
Cover Page

DOI: http://ijmer.in.doi./2022/11.01.84

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(5), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

RANDOMWARE

S. Radha Krishna
Lecturer in Computer Science
B.R. R & G.K. R Chambers Degree College, L. R. Peta
Palakol, W.G. Dist, Andhra Pradesh, India

Ransomware definition

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

How ransomware works

There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. If you want the technical details, the Infosec Institute has a great in-depth look at how several flavors of ransomware encrypt files. But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.

In some forms of malware, the attacker might claim to be a law enforcement agency shutting down the victim's computer due to the presence of pornography or pirated software on it, and demanding the payment of a "fine," perhaps to make victims less likely to report the attack to authorities. But most attacks don't bother with this pretense. There is also a variation, called leakware or doxware, in which the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. But because finding and extracting such information is a very tricky proposition for attackers, encryption ransomware is by far the most common type.

Who is a target for ransomware?

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it's a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet — and these organizations may be uniquely sensitive to leakware attacks.

But don't feel like you're safe if you don't fit these categories: as we noted, some ransomware spreads automatically and indiscriminately across the internet.

How to prevent ransomware

There are a number of defensive steps you can take to prevent ransomware infection. These steps are a of course good security practices in general, so following them improves your defenses from all sorts of attacks:

- Keep your **operating system patched and up-to-date** to ensure you have fewer vulnerabilities to exploit.
- Don't **install software or give it administrative privileges** unless you know exactly what it is and what it does.


Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(5), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

DOI: http://ijmer.in.doi./2022/11.01.84

- Install **antivirus software**, which detects malicious programs like ransomware as they arrive, and **whitelisting software,** which prevents unauthorized applications from executing in the first place.
- And, of course, **back up your files,** frequently and automatically! That won't stop a malware attack, but it can make the damage caused by one much less significant.

Ransomware removal

If your computer has been infected with ransomware, you'll need to regain control of your machine. CSO's Steve Ragan has a great video demonstrating how to do this on a Windows 10 machine:

SECURITY DEFINITION

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This class of malware is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message or website. It has the **ability to lock a computer screen or encrypt important, predetermined files with a password**.

Examples of Ransomware

Scareware is the simplest type of ransomware. It uses scare tactics or intimidation to trick victims into paying up. It can come in the form of fake antivirus software in which a message suddenly appears claiming your computer has various issues and an online payment is necessary to fix them!

The level of this type of attack varies. Sometimes, users may be bombarded with endless alerts and pop-up messages. Other times, the computer will fail to work at all. Yet, another type of ransomware can impersonate a law enforcement agency by opening up a page that appears to be from a local law enforcement office and claiming the computer user was caught performing illegal activities online. Files are then locked in hard-to-crack, encrypted files, making it difficult for users to recover unless the ransom is paid.

Typical attacks usually ask for $100 to $200. Other attacks seek much more, especially if the attacker knows the data being held hostage would be can cause a significant direct financial loss to a company. As a result, cybercriminals who set up these scams can make big sums of money.

No matter what the scenario, even if the ransom is paid, there is no guarantee that computer users will be able to fully access their systems again. While some hackers' direct victims to pay through Bitcoin, MoneyPak or other online methods, attackers could also demand credit card data, adding another level of financial loss.

History of Ransomware

The first cases were reported in Russia in 2005. However, since then, the scams have spread throughout the world, with new types still successfully targeting victims. In September 2013, Crypto Locker surfaced and targeted all versions of Windows! It has successfully infected hundreds of thousands of personal computers and business systems. Victims unknowingly opened up emails impersonating customer support services from FedEx, UPS, DHS and other companies. Once activated, the malware's onscreen timer demanded an average payment of $300 within 72 hours. Some versions affected local files and removable media. The United States Computer Emergency Response Team warned the malware had the ability to jump from machine to machine and advised infected computer users to immediately remove infected machines from their networks.

Kaspersky security experts have been able to decrypt hijacked data, but they admit it isn't always possible if the encryption is very strong, as is the case with Crypto Locker. It is essential for private users and businesses to regularly back up their computers to prevent the loss of important data.

