Cubbit

The ultimate guide to **ransomware protection** in 2023

Stefano Baldi
VP R&D at Cubbit

Blaine Harnack
Head of Technical Services & User Data Management at Cubbit

Introduction

Ransomware has become a real threat to businesses, individuals, and institutions.

We are talking about a type of malware that takes a victim's data and/or devices hostage and releases them upon payment of a ransom, usually in bitcoin. To create urgency, it can also threaten to publish (e.g., Ryuk) or delete (e.g., Jigsaw) critical information of the affected company.

In fact, in recent years we have seen an increase in ransomware victims: Apple in 2021, Uber and Continental in 2022, and VMware in 2023.

A report by Veeam states that 85 percent of companies surveyed were attacked by ransomware in 2022. And according to an IBM report, the average cost of ransomware is $4.62 million, excluding ransom payment.

That's why in 2023, it is critical for IT managers, developers, and C-levels to know this threat inside out and take action against it.

Ransomware: facts and statistics

Statistics

75% of IT organisations will be hit with at least one ransomware attack by 2025
Cyber Defense Magazine

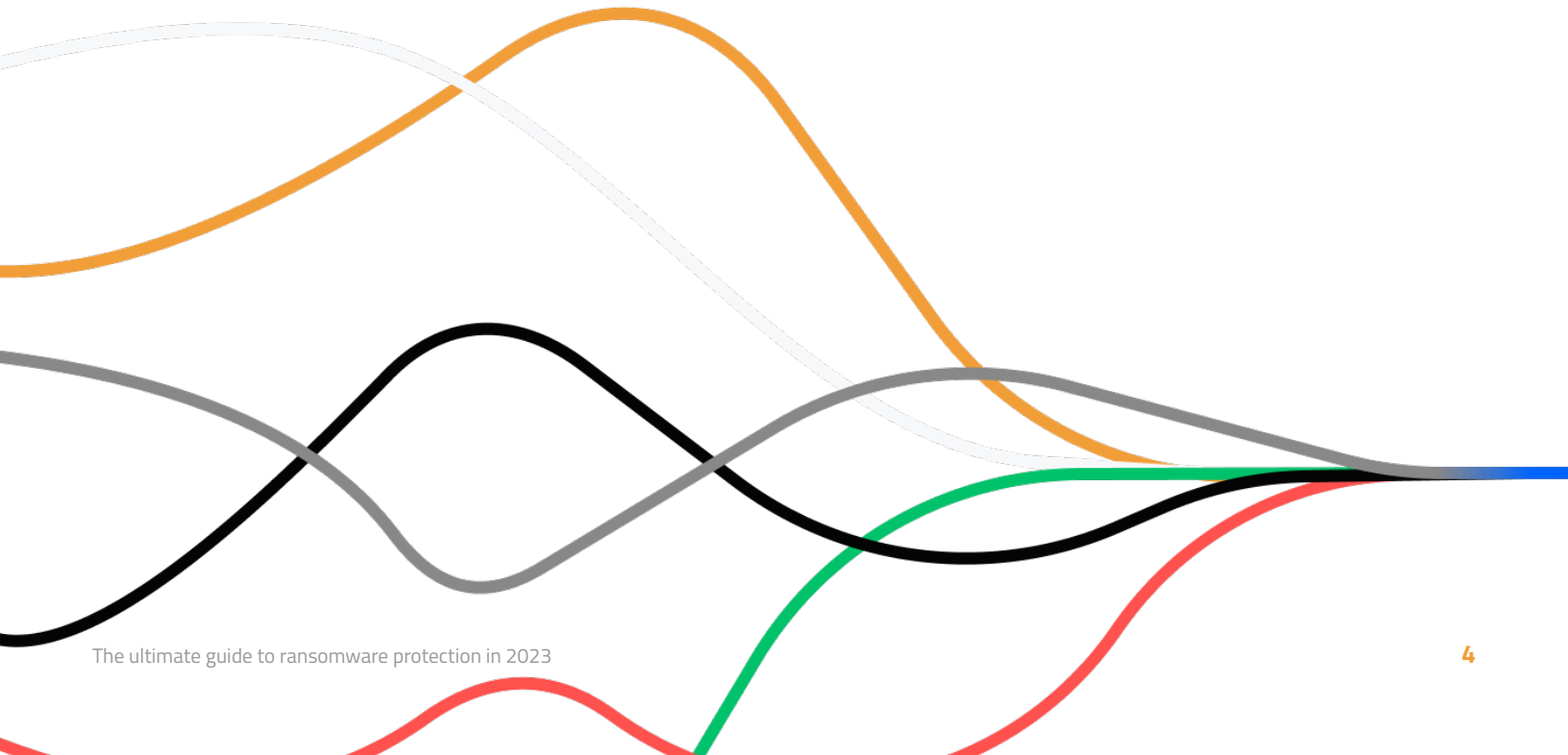
93% of backup repositories were targeted by ransomware attacks
Infosecurity

