6 best practices for escaping ransomware

A complete guide to tackling ransomware attacks.

ManageEngine
IT Management, Simplified

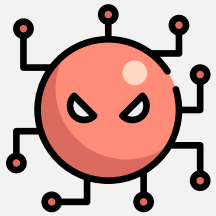
Contents

Cyberattacks

A cyberattack is an offensive act targeting computers, networks, or other devices in an attempt to either steal, encrypt, or destroy information on a system or network. A nation, state, individual, organization, or group may orchestrate an attack. There are different types of cyberattacks, including DDoS attacks, brute force attacks, phishing, Hacking, watering hole attacks, ransomware attacks, and more. But if we look closely, most cyberattacks follow one of five general strategies

Of these strategies, number five has gained popularity recently. This strategy is used by ransomware attacks, most notably the WannaCry attack that began on May 12, 2017. WannaCry started rapidly breaching networks around the globe, and infected over 400,000 computers across 150 countries, with England's National Health Service (NHS) being the primary victim of this cyberattack.

Bombard networks with one type of malware around the clock.



Unleash different forms of malware to breach networks.

Break into the weakest network first.

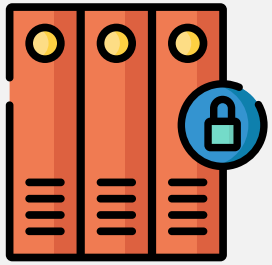
Sneak in, grab data, and take off.

Encrypt files and extort victims to make money.

What is ransomware?

Ransomware is a type of malware that encrypts a system and then extorts money from the users or the entire organization. Basically, ransomware encrypts the victim's files, restricting the user from using their own files or documents, or locks the computer to prevent normal usage and demands payment as ransom to decrypt the files and provide access.

Prevents you from accessing your files and folders.



Completely locks you out of your system.

Demands ransom to restore your system to working order.

Type of ransomware?

People often get confused about the different types of ransomware and their abilities to encrypt files. There are currently three main types of ransomware, but as newer versions come along, other variants may show up. The three types of ransomware are:

1. **Encryption ransomware**
2. **Lock screen ransomware**
3. **Master boot record ransomware**

Encryption ransomware

This ransomware encrypts your files and folders, preventing you from accessing your files by locking them with an AES-256 key, which is notoriously tough to decipher. Depending on the hacker's motive, the encrypted files may or may not be recoverable. After encrypting your files and folders, encryption ransomware displays a pop-up message explaining that your files have been encrypted and you must pay a ransom to have those documents decrypted. This is the method WannaCry used against its victims.

Lock screen ransomware

As the name implies, lock screen ransomware locks your screen and demands a ransom. While this type of ransomware won't encrypt your files, it will block all your windows straightaway. Once your system is infected, you won't be able to access your windows until you pay the ransom or the hackers lift the attack.

Master boot record ransomware

The master boot record (MBR) is an essential part of a hard drive, allowing the operating system to boot up. MBR ransomware changes the MBR, interrupting the normal boot process by displaying a demand for ransom on the boot up screen. Users can't even boot their systems up until the ransom is payed. Of all three types of ransomware, this ransomware is arguably the most dangerous.

The ransomware Petya was initially launched as master boot record ransomware, but after its immediate discovery by security professionals, Petya was upgraded and released as a new variant called Wiper. As the name implies, this variant will completely wipe your entire hard drive and leave you empty-handed with a blank system.

How does ransomware work?

Unlike other cyberattacks, ransomware actually locks away victims' data rather than stealing or destroying it. Recently, encryption ransomware has been the most publicized type of ransomware. Most ransomware enters a network either through email attachments, social networks, or malicious sites.

WannaCry infected systems through email attachments, but then used a known Windows vulnerability, EternalBlue, to propagate within networks. This propagation technique sets WannaCry apart from most encryption ransomware, in that its exposure wasn't limited to machines that directly downloaded the malicious file.

Let's break down the typical encryption ransomware workflow into five stages

1. A user downloads a malicious file from a web page or an email.
2. The downloaded file contains the ransomware, which begins infecting the user's system.
3. Some ransomware types will spread to other systems on the network if the network contains vulnerabilities.
4. The ransomware will prevent access in some way. Many encryption ransomware versions will encrypt users' files across the network with AES-256, a one-time key.
5. The ransomware creates a unique key for each file that was encrypted (these are used for decrypting the files once the ransom is paid).