Prevention and Removal

Computer users should make sure their firewalls are on, avoid questionable websites and be alert when opening any suspicious email messages. Choosing proven antivirus software from a reputable company can help protect your computer against the latest ransomware threats.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(5), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

DOI: http://ijmer.in.doi./2022/11.01.84

History of Ransomware Attacks

Ransomware can be traced back to 1989 when the "AIDS virus" was used to extort funds from recipients of the ransomware. Payments for that attack were made by mail to Panama, at which point a decryption key was also mailed back to the user.

In 1996, ransomware was known as "cryptoviral extortion," introduced by Moti Yung and Adam Young from Columbia University. This idea, born in academia, illustrated the progression, strength, and creation of modern cryptographic tools. Young and Yung presented the first cryptovirology attack at the 1996 IEEE Security and Privacy conference. Their virus contained the attacker's public key and encrypted the victim's files. The malware then prompted the victim to send asymmetric ciphertext to the attacker to decipher and return the decryption key—for a fee.

Attackers have grown creative over the years by requiring payments that are nearly impossible to trace, which helps cybercriminals remain anonymous. For example, notorious mobile ransomware Fusob requires victims to pay using Apple iTunes gift cards instead of normal currencies, like dollars.

Ransomware attacks began to soar in popularity with the growth of cyptocurrencies, such as Bitcoin. Cryptocurrency is a digital currency that uses encryption techniques to verify and secure transactions and control the creation of new units. Beyond Bitcoin, there are other popular cryptocurrencies that attackers prompt victims to use, such as Ethereum, Litecoin, and Ripple.
Ransomware has attacked organizations in nearly every vertical, with one of the most famous viruses being the attacks on Presbyterian Memorial Hospital. This attack highlighted the potential damage and risks of ransomware. Labs, pharmacies and emergency rooms were hit.

Social engineering attackers have become more innovative over time. The Guardian wrote about a situation where new ransomware victims were asked to have two other users install the link and pay a ransom in order to have their files decrypted.

Examples of Ransomware

By learning about the major ransomware attacks below, organizations will gain a solid foundation of the tactics, exploits, and characteristics of most ransomware attacks. While there continues to be variations in the code, targets, and functions of ransomware, the innovation in ransomware attacks is typically incremental.

- **WannaCry**—A powerful Microsoft exploit was leveraged to create a worldwide ransomware worm that infected over 250,000 systems before a kill switch was tripped to stop its spread. Proofpoint was involved in finding the sample used to find the kill switch and in deconstructing the ransomware. Learn more about Proofpoint's involvement in stopping WannaCry.
- **Crypto Locker**—This was one of the first of the current generation of ransomware that required cryptocurrency for payment (Bitcoin) and encrypted a user's hard drive and attached network drives. Crypto locker was spread via an email with an attachment that claimed to be FedEx and UPS tracking notifications. A decryption tool was released for this in 2014. But various reports suggest that upwards of $27 million was extorted by Crypto Locker.
- **NotPetya**—Considered one of the most damaging ransomware attacks, NotPetya leveraged tactics from its namesake, Petya, such as infecting and encrypting the master boot record of a Microsoft Windows-based system. NotPetya leveraged the same vulnerability from WannaCry to spread rapidly, demanding payment in bitcoin to undo the changes. It has been classified by some as a wiper, since NotPetya cannot undo its changes to the master boot record and renders the target system unrecoverable.
- **Bad Rabbit**—Considered a cousin of NotPetya and using similar code and exploits to spread, Bad Rabbit was a visible ransomware that appeared to target Russia and Ukraine, mostly impacting media companies there. Unlike NotPetya, Bad Rabbit did allow for decryption if the ransom was paid. The majority of cases indicate that it was spread via a fake Flash player update that can impact users via a drive by attack.

How Ransomware Works

Ransomware is a type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems. The two most prevalent types of ransomwares are encryptors and screen lockers. Encryptors, as the name implies, encrypt data on a system, making the content useless without the decryption key. Screen lockers, on the other hand, simply block access to the system with a "lock" screen, asserting that the system is encrypted.