22 days is the average downtime following a ransomware attack
Cyber Protection Magazine

$4.45M is the average cost of a data breach
Technology Magazine

71% of ransomware victims are unable to restore all data
MSSP Alert

75% of ransomware victims have lost at least some of their backup repositories during the attack
Infosecurity



Top 5 ransomware attacks

February 2023

As a result of a global ransomware attack exploiting VMware vulnerabilities, 5,000+ companies fall victim and 1,000+ public and private services go offline.

January 2023

Yum! (operator of KFC, Pizza Hut, and Taco Bell) shuts down 300+ stores following a ransomware attack.

August 2022 — February 2023

40% of all ransomware attacks as of August 2022 are attributed to the ransomware gang LockBit, which counts famous victims such as Uber, GTA 6, Continental, and Royal Mail.

May 2021

Ransomware completely shuts down the operations of the giant Colonial Pipeline. The company is forced to pay $4M to restore business operations.

April 2021

REvil group targets Quanta, an Apple supplier, with a $50M ransomware attack. The goal was to shut down the Cupertino company's operations and force it to pay the ransom.

The true cost of ransomware

Although IBM claims that $4.62M (excluding ransomware payments) is the average cost of a ransomware attack, this figure is not limited to short term financial damages, but also involves significant long-term expenses.

In addition to the direct costs of the attack, such as paying the ransom itself,

organisations face three main “expense items”:

- Cost of downtime
- Fine for GDPR violation
- Reputational damage

The most significant consequence of a ransomware attack is the **cost of downtime**. A successful ransomware attack can prevent access to critical data and systems, resulting in downtime, lost revenue, and reduced productivity. The impact can be particularly severe for companies that base their strategy on real-time data management or operate in time-sensitive industries.

In addition to the cost of downtime, organisations can incur heavy fines for **violating the GDPR**. These regulations are designed to protect the privacy of personal data, and organisations that fail to comply can face substantial fines that may represent a significant financial burden. Fines for noncompliance can be very high, between 10 million euros and 2% of the annual turnover, putting even large companies at risk.

Reputational damage is another meaningful risk associated with ransomware attacks. A successful attack can cause stakeholders to lose trust, generating long-term consequences for a company’s reputation and revenues. Consumers avoid companies that do not ensure compliance and resilience in managing their data. A study conducted by IBM and Forbes Insights found that 46% of companies that suffered a cybersecurity breach experienced a significant decline in brand value and reputation.

6 myths and misconceptions about backup and ransomware

There are several myths and misconceptions about ransomware and backup strategies that can make companies vulnerable. Here are six famous myths about backup and ransomware and the truth behind them:

Myth No. 1 - Backing up regularly protects you from ransomware

Although performing regular backups is good practice, more needs to be done for recovering data from ransomware reliably. According to the Veeam 2022 Ransomware Trends Report, more than 90 percent of ransomware attacks now

specifically target backups by encrypting or destroying them. Recently, we have also seen how ransomware directly attacks servers and infrastructure, as in the case of the attack on VMware's servers.

Myth No. 2 - Tape Backup is the gold standard of ransomware protection

Although tape backup is a proven and reliable backup method, there are better options for recovering encrypted files from ransomware. Restoring tape backups can take a long time, and during a ransomware attack every second counts. Companies should adopt reliable ransomware solutions that guarantee fast data recovery. However, tape backups can still be critical for long-term data retention and archiving.

Myth No. 3 - Ransomware cannot encrypt a backup

Unfortunately, ransomware can encrypt a backup, which happens more often than people think. To protect against this, companies should implement data immutability, which prevents the modification and deletion of information even by users with administrative privileges.

Myth No. 4 - It is sufficient to back up only critical data

Backing up only critical data is not enough to defend against ransomware. Attackers can target not only critical data but also infrastructure components, such as servers and network devices, causing downtime. Companies should implement a comprehensive backup strategy against ransomware that covers all infrastructure components, from virtual machines to servers.

