Ontrack®

# A definitive guide to ransomware

## The ransomware epidemic

Ransomware incursions have reached epidemic proportions. According to a survey by cybersecurity and backup firm Datto, one in five small to medium-sized businesses fell victim to a ransomware attack in 2019. The consequences of a ransomware attack can be dire: from an organisation finding itself locked out of its enterprise data for weeks, to deletion of entire databases, massive reputational damage, and the loss of customer trust.

Cyber Security Ventures states that, in 2019, a new organisation fell victim to ransomware every 14 seconds, with a prediction that by 2021 this will increase to every 11 seconds. In 2018, the FBI received 1,493 complaints about ransomware with victims incurring losses on average of $3,621,857 – but that only counts the actual ransom payments, not the fallout. The City of Atlanta, for example, spent around $2.6 million on its recovery efforts from a ransomware demand of about $52,000.

In 2019, a business fell victim to a ransomware attack every 14 seconds.

The leading provider of human-driven phishing defence solutions, PhishMe, claims that over the past two years, ransomware attacks have risen by over 97%; a big reason for organisations to have a renewed emphasis on comprehensive and up-to-date backups.

However, organisations' backup files are often incomplete, neglected or in some cases, infected with the same ransomware that attacks the primary systems. If backups fail to provide adequate recovery, further response mechanisms include data recovery techniques such as decryption tools, recovery of logical data directly from storage devices and sending media to a lab where technicians attempt to extract as much information as possible.

## What is ransomware?

Ransomware is a type of malware that encrypts or otherwise locks users out of their files. When users try to access their data, they receive a notice demanding the payment of a ransom to regain its use.

Around since the 1980s, the last decade has seen various ransomware trojans crop up, but the real opportunity for attackers has ramped up since the introduction of Bitcoin.

This cryptocurrency allows attackers to collect money from their victims without going through traditional channels.

## How much does ransomware cost an organisation?

Figures from Datto show that ransomware costs businesses on average, $75 billion a year; this includes the ransom itself, subsequent recovery efforts, organisational and IT initiatives to protect the organisation from further attacks, as well as downtime, forensic investigation, training costs, restoration, and loss of revenue/productivity.

More conservative estimates by Cybersecurity Ventures places ransomware damage at more than $11.5 billion in 2019, which is a startling rise from a modest $325 million four years ago. Whether the figure is

$75 billion or $11.5 billion, the devastation is very real to those experiencing ransomware. In May of 2019, for example, the City of Baltimore was shut out of government systems for over a month. Vital systems for vaccine production, ATMs, airports, and hospitals were all impacted. Although the ransomware demand was $76,000, the recovery price tag amounted to nearly $20 million.

## Who is behind ransomware?

Those behind ransomware attacks are usually highly knowledgeable scammers with expertise in computer programming.

Typically, ransomware infects computers via an email attachment, network or infected browser.

## How does ransomware attack?

### Spear-Phishing

The most common delivery system for ransomware is a phishing email that includes an attachment or a link. When the user opens the attachment or clicks the link, the ransomware runs a program that locks the system, and displays a demand for payment. When this happens, the only way to decrypt the data is through a mathematical key only known by the attacker.

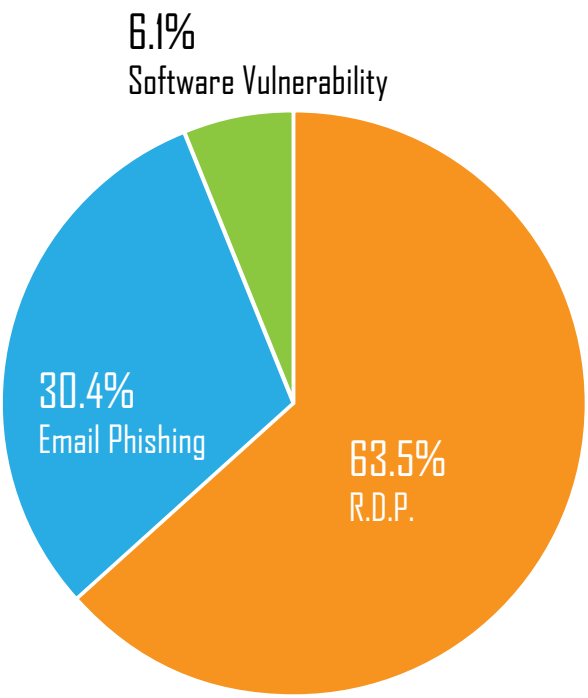
There have also been cases where malware will display a message claiming that the user's 'Windows' is locked. The user is then encouraged to call a "Microsoft" phone number and enter a six-digit code to reactivate the system. The message alleges that the phone call is free, but this isn't true. While on the phone calling the fake 'Microsoft', the user racks up long-distance call charges.

