrypter for HydraCrypt and UmbreCrypt Ransomware" (https://www.thewindowsclub.com/emsisoft-decrypter-hydracrypt-umbrecrypt-ransomware). *Thewindowsclub.com*. 17 February 2016. Retrieved 28 July 2016.
146. "Ransomware removal tools" (https://www.avast.com/c-ransomware). Retrieved 19 September 2017.
147. "About the Project - The No More Ransom Project" (https://www.nomoreransom.org/en/about-the-project.html). Archived (https://web.archive.org/web/20211122131432/https://www.nomoreransom.org/en/about-the-project.html) from the original on 22 November 2021. Retrieved 3 December 2021.
148. "Crypto Sheriff - The No More Ransom Project" (https://www.nomoreransom.org/crypto-sheriff.php). Archived (https://web.archive.org/web/20211026165032/https://www.nomoreransom.org/crypto-sheriff.php) from the original on 26 October 2021. Retrieved 3 December 2021.
149. O'Gorman, G.; McDonald, G. (2012), *Ransonmware: A Growing Menace* (https://www.01net.it/whitepaper_library/Symantec_Ransomware_Growing_Menace.pdf) (PDF), Symantec Security Response, Symantec Corporation, retrieved 5 October 2019
150. Cyberattack Report ArcTitan (18 February 2021). "Phishing Emails Most Common Beginning of Ransomware Attack" (https://www.arctitan.com/blog/phishing-emails-most-common-beginning-of-ransomware-attack/). *ArcTitan*. Retrieved 29 March 2021.
151. Robeznieks, A. (2017). "Ransomware Turning Healthcare Cybersecurity Into a Patient Care Issue" (https://web.archive.org/web/20170616193656/https://www.hfma.org/Content.aspx?id=54012). *Healthcare Business News*. Healthcare Financial Management Association. Archived from the original (https://www.hfma.org/Content.aspx?id=54012) on 16 June 2017.
152. Heater, Brian (13 April 2016), "The Growing Threat of Ransomware" (http://www.cdsystems.com/docs/PcMagRansomware.pdf) (PDF), *PC Magazine*, retrieved 5 October 2019
153. "Activity begins to drop, but remains a challenge for organizations" (https://www.symantec.com/security-center/threat-report), *Internet Security Threat Report (ISTR) 2019*, Symantec Corporation, vol. 24, p. 16, 2019, retrieved 5 October 2019
154. *First death reported following a ransomware attack on a German hospital* (https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/), ZDNet, retrieved 5 October 2020
155. "Zain Qaiser: Student jailed for blackmailing porn users worldwide" (https://www.bbc.com/news/uk-47800378). *BBC News*. 9 April 2019.

156. "British hacker Zain Qaiser sentenced for blackmailing millions" (https://www.teiss.co.uk/zain-qaiser-cyber-crime/). 9 April 2019.
157. Cimpanu, Catalin. "Reveton ransomware distributor sentenced to six years in prison in the UK" (https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/). *ZDNet*.
158. "How police caught the UK's most notorious porn ransomware baron" (https://www.wired.co.uk/article/porn-ransomware-reveton), Matt Burgess, *Wired*, 12 Apr 2019]
159. "Angler by Lurk: Why the infamous cybercriminal group that stole millions was renting out its most powerful tool" (https://usa.kaspersky.com/about/press-releases/2016_angler-by-lurk-why-the-infamous-cybercriminal-group-that-stole-millions-was-renting-out-its-most-powerful-tool). *usa.kaspersky.com*. 26 May 2021.
160. Francisco, Shaun Nichols in San. "Florida Man laundered money for Reveton ransomware. Then Microsoft hired him" (https://www.theregister.com/2018/08/15/reveton_microsoft_hire/). *Theregister.com*.
161. Fields, Logan M. (25 February 2017). "The Minority Report – Week 7 – The Half-Way Point" (http://www.d-worldnews.life/2017/02/the-minority-report-week-7-half-way.html). World News.
162. "Maryland Ransomware Bill Makes Attacks Felonies" (http://www.netsec.news/maryland-ransomware-bill-makes-attacks-felonies). Network Security News. 15 February 2017.
163. Wei, Wang (6 June 2017). "14-Year-Old Japanese Boy Arrested for Creating Ransomware" (http://thehackernews.com/2017/06/japanese-ransomware-malware.html). The Hacker News.
164. Young, Adam L.; Yung, Moti (2005). "An Implementation of Cryptoviral Extortion Using Microsoft's Crypto API" (http://www.cryptovirology.com/cryptovfiles/newbook/Chapter2.pdf) (PDF). Cryptovirology Labs. Retrieved 16 August 2017.

Further reading

- Young, A.; Yung, M. (2004). *Malicious Cryptography: Exposing Cryptovirology*. Wiley. ISBN 978-0-7645-4975-5.
- Russinovich, Mark (7 January 2013). "Hunting Down and Killing Ransomware" (http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx). *Microsoft TechNet*. Microsoft.
- Simonite, Tom (4 February 2015). "Holding Data Hostage: The Perfect Internet Crime? Ransomware (Scareware)" (http://www.technologyreview.com/news/534516/holding-data-hostage-the-perfect-internet-crime/). *MIT Technology Review*.
- Brad, Duncan (2 March 2015). "Exploit Kits and CryptoWall 3.0" (https://web.archive.org/web/20150924083938/http://www.rackspace.com/blog/exploit-kits-and-cryptowall-3-0/). The Rackspace Blog! & NewsRoom. Archived from the original (http://www.rackspace.com/blog/exploit-kits-and-cryptowall-3-0/) on 24 September 2015. Retrieved 15 April 2015.
- "Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat" (https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise). *NEWS*. Federal Bureau of Investigation. 20 January 2015.
- Yang, T.; Yang, Y.; Qian, K.; Lo, D.C.T.; Qian, L. & Tao, L. (2015). *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*. IEEE Internet of Things Journal, CONFERENCE, AUGUST 2015. pp. 1338–1343. doi:10.1109/HPCC-CSS-ICESS.2015.39 (https://doi.org/10.1109%2FHPCC-CSS-ICESS.2015.39). ISBN 978-1-4799-8937-9. S2CID 5374328 (https://api.semanticscholar.org/CorpusID:5374328).
- Richet, Jean-Loup (July 2015). "Extortion on the Internet: the Rise of Crypto-Ransomware" (https://blogs.harvard.edu/jeanlouprichet/files/2015/07/Extortion_on_the_Internet_Rise_of_Crypto_Ra

nsomware.pdf) (PDF). Harvard University.
- Liska, Allan (20 October 2021). "Ransomware - Understand. Prevent. Recover" (https://ransomware.org/). *Recorded Future*. ActualTech Media.

External links

- Media related to Ransomware at Wikimedia Commons
- Incidents of Ransomware on the Rise (https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise) – Federal Bureau of Investigation

---