Myth No. 5 - Encrypting data is not useful in ransomware defence

Encrypting backups can be a viable solution to prevent data exfiltration because it protects data stored in backup files from unauthorised access. It is not a panacea for ransomware attacks, but it prevents double extortion ransomware from causing urgency in the victim, as happened with the Colonial Pipeline attack.

Myth No. 6 - Paying the ransom is cheaper than investing in prevention

Paying the ransom should never be considered a viable solution for recovering encrypted files from ransomware. Not only does it fund criminal organisations, it is also not guaranteed to lead to data recovery.

Let’s get to know our enemy better

What is the main target of ransomware?

Ransomware attacks primarily target organisations with valuable data and considerable financial means to pay for recovery. The main targets of ransomware attacks include healthcare providers, financial institutions, government, and companies (e.g., manufacturing, ICT, multimedia) that handle sensitive, personal, and financial data.

Small businesses, however, remain a prime target to cyber criminals. According to CNBC, 43% of all data breaches are against SMBs. Indeed, 61% of SMBs were hit by a successful cyberattack in 2022.

In addition to these organisations, network attached storage (NAS) devices such as those produced by QNAP and Synology have also been targeted by these attacks, as in the case of the eCh0raix ransomware. Small and medium-sized businesses often use these devices to store important data and files.

The cost of a ransomware attack to these organisations can be devastating, with inaccessibility to critical data and operations, the cost of downtime, and the threat of publication of private information.

How ransomware works

In a nutshell, ransomware encrypts the victim’s files using symmetric and asymmetric encryption methods. The process occurs correctly when the attacker generates a public key locally, which is then encrypted using asymmetric encryption. The keys can be single or multiple and are based on complex encryption methods such as RSA. Finally, the ransomware encrypts the data and makes it inaccessible.

The attacker demands a ransom to restore the encrypted files. Payment is often demanded in cryptocurrencies such as bitcoin.

Sometimes, when encryption is not properly executed, it can be hacked

through ‘trial and error’ attempts or by exploiting vulnerabilities in the algorithm. However, this can be time-consuming and difficult, and there is no guarantee that it will work or cause further damage.

7 different types of ransomware

Knowing the different types of ransomware can help IT managers, CTOs, and developers effectively respond to and prevent attacks.

1) Cryptographic ransomware

This threat encrypts data and demands payment to return access to your files. This family of ransomware spreads through malicious emails, websites, and downloads and can infect shared, networked, and cloud drives. A well-known example of cryptographic ransomware is WannaCry, which affected hundreds of thousands of computers in more than 150 countries in 2017.

2) Locker Ransomware

This attack completely locks down your system. A pop-up may appear on the victim’s screen stating that the computer has been infected with a virus or has been used to visit illegal websites and requires a payment to unlock it.

3) Double extortion ransomware

The attacker encrypts files and exports data to blackmail the victim into paying a ransom. The attacker threatens to publish the stolen data if his demands are not met, even if the victim can restore his data from a backup. An example of double extortion ransomware is Ryuk, which targeted several large companies in the United States and Europe in 2019 and 2020.

4) Leakware

Unlike double extortion, this ransomware threatens to publish sensitive data stolen from the victim’s computer or network if the ransom is not paid.

5) DDoS Ransomware

A ransom DDoS (RDDoS) is a type of malware that targets servers and network infrastructure. It works by launching a distributed denial of service (DDoS) attack against the target, making its systems and services unavailable to users.

The attacker then demands money to disrupt the attack and restore access. An example of RDDoS attack is Armada Collective, which targeted several high-profile companies in 2016.

6) Scareware

This type of malware typically pops up ads or alerts stating that your computer is infected with viruses or other threats and offers to clean up the reported problems for a fee. An example of scareware is Antivirus Pro 2010, which infected computers through malicious ads and pop-ups.

7) MBR Ransomware

This threat infects the Master Boot Record (MBR) of a computer's hard drive, making the operating system inaccessible until the ransom is paid. A well-known example of MBR ransomware is Petya, which first appeared in 2016 and quickly gained notoriety for its ability to spread quickly and cause widespread damage.