### Remote access points

McAfee researchers observed while cybercriminals are still using spear-phishing tactics, an increasing number of attacks are gaining access to a company that has open and exposed remote access points, such as RDP and virtual network computing (VNC).

RDP credentials can be brute-forced, obtained from password leaks, or simply purchased in underground markets.

Where past ransomware criminals would set up a command and control environment for the ransomware and decryption keys, most criminals now approach victims with ransom notes that include an anonymous email service address, allowing bad actors to remain better hidden.




*Source: Coveware - https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases*

## New ransomware families

According to the latest McAfee threat report, in the first quarter of 2019, ransomware attacks grew by 118%. Not only was there a significant rise in the number of attacks, but the year also saw new ransomware families appearing, and cyber criminals using more innovative techniques to cause chaos. Some of the major ransomware variants to cause major disruption over the year few years are described below.

### Anatova

A discovery for 2019 was the ransomware, Anatova. This new ransomware family disguises itself as the icon of a game or application to trick the user into downloading it.

An extremely advanced form of malware, it adapts quickly and uses evasion and spreading techniques to prevent its discovery. Due to its modular design, it can embed additional functions allowing it to thwart anti-ransomware methods. Fortunately, the McAfee Advanced Threat Research team discovered this new ransomware family in early 2019 before it became a significant threat.

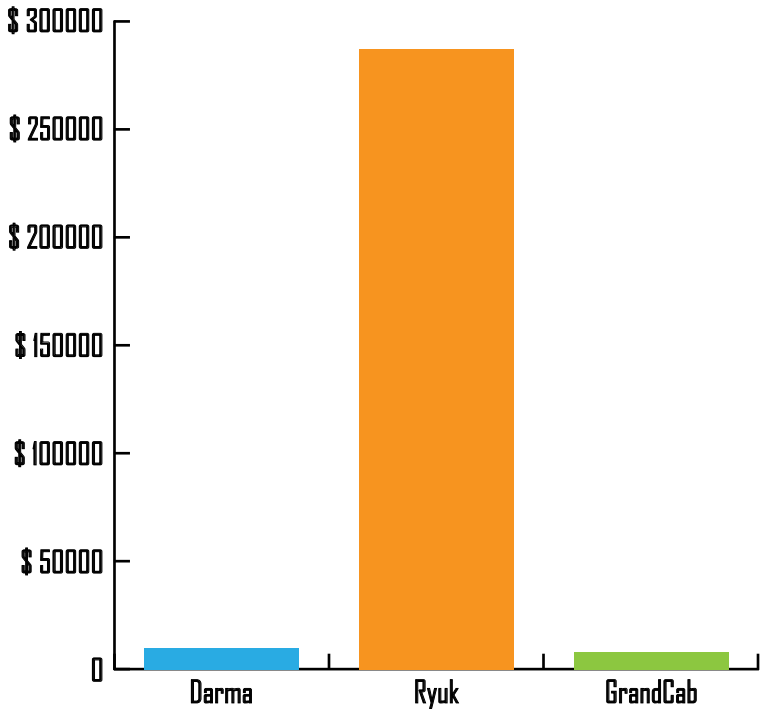
### Dharma

A variant of CrySiS, Dharma ransomware has been around since 2018, but cybercriminals continue to release new variants, which are impossible to decrypt.

### GandCrab

A malicious ransomware that uses AES encryption and drops a file called 'GandCrab.exe' onto the system. GandCrab targets consumers and businesses with PCs running Microsoft Windows.

On May 31st, 2019, the cybercriminals behind GandCrab sent an announcement saying they were stopping all further GandCrab ransomware attacks claiming they had received over $2 billion in ransom payments and they were "…leaving for a well-deserved retirement." (Reference: https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/).