Victims are often notified on a lock screen (common to both encryptors and screen lockers) to purchase a cryptocurrency, like Bitcoin, to pay the ransom fee. Once the ransom is paid, customers receive the decryption key and may attempt to decrypt files. Decryption is not guaranteed, as multiple sources report varying degrees of success with decryption after paying ransoms. Sometimes

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(5), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

DOI: http://ijmer.in.doi./2022/11.01.84

victims never receive the keys. Some attacks install malware on the computer system even after the ransom is paid and the data is released.

While originally focused largely on personal computers, encrypting ransomware has increasingly targeted business users, as businesses will often pay more to unlock critical systems and resume daily operations than individuals.

Enterprise ransomware infections or viruses usually start with a malicious email. An unsuspecting user opens an attachment or clicks on a URL that is malicious or has been compromised.

At that point, a ransomware agent is installed and begins encrypting key files on the victim's PC and any attached file shares. After encrypting the data, the ransomware displays a message on the infected device. The message explains what has occurred and how to pay the attackers. If the victims pay, the ransomware promises they'll get a code to unlock their data.

Ransomware Prevention and Detection

Prevention for ransomware attacks typically involves setting up and testing backups as well as applying ransomware protection in security tools. Security tools such as email protection gateways are the first line of defense, while endpoints are a secondary defense. Intrusion Detection Systems (IDSs) are sometimes used to detect ransomware command-and-control to alert against a ransomware system calling out to a control server. User training is important, but user training is just one of several layers of defense to protect against ransomware, and it comes into play after the delivery of ransomware via an email phish.

A fallback measure, in case other ransomware preventative defenses fail, is to stockpile Bitcoin. This is more prevalent where immediate harm could impact customers or users at the affected firm. Hospitals and the hospitality industry are at particular risk of ransomware, as patients' lives could be affected or people could be locked in or out of facilities.

Before / After

How to Prevent Ransomware Attacks

- **Defend your email against Ransomware**—Email phishing and spam are the main way that ransomware attacks are distributed. Secure Email Gateways with targeted attack protection are crucial for detecting and blocking malicious emails that deliver ransomware. These solutions protect against malicious attachments, malicious documents, and URLs in emails delivered to user computers.
- **Defend your mobile devices against Ransomware**—Mobile attack protection products, when used in conjunction with mobile device management (MDM) tools, can analyze applications on users' devices and immediately alert users and IT to any applications that might compromise the environment.
- **Defend your web surfing against Ransomware**—Secure web gateways can scan users' web surfing traffic to identify malicious web ads that might lead them to ransomware.
- **Monitor your server, network and back up key systems**—Monitoring tools can detect unusual file access activities, viruses, network C&C traffic and CPU loads, possibly in time to block ransomware from activating. Keeping a full image copy of crucial systems can reduce the risk of a crashed or encrypted machine causing a crucial operational bottleneck.

How to Remove Ransomware

- **Call federal and local law enforcement**—Just as someone would call a federal agency for a kidnapping, organizations need to call the same bureau for ransomware. Their forensic technicians can ensure systems aren't compromised in other ways, gather information to better protect organizations going forward and try to find the attackers.

Ransomware Recovery

- **Learn about anti-ransomware resources**—No More Ransom portal and Bleeping Computer have tips, suggestions and even some decryptors for selected ransomware attacks.
- **Restore data**—If organizations have followed best practices and kept system backups, they can restore their systems and resume normal operations.

Ransomware Statistics

The following ransomware statistics illustrate the rising epidemic and the billions it has cost victims. To stay up to date on the latest ransomware statistics, you can also check out the Proofpoint blog.


Cover Page




INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(5), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

DOI: http://ijmer.in.doi./2022/11.01.84

4,000

An average of 4,000 ransomware episodes occurs every day. Source: FBI Internet Crime Report

39%

Ransomware is the top variety of malicious software, found in 39% of cases where malware was identified. Source: Verizon's 2018 Data Breach Investigations Report

46%

In our latest State of the Phish™ Report, only 46% of respondents could correctly define ransomware.

42%

of U.S. respondents to our 2017 User Risk Report could not correctly identify what ransomware is.

Ransomware Survival Guide

Ransomware attackers collected more than $209 million from victims during the first three months of 2016 alone, with the volume of attacks 10 times higher than all of 2015. In addition to the ransom itself, these attacks can exact a heavy cost: business disruption, remediation costs, and a diminished brand.