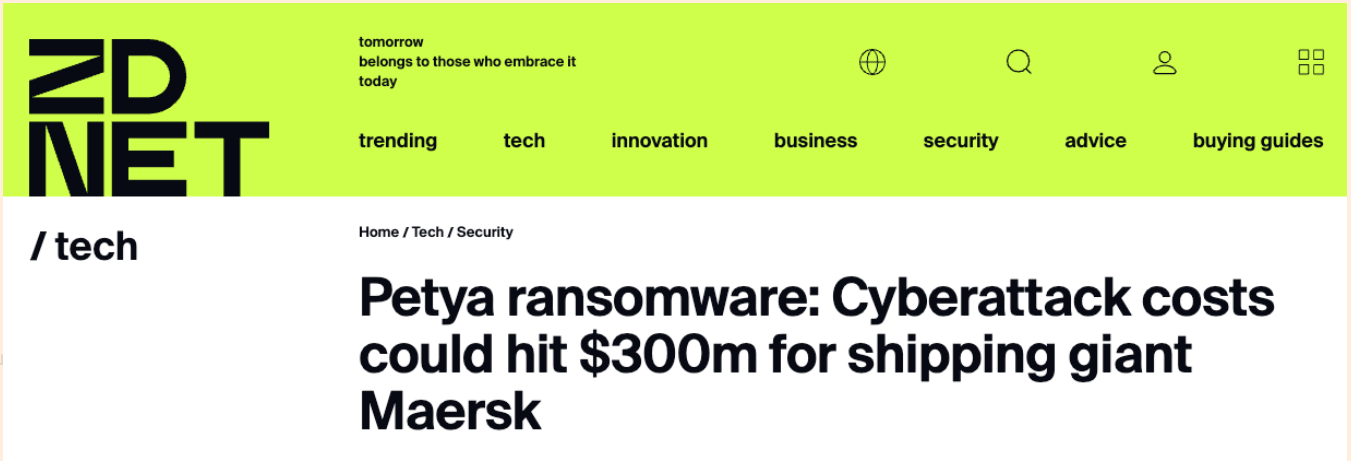
24 examples of ransomware attacks

Knowing the different types of ransomware can help IT managers, CTOs, and developers effectively respond to and prevent attacks.

Different types of ransomware have become increasingly common in recent years. Some famous examples of attacks are Petya, Ryuk, and WannaCry. This section will discuss these 24 attacks and the damage they have caused.

1) Petya and NotPetya

First discovered in 2016, Petya is a type of MBR ransomware. It works by infecting the master boot record of a computer's hard drive, rendering the operating system inaccessible. Initially used in 2017 for a massive cyber attack against Ukraine, it quickly spread around the world, causing more than $10 billion in damage.



Petya has since evolved into NotPetya: one of the most destructive ransomware in history, capable of spreading across computers and networks without human intervention for phishing or other types of initial access. In addition, NotPetya is famous for going beyond the master boot-of-record attack and encrypting everything that can be encrypted.

2) Wannacry/Wannacrypt0r ransomware

WannaCry is a cryptographic ransomware that first appeared in May 2017. WannaCry is famous for encrypting all data in Windows operating systems and demanding a ransom to return files. WannaCry attacks have affected more than 300,000 computers in 150 countries, with a total damage of more than $100,000,000.

3) CryptoLocker

Similarly to Wannacry ransomware, CryptoLocker encrypts all data on infected computers. It first appeared in September 2013, asking victims to pay the ransom to get their data back. Numerous reports claim that the CryptoLocker ransomware has extorted $27 million in total.

4) Ryuk ransomware

First appearing in late 2018, Ryuk is a double extortion ransomware. Similar to cryptographic ransomware, it encrypts all the victim's data; however, it has gained fame due to its ability to exfiltrate information and create urgency to pay the ransom in the victim. If the demand is not met, Ryuk will publish all confidential data. United Health Services estimated that the attack inflicted via Ryuk ransomware in 2020 cost $67 million.

5) SamSam ransomware

Released in 2016, SamSam ransomware uses brute-force attacks from remote desktops to steal passwords as initial access. Once it enters the system, it encrypts everything from data to applications, sometimes even removing them. This cyber attack netted over $6 million and had an impact on victims of about $30 million (U.S. Department of Justice).

6) GandCrab

Discovered in 2018, GandCrab is a family of cryptographic ransomware. Since its launch, its authors have claimed to have obtained over $2 billion in ransom payments and announced that "it was time for a well-deserved retirement."

7) Cryptowall

Cryptowall first appeared in 2014 and went through several iterations that made it increasingly dangerous. It has raised over $325 million in revenue for its creator.

8) Dharma (CrySiS) ransomware

Dharma ransomware, also known as CrySiS, is a cryptographic trojan. Unlike classic ransomware, Dharma enters the victim's computer with legitimate software used as a camouflage shield. It then encrypts every file added to the directory by adding the suffix [bitcoin143@india.com].dharma. Dharma, on average, demands $42,900 to return access to the files.