### Emotet

Emotet was first discovered in 2014 as a trojan used to steal banking credentials. More recently, cybercriminals use it as a dropper of other trojans. It has introduced several advanced capabilities over the years due to its modular structure, including an installation module, banking module, and DDoS module. Emotet is mainly distributed through phishing emails using various social engineering techniques.

### Ryuk

Ryuk specifically targets large organisations for high-financial return. According to CrowdStrike, between August 2018 and January 2019, Ryuk netted over 705.80 bitcoins across 52 transactions totaling a value of $3,701,893.98. It first turned heads with its attack on Tribune Publishing's operations over the Christmas period of 2018. At first, the company thought the attack was just a server outage, but it was soon clear it was the Ryuk ransomware.

Another term for ransomware such as Ryuk that targets large enterprises for high ROI is 'big game hunting.' These large-scale attacks involve detailed customisation of campaigns to best suit the individual targets, increasing the effectiveness of the attacks. 'Big game hunting' therefore requires much more work from the hacker; it is also normally launched in phases.

For example, phase one might be a phishing attack with an aim to infect an enterprises network with malware to map the system and identify crucial assets to target. Phases two and three will then be a series of extortion and ransom attacks.

## How to prevent ransomware

Due to the continued success of phishing, user training is very much a front-line defence against ransomware. Standard IT security practices and technologies such as anti-virus, anti-malware, intrusion detection/prevention, firewalls, network monitoring, and access controls must also be in place.

User training is very much a front-line defence against ransomware.

Organisations should close any ports that do not need internet access, and those that do should be carefully watched and protected. More recently, machine learning and heuristics programmes have appeared on the market that can scan for ransomware behaviour such as encryption by unauthorised programmes. Backed up by threat intelligence and other safeguards, a vigilant IT department can limit the possibility of an incursion.

In addition, further layers of protection must be in place, such as regular backups. These backups must be comprehensive, must be easily accessible and organisations should test them regularly to verify reliability.

Unfortunately, ransomware continually evolves and finds new ways to infect systems. Sometimes it attacks specific systems or databases. The malware often begins by using stolen administrator rights to disable online backups, especially on SANs. Then, the malware will delete NAS systems. At other times, it manages to infiltrate and encrypt backup files, too. Virtualised backup applications such as Veeam, for example, have been a target of ransomware attacks in the past. It isn't a case, then, of if it will strike, but

when.

Organisations need to be prepared. Tapes that remain in a tape library system have the potential to be overwritten, encrypted or otherwise corrupted by ransomware. Air gap backups would eliminate the possibility of further infection if the original backup was free from malware.

Specific best practices have evolved, detailing actions to initiate if ransomware strikes. A significant principle is never to pay the ransom. The FBI is a firm advocate of non-payment, and the U.S. Conference of Mayors had all its members pledge never to pay a ransom to cybercriminals. After all, those who satisfy ransom demands have no guarantee of the decryption of their files. They may also be asked to pay more money, or they may find their data and systems now riddled with other types of malware.

Along with not paying the ransom, victims should immediately contact law enforcement. Organisations should shut down and disconnect any impacted systems from the network immediately, and always clone critical disks before making any changes. Once an organisation detects an attack, no time should be lost. Otherwise, the infection could spread to more users, systems and applications.

The last few years have seen the development of new programmes that are able to decrypt certain strains of ransomware. An organisations' IT department should contact providers or law enforcement to see if their infection can easily be decrypted. These days, there are over 100 decryption tools that can be used against more than 400 ransomware variants.

Case in point: the FBI released the master decryption keys for the GandCrab ransomware to enable victims to decrypt.

Note, however, that cybercriminals endeavour to stay one step ahead. When one strain can be effectively decrypted, they begin developing an altered strain to make it undecryptable. Once an infection is contained, backups are traditionally the best way to recover data.

Adequate backup files, whether from the cloud, backup applications or tape, permit the organisation to get back up and running. But care should be taken with backup files to ensure they were not subject to infection. Restoring files that contain ransomware will lead to reinfection of IT systems. Further, backups are notorious for either being incomplete, out of date or even corrupted.