Motive behind these ransomware attacks

Generally, the main motive behind any ransomware attack is to make money. With many iterations of ransomware demanding payment in Bitcoin or other cryptocurrencies, tracking the creators is often difficult. Although WannaCry is the most prolific ransomware attack to date, it's likely the hackers behind the attack could have profited even more. It's estimated that organizations across the world collectively paid more than $80,000 to decrypt their data before security researcher Marcus Hutchins discovered WannaCry's kill switch.

Doing some simple math, consider an organization that has 3,000 systems and their entire network becomes encrypted by ransomware. Hackers demand the organization pay $200 per system to decrypt their files. That means the organization could theoretically end up paying $600,000 in ransom. Looking at this from hackers' perspective, they can make a lot of money in a short period of time if just a few organizations pay to get their files back.

Should you pay the ransom or not?

Paying a ransom to hackers is never going to keep your network safe. Even if an organization decides to pay the ransom to decrypt their files, hackers may use this money to create new malware or ransomware and start attacking the organization again. It's clear that paying the ransom is a one-time solution to an ongoing problem.

All in all, security experts recommend victims avoid paying ransoms, and instead try to prevent attacks in the first place. In this case, a good defense truly is the best offense. What organizations should do is use proactive measures to prevent any future ransomware threats, like the solutions listed in the next section.

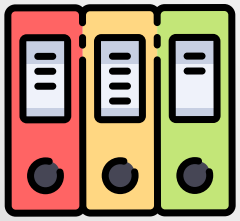
More importantly, paying the ransom to an unknown entity doesn't ensure your encrypted data will be decrypted. On a similar note, paying to get your files back doesn't necessarily mean your data is secure. Even if hackers decrypt your data, there is no assurance that the data was not copied or stored elsewhere, which means hackers could use your confidential information for future threats.

Best practices to stay vigilant against ransomware

Now that we have seen what not to do in response to ransomware attacks, let's take a look at what you should do to stay safe. Here are six simple steps to protect your data from cyber attacks

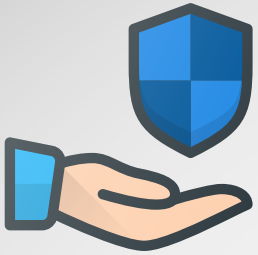
1. Educate users about phishing attacks.

Cybercriminals often send seemingly innocent emails to users, luring them to download attachments so hackers can infect their systems and infiltrate their network. Enterprises need to properly educate users and employees about phishing attacks, stressing that they should not download unwanted attachments from random email addresses.



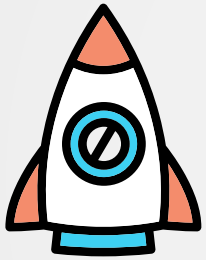
2. Back up your files regularly.

The best way to keep your data safe is by backing up your systems regularly. With backups in place, ransomware attacks won't be able to interrupt the regular business flow. And make sure the backup is restricted to read/write permissions so no one gets an undue opportunity to modify or delete your data. Once you've backed up your files, make sure to check on the status of those backups periodically to detect any breaches immediately.



3. Architect your security.

Divide your network into macro zones and micro zones to prevent hackers from accessing confidential information. Separate your computers based on critical, moderate, and low priority, and provide security levels based on network importance. For example, protect your servers more securely than your least important user computers or devices.



4. Employ deception technology.

If the data in your organization has to be secured at all costs, then implement deception technology to stay safe against potential data breaches. Deception technology is the practice of deploying a decoy system outside of your firewall, confusing hackers with fake data. With deception technology like honeypots, your security team can identify threats based on multiple breaches at one time, all without compromising your confidential data. Once you've identified the threat, your organization can defend itself against the attack accordingly.

5. Regularly patch your operating systems.

Even if you have all the above security measures in place, your network may still be suspectible to ransomware attacks if your operating systems are out-of-date. To evade ransomware completely, you need to keep your Windows, Mac, and Linux systems up-to-date at all times. Deploy missing patches immediately to stay secure.

6. Update your third-party applications.

On top of your operating systems, you need to make sure your third-party applications are updated as well. If, for example, a vulnerability exists in your design department through an application like Adobe Photoshop, hackers can use this vulnerability to breach your network and start infiltrating other systems. With that being said, leave no holes unpatched.

Real-world scenario: Responding to WannaCry and Petya

Once word broke about the WannaCry and Petya attacks, our team at UEM Central immediately reached out to customers with a defense plan. We first asked customers to block the vulnerable SMB ports that WannaCry and Petya were using to spread across networks. After successfully blocking those ports, we urged clients to deploy any missing patches to their Windows systems. Once customers ensured that all their systems were up-to-date, they were able to unblock the vulnerable SMB ports. Just by going through a few short steps, our customers were able to protect their entire network from these two serious ransomware attacks.

If ransomware has already breached your network, the best strategy is to reduce the spread of malware by blocking any affected SMB ports and updating other systems in your network. Regardless of these immediate measures, having proper backups is the best way to prevent ransomware from becoming a major headache for your enterprise. When it comes to things like backups, you can either be reactive or proative in securing your network for ransomware. Most security professionals agree that being proactive is always better, and will help you stay protected.

Combat ransomware attacks with ManageEngine

Cybercrime is evolving fast, so make sure you have the right solution in place to stay vigilant and safe. ManageEngine offers four different solutions to tackle ransomware attacks based on your network's structure and other needs. Mitigate attacks both proactively and reactively to keep your organization's data safe.

All the solutions below help in correcting vulnerabilities automatically, keeping your network secured 24/7.

UEM Central

An endpoint management solution that helps in managing servers, desktops, laptops, smartphones, and tablets, all from one central location.

FREE TRIAL

Patch Manager Plus

An exclusive patch management solution that helps in managing Windows, Mac, Linux, and over 250 third-party applications from one central location.

FREE TRIAL

Desktop Central MSP

An endpoint management solution designed for managed service providers (MSPs).

FREE TRIAL

Patch Connect Plus

Automatic third-party patch management for Microsoft SCCM.

FREE TRIAL

Benefits

Employ any of the above solutions and experience hassle-free endpoint management.

- ✓ Prevent future ransomware attacks
- ✓ Reduce security breaches
- ✓ Minimize downtime
- ✓ Keep corporate data secure
- ✓ Avoid data loss
- ✓ Maintain productivity
- ✓ Sustain brand image, reputation, and customer satisfaction

K. Ryan Coe,
I.T. Network Manager

“UEM Central has become an valuable tool in our enviroment.
The setup was a snap, I had the server up, running, and installing agents across my network within an hour. Keeping our computers updated, safe, and secure, protects us as well as our customers. Having the ability to push patches, updates, install and remove programs en masse, allows me to focus on other projects and areas.”

Try UEM Central

UEM Central is a unified endpoint management solution that helps in managing thousands of servers, desktops, and mobile devices from a central location. It automates the complete desktop and mobile device management life cycle, ranging from a simple system configuration to complex software deployment. Used by more than 6,000 customers around the globe, UEM Central helps businesses cut costs on IT infrastructure, achieve operational efficiency, improve productivity, and combat network vulnerabilities.

For more information, please visit **www.manageengine.com/products/desktop-central**.

Also available in

Windows Azure Marketplace | awsmarketplace

Integration with other products

SPICEWORKS | servicenow | ManageEngine ServiceDesk Plus

About ManageEngine

ManageEngine is bringing IT together for IT teams that need to deliver real-time services and support. Worldwide, established and emerging enterprises—including more than 60 percent of the Fortune 500—rely on our real-time IT management tools to ensure tight business-IT alignment and optimal performance of their IT infrastructure, including networks, servers, applications, desktops, and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the United States, India, Singapore, Japan, and China. For more information, please visit buzz.manageengine.com/; follow the company blog at blogs.manageengine.com/, on Facebook at www.facebook.com/ManageEngine and on Twitter @ManageEngine.

Giridhara Raam is a product expert at ManageEngine, a division of Zoho Corp. He works with the endpoint management team, marketing **UEM Central** and ManageEngine's Free Windows Admin Tools. Meanwhile, he also immerses himself in cybersecurity research from an endpoint management context.

IT Management, Simplified