9) Maze ransomware

First appearing in 2019, Maze ransomware is a double extortion ransomware. Unlike traditional attacks, Maze encrypts critical data and threatens the victim with publication if they refuse to pay the ransom. In 2020, Maze infected Canon, Xerox, and LG Electronics, stealing more than 10 TB of confidential data and source code.

10) Locky ransomware

Locky ransomware is a cryptographic ransomware. It is famous for the variety of files it can encrypt: from documents to source code, destroying your computer. Its typical initial access is via a phishing attachment on an email that apparently seemed unreadable. The entire Locky ransomware campaign is estimated to have generated more than $7.8 million in revenue.

11) BitPaymer

Initially identified in 2017, BitPaymer primarily targeted medical institutions, locking all their data and demanding a payment between $500 and $1,500

in cryptocurrency. Its popularity gave rise to even more dangerous types of ransomware, such as DoppelPaymer.

12) DoppelPaymer

Launched in April 2019 with a similar mode of operation to BitPaymer, the DoppelPaymer-origin crypto ransomware belongs to the Dridex family of malware. Unlike BitPaymer, this new ransomware has different command-line parameters to avoid easy detection. The average ransom demand varies from $25,000 to $1.2 million.

13) Jigsaw ransomware (BitcoinBlackmailer)

Jigsaw first entered the hacker scene in 2016. Here's how it works: first it encrypts all data (only on Windows computers!), then it starts a countdown. If the ransom is not paid within the first hour, the first file is deleted and the demand increases. After sixty minutes, the number of deleted files increases exponentially.

14) NetWalker

Netwalker became famous in 2020 by exploiting a Ransomware-as-a-Service (RaaS) model. This means that the creator (Circus Spider) provides affiliates with all the support and tools they need to profit from this cyber attack. Like Maze, Netwalker is a double extortion ransomware: it encrypts data and exploits the threat of publishing it to put urgency into paying the ransom. Netwalker is among the top ransomware by revenue, with over $46 million generated.

15) Cerber ransomware

Like Netwalker, Cerber also exploits a Ransomware-as-a-Service model; $2.3 million is the annual revenue generated by this cryptographic ransomware.

16) Bad Rabbit

Bad Rabbit is a variant of Petya and WannaCry that emerged in 2017. Unlike the two aforementioned ransomware strains, Bad Rabbit is a locker ransomware that encrypts data as well as the entire system and servers. It became famous by spreading a fake Adobe Flash update. Bad Rabbit requires about $280 in

cryptocurrency within 40 hours.

17) MedusaLocker

MedusaLocker is a crypto ransomware that threatens the victim to publish data, but there is no evidence of its ability to actually perform this action. MedusaLocker exploits the Ransomware-as-a-Service model.

18) Reveton (also known as FBI Virus or Police Trojan)

Reveton became popular in 2012 as a password stealer. It then evolved into a locker ransomware, appearing on the victim's PC as a "police officer" and demanding to pay a fine to unlock the system and avoid arrest. It generated $400,000 per month between 2012 and 2014.

19) Teslacrypt

First identified in 2015, Teslacrypt is a ransomware notorious for encrypting video game-related files: from saves to replays. In 2016, it was terminated and the main decryption key was released.

20) AIDS trojan (also known as PC Cyborg virus)

The AIDS trojan is the first ransomware to ever appear in history. It was spread by means of a floppy disk sent directly to the victim under the name of "AIDS Information Introductory Diskette." Once it enters the system, this ransomware counts a certain period of time from when you open a file and once a set threshold is exceeded, the file is encrypted.

21) SimpleLocker

SimpleLocker is ransomware that encrypts data and locks the entire system. As reported by the BBC, SimpleLocker is the first case of ransomware that encrypts Android devices.

22) Troldesh

Troldesh is a double extortion ransomware: it encrypts data and steals it. Numerous file extensions are targeted by this cyber attack.

23) ZCryptor

ZCryptor is 50% ransomware and 50% a worm, which encrypts data as it copies it to external media. It usually targets Windows systems, masquerading as an installer of Adobe Flash or other popular programs.

24) Medusa ransomware

Not to be confused with MedusaLocker, Medusa is a double extortion ransomware that was born in 2021 and is gaining popularity in 2023. Its specialty is to encrypt with a combination of AES-256 and RSA-2048 and then publish victims' sensitive data in its Medusa Blog.

Bleeping Computer reported its ability to terminate over 280 different Windows services and processes, including those related to e-mail, databases, antivirus, and backups. In addition, it can eliminate shadow copies to hinder file recovery. In February 2023, as stated by Pierguido Iezzi (Cybersecurity Director and CEO, Swascan), Medusa was able to hit 17 different targets.

7 ransomware attack vectors

How does malware get into your computer? Here are the top 7 attack vectors for initial access.

1) Exploitation of exposed services with high-risk vulnerabilities

Attackers often target vulnerabilities in outdated or inadequately patched systems and software, making initial access easier. For example, on February 3, 2023, a high-risk vulnerability in VMware servers caused more than 1,000 servers and websites worldwide to go offline. Examples of these vulnerabilities include "zero-day" exploits, which are unknown vulnerabilities that are exploited before the vendor can release a patch.

2) Phishing attacks

These are social engineering attacks that aim to get users to click on malicious links or open attachments containing malware. Phishing can take many forms, including email attachments, SMS messages with malicious links, phone

calls, infected websites, and more. Attackers often disguise themselves as trustworthy people, such as colleagues, banks, or government agencies.

3) Compromised credentials

This occurs when an attacker gains access to a user's login credentials by guessing them, cracking them or obtaining them through a data breach. For this reason, it is essential to adopt strong password policies, update login credentials regularly, and monitor any suspicious activity.

4) Insider threat

In some cases, attackers target and bribe the victim's employees to gain access to a company's systems. This can be devastating because insiders often have privileged access to sensitive information and systems. The LAPSUS ransomware gang used to bribe employees of well-known companies to get inside their systems.

5) Drive-by downloads

These are malicious downloads that occur when a user visits a suspicious website or clicks on a malicious advertisement. The attacker can then install malware on the user's computer without the user's knowledge.

6) Malvertising/Adware

Attackers can create fake pop-ups or advertising software updates that contain malware, inducing users to download and install them on their systems.

7) Remote Desktop Protocol (RDP) exploitation

RDP is a protocol that allows remote access to a computer, and attackers can exploit it to gain unauthorised access to systems.

As you may have noticed, the ways ransomware can get into your computer are countless. But how does ransomware spread through a network once it enters? In the next section, we will look at the 5 key capabilities that allow this threat to spread to your business.

How does ransomware spread through a network?

Once ransomware has exploited the attack vectors listed above, it can use various techniques to spread across the network.

Here are the 5 key capabilities that enable it to get this job done.

1) Cross-compatibility

Some ransomware strains are designed to be compatible with multiple operating systems, such as Windows, Linux, and macOS. This way, ransomware is able to infect a wide range of devices and systems.

2) Network-wide spread

Ransomware can spread quickly and efficiently across the network by exploiting network-level capabilities, such as exploiting shares, protocols (e.g., SMD and NetBIOS), tools (e.g., PsExec, WMI), and other connected devices (e.g., printers).

3) Lateral movement

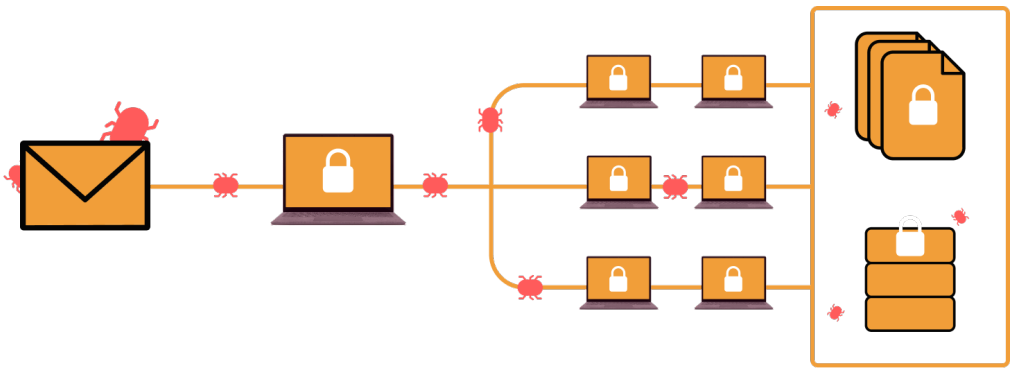
Once an attacker gains access to a system, he can use various techniques, such as exploiting trust relationships and using privileged access, to move laterally within the network and infect other systems.

4) Elimination of backups and restore points

Many ransomware strains can eliminate the local versioning system (such as Windows “shadow copies”) and even interact with local backups, making it difficult for victims to restore their data without paying the ransom.

5) Direct attacks on disk images

Some strains of ransomware, such as Hive, are able to communicate with systems such as VMware ESXi and directly attack disk images, causing widespread damage to the network.



7 stages of a cyber attack

Knowing your enemy is critical to protecting yourself from ransomware attacks. Here is an in-depth explanation of the 7 stages of a ransomware attack and the capabilities used by ransomware to enter an organisation.

1) Initial access

The attacker will typically gain initial access to the target's network through various ransomware attack vectors, such as phishing emails (e.g., sending an infected Excel file), exposed services with high-risk vulnerabilities, insiders, or compromised credentials.

2) Climbing the ranks

Once in the network, the hacker moves laterally to gain privileged access and permissions.

3) Infection via malware

Once privileged access to the network is gained, the attacker deploys the ransomware payload.

4) Propagation

The ransomware spreads across the network within seconds, infecting all connected systems and devices. This can be done by exploiting cross-compatibilities, using network scanning tools, or by exploiting the ability to move laterally within the network.

5) Encryption of files by ransomware

Once all systems are infected, the ransomware encrypts and makes your data inaccessible. Encryption is done properly using locally generated symmetric keys, which are then encrypted using asymmetric encryption. The keys can be single or multiple, relying on strong encryption schemes such as RSA.

6) Ransom demand

The attacker demands payment, usually in the form of cryptocurrency, in exchange for the decryption key. He may also threaten to publish the victim's

sensitive data if the ransom is not paid, further increasing the pressure on the victim to comply with the demand.

7) Cleanup and recovery

Experts suggest not paying the ransom so that the criminal has no incentive to carry out further attacks. Instead, it is necessary to clean everything up, delete the ransomware and start the recovery process.

Best practices: defence and prevention from ransomware

Ransomware prevention checklist

Ransomware can encrypt 100% of your data and system in seconds. This is why it is essential to always have a complete and up-to-date backup.

Also note that some cloud storage and backup services zero out egress fees but impose a maximum number of downloads that can be executed per day. This allows for efficient backup of critical data but not quick recovery of all assets, hindering business continuity.

Here are 6 best practices to always follow to keep your business operational and competitive.

#1 Check bandwidth availability by putting the system under stress during testing

The main critical backup issue for most companies is not ransomware, but available bandwidth for fast recovery with minimised damage.

Companies need to back up and restore data in a reasonable amount of time. Suppose, for example, that the available bandwidth is 100 MB (e.g., your company's headquarters is in an area not covered by fibre). During the day, the

company already saturates it at about 50%. If, on the other hand, we use 100% of our bandwidth at night for backups, antitheft and other systems will be unavailable due to internet saturation.

That is why, in addition to regularly performing backup tests, it is critical to know in advance what is the maximum bandwidth we can use for recovery and how long it takes to restore business continuity after a disaster.

This problem can be solved with a little-used (but extremely efficient) Veeam capability: the Veeam forever forward incremental backup. This strategy has two advantages:

1. It reduces file sizes through deduplication technology.
2. It only patches/updates the full backup you performed in the first phase.

This way, when it comes time to recover ransomware data, you will only have to restore the initial backup (instead of hundreds of incremental backups), which you can do in a reasonable time.

Watch the demo and learn how to create a secure, high-performance cloud backup with Veeam and Cubbit.

#2 Review and update storage policies

Ransomware is evolving and can now delete and exfiltrate critical backups. Because of this, it is increasingly important to monitor backup policies.

One key thing is to enable a policy based on immutability.

Built on the S3 Object Locking feature, immutable storage allows users to choose the data they want to protect, along with an expiration date: Within that time, no one — nor hackers, nor ransomware, nor service providers — can delete, encrypt or modify the data.

Here are some best practices your company should follow:

1. Verify and test your backups daily.
2. Use immutable storage as a solution for ransomware resilience.
3. Adopt a WORM (“write once, read many”) strategy.
4. Keep a copy on offline, air-gapped storage.

5. Always verify that you are using a versioned backup.
6. Ensure endpoint protection on backups and servers.
7. Maintain multiple recovery points with backup copy jobs.
8. Apply Veeam's 3-2-1-1-0 backup rule with more than one immutable storage.

#3 Apply Veeam's 3-2-1-1-0 backup rule

The 321 backup rule states that you should:

1. Make 3 copies of your data.
2. Keep them on at least 2 different media.
3. And save 1 off-site.

Industry leader Veeam has updated this excellent rule of thumb by suggesting the 3-2-1-1-0 backup rule. The additional 1 and 0 stand for:

1: Store the offsite copy offline, air-gapped or on immutable storage.

0: Backups and recovery should be checked daily. If you find errors, fix them quickly. You never know when the next disaster or ransomware will occur.

#4 Enable end-to-end encryption to prevent data exfiltration

With the rise of double extortion ransomware such as Ryuk, the victim faces not only downtime, but also the legal and reputational risks of publishing their private data.

This is why encryption does not directly protect against ransomware, but it still encrypts data. You avoid the urgency of paying the ransom as Colonial Pipeline did, paying over $4 million to obtain a decryption tool.

#5 Follow digital hygiene best practices

According to IBM, 95% of cyber attacks are caused by human error. This is why it is so important to stick to the essentials:

1. Train your employees regularly.
2. Minimise the attack surface through the principle of least privilege.
3. Patch software vulnerabilities.

4. Use layered security.
5. Adopt unique passwords and enable multi-factor authentication.

#6 Protect your entire corporate infrastructure.

In the fight against ransomware, it is not only backups and data that are at risk. Many ransomware directly attack the system and spread through the network via lateral movement.

That's why you should monitor networks and systems for signs of intrusion or suspicious activity and respond promptly to alerts or incidents and use security information and event management (SIEM) systems to automate monitoring and quickly identify and respond to potential threats.

Also, adopt endpoint protection solutions, such as endpoint detection and response (EDR) software, to detect and prevent ransomware attacks at the endpoint level.

Especially when dealing with large and geographically dispersed companies, it is critical to pay attention to branch offices in terms of security education, initial access, and more. Prevent them from being an easy initial access for cybercriminals.

How to recover from a ransomware attack in 7 steps

[Don't have an up-to-date backup of your data available? Find out how to decrypt files encrypted by ransomware in the next section].

Recovering data from a ransomware attack can be a complex process. The following steps are recommended to help IT managers, CTOs, and developers recover data following an attack.

1) Verify that your PC has been infected with ransomware

The first step in dealing with a ransomware attack is to verify whether your business has been affected. Here are some signs that your PC may have been infected with ransomware:

1. **Ransom demand message:** One of the most obvious signs of a ransomware attack is the appearance of a ransom demand message on your screen. This message typically indicates that your files have been encrypted by ransomware.
2. **Inaccessible files and data:** If you cannot access your files or find that they have been renamed with a strange extension, this may indicate that your PC has been infected with ransomware.
3. **Slow or unresponsive computer:** A ransomware attack can also slow down your computer. This is because the malware encrypts files, consuming a lot of system resources.
4. **Unusual pop-ups and system alerts:** Unusual pop-ups or system alerts may indicate that your PC has been infected with malware, such as ransomware. These alerts may appear while you are using your computer or be displayed on your screen when you start your computer.

2) Do not restore the backup immediately

Hackers expect this move on your part and will re-encrypt your data as soon as you restore it. Instead, delete the ransomware first and then recover your data.

In any case, don't pay the ransom. As one ransomware negotiator suggests, keep calm and don't incentivize the criminal to do it again.

3) Isolate and contain infected systems

As soon as you become aware of a ransomware attack, it is critical to isolate infected systems to prevent the malware from spreading further. Immediately disconnect the infected computer from the internet and any external storage devices, and check other computers and servers on the network for signs of encryption. Once you have contained the affected systems, you can move on to the next steps.

4) Identify the ransomware and remove it

IT managers and CTOs need to catalogue the different types of ransomware that have infected their systems to take appropriate recovery actions. Observe the note left by the hacker or seek help with an identification tool such as ID Ransomware. Then, adopt a ransomware removal tool or seek professional help to remove it manually.

5) Determine if the attacker has exfiltrated the data

Some ransomware attacks involve theft. The attacker copies sensitive data before encrypting it and threatens to leak the confidential information unless a ransom is paid. For GDPR purposes, it is essential to determine whether data has been exfiltrated and, if so, what data was taken and to whom it was sent. Especially if you were handling your customers' data.

6) Notify the right stakeholders and legal entities of the incident

Take a picture of the ransomware request message and report the attack to legal entities. This will help identify the perpetrators of the ransomware attack and develop new prevention methods.

Also, if you have multiple users on the network, it is good to inform them of the attack so they can take the necessary steps to protect themselves. To learn how to report it, look here.

7) Rebuild and restore