## Top ransomware prevention tips

### 1 Email security is king

According to McAfee, phishing email continues to be one of the main entry points for ransomware viruses, especially in the case of targeted attacks. Therefore, securing this primary source of vulnerability is essential to everybody who runs a network or connects to the internet.

Most individuals trigger a ransomware attack by opening, what looks like, a normal email that contains the virus in a document, photo, video or other type of file. Most hackers today don't need much knowledge to insert a piece of malware into a file; there are numerous articles and YouTube tutorials with step-by-step instruction on how to do it.

**Top prevention tips**

1. Email security is king
2. Make your network and IT environment secure
3. Employee education
4. Secure your organisation's Remote Desktop Protocol (RDP)
5. Ensure you have an up-to-date backup

With this in mind, you should always avoid opening an email from an unknown sender. If you receive an email from an unknown source, inform your company data security advisor or IT team immediately.

Remember: Keeping your company's IT systems and data secure is always the right decision.

## 2 Make your network and IT environment secure

When ransomware infects a single computer it is undoubtedly a serious problem. But, when it spreads throughout the network, it can become a nightmare for the IT department and endanger the entire business.

Companies that have not already done so should consider implementing a data security software program, which checks all incoming emails before the intended recipient receives them. Such a solution will dramatically reduce the risk that a virus spreads inside a company network. Additionally, IT administrators and management should consider implementing network security software, which automatically monitors the network and its files for threats. The solution will also alert administrators if a ransomware attack is trying to encrypt vast quantities of files over the network.

Last but not least: Always update your software and operating systems with the latest patches, whenever they are available. As pointed out so often, hackers are only successful with their attacks when the victim has gaps in their data security policies.

## 3 Employee education

Even experienced computer users get into a panic when they realise they are facing a ransomware attack. It is therefore important that every employee in a company knows exactly what to do if a ransomware attack occurs, even high-level execs and IT Directors.

Protocols for handling a ransomware attack should not only be part of a business continuity plan for higher management or IT experts but precise guidelines on what to do when an infection occurs should be visible and understood in every office. These can be simple, but effective, for example:

- Disconnect computers from the internet and internal network
- Try to shut down the infected device properly and immediately call IT security/IT administration

## 4 Secure your organisation's Remote Desktop Protocol (RDP)

If your organisation doesn't need to use a RDP, then it's best if you replace it with a more secure solution. If this is not possible, then the following measures should be put in place:

- Use a VPN to access your organisations RDP as this creates a secure connection between an organisations' employees and the internet. All data traffic is sent through an encrypted virtual tunnel, which should prevent cybercriminals from being able to brute force a system
- Ensure you have two-factor authentication set up
- Those employees that service important internal services should have the maximum access required to be able to complete their job. Any employee that accesses critical systems or backups should have two-factor authentication set up
- Have an up-to-date disaster recovery plan in place to ensure if your RDP is compromised, you have a backup of all critical data.

### 5 Ensure you have an up-to-date backup

Protecting yourself also means having a backup of your data. A highly secure backup is a crucial element in preparing your organisation for a ransomware attack. You should test your backup thoroughly and frequently, but most importantly, it must also be easy to restore data.

This means that if you are hit by any form of malware you will be able to rebuild your system quickly and hassle-free. If possible, make sure that your backup system is not connected to your network (or only for the time when it's needed), this will prevent your backup being affected by malware as well.

## What should you do if you're hit by ransomware?

If for some reason, ransomware gets through your defensive line, you should do the following:

- **Never pay the ransom!**
  Paying the criminals doesn't guarantee that you will get your data back. In many cases (and most definitely, if it is a 'ranscam' or wiper malware) you will not get your data back, leaving you with no data and a lot less money!
- **Do not try to decrypt the data by yourself.**
  Some computer specialists may have the capabilities to recover lost data, but it is risky – if something goes wrong, you could destroy your data forever.
- **Check your backup!**
  Even if your backup is missing after a ransomware attack, you should never rule out the possibility of recovery. Possible solutions depend on the type of media or storage system, and the type of ransomware.

## Data recovery from Veeam backup

Veeam is the market leader for virtual machine backups. Many organisations rely on virtual machines in their data centres and implement backup through Veeam software products.

Organisations should take extra care to protect virtual, physical and cloud-based servers, NAS devices and more.

Typically, midsize and large organisations place their backups on dedicated volumes on MS NTFS / ReFS file systems. Smaller businesses often use external NAS systems with Linux Ext3/Ext4/XFS/BTRFS/ZFS.

Veeam Software is a reliable and secure method of backing up. However, since ransomware is so prevalent today—and is prone to target backup data, organisations should take extra care to protect virtual, physical and cloud-based servers, NAS devices and more.

## How to prevent ransomware attacks on Veeam backup files

Ontrack advises that organisations:

- Implement a backup and recovery plan for all critical data using the 3-2-1 strategy:
  3. Retain a minimum of three copies of data
  2. Store data on two different types of media
  1. Secure one copy of your backups offsite
- Test backups regularly to ensure proper configuration, which will limit the impact of a data breach and accelerate the recovery process
- Isolate critical backups from the network (air gap) for maximum protection
- Implement copy-on-write file systems (NetApp WAFL – Linux ZFS) or WORM features in NAS systems or appliances
- Patch critical operating systems, antivirus, security, and backup software as soon as possible
- Establish ongoing cybersecurity training for users and admins to identify phishing emails

## How Ontrack can help

If ransomware gets through the network perimeter and a full backup is not available, data recovery may still be possible. Each scenario requires a different approach to data recovery. However, only global vendors with a proven track record with enterprise systems should be trusted.

Ontrack has extensive experience in recovering data from all major storage platforms and media. As a point of firm policy, Ontrack will never pay a ransom. Instead, it endeavours to recover all possible data using advanced techniques. Ontrack has exceptional in-house expertise, facilities and tools required for comprehensive enterprise data recovery.

Each scenario requires a different approach to data recovery.

## Ontrack can recover from Veeam backups

Ontrack fully supports the recovery of VMware, vSphere, and Microsoft Hyper-V integrated with the Veeam environment. Ontrack has years of specialised expertise and has developed proprietary software to recover data from Veeam backup files.

As a result, Ontrack can recover data from a significant amount of Veeam jobs—even in cases where malware has corrupted the file.

Our exclusive recovery methods address damaged VBK, VIB, VBM files and others.

Case study

## A €400,000 ransom and 100 servers

A top European exhibition company experienced a cyber-attack where 100 of its servers were partially encrypted. With a ransom of €400,000 demanded, both the federal police and an international team of Cybersecurity and IT-Forensic experts were involved, but both failed to identify the ransomware type. It was determined that the customer had been directly targeted, and nothing like it had been seen before.

The customer had an IBM SAN with 50 drives, and after forensic analysis, it was found that data inside the LUNs were either deleted or overwritten. This affected six LUNs that were 25TB each and had different file systems – four ReFS and two with NTFS.

The Ontrack engineers managed to repair the logical damage to the point that a 100% recovery of the ReFS file system was achieved. Ontrack's in house development team then created custom tools to piece together the NTFS file system and reduplicate the database, so that data from a Veeam backup could be extracted and delivered on an ongoing basis to the customer.

Case study

## How NetApp technology helped Ontrack solve a ransomware infection

A laptop that was connected to a corporate network was the target of a Cryptolocker ransomware attack. The malware infected a CIFS volume that was set up as a file share on a NetApp FAS encrypting the majority of the files. Due to the IT team not being notified until after the expiration of the backup retention period, all backup files were affected.

The total impact of the ransomware resulted in inaccessible data on:

- 46 drives
- One aggregate
- One volume infected on a RAID-DP

For the recovery to go ahead, the Ontrack engineers had to take the aggregate offline, and the customer was advised to bring the 46 drives to the Ontrack lab for evaluation.

The Ontrack engineering team:

- Virtually rebuilt the RAID groups across ten different shelves
- Virtually rebuilt the aggregate
- Virtually rebuilt the critical volume
- Virtually rebuilt the critical volume

This recovery was additionally challenging due to the aggregate having still be in use for two weeks after the attack occurred, which resulted in some data being overwritten.

Leveraging NetApp's proprietary OS (OnTap) and file system (WAFL), Ontrack's engineers used multiple consistency points to "walk back" in time to find and merge unencrypted copies of the critical data to return to the customer.

This type of recovery is only possible on storage like NetApp's FAS because of the way the data is stored in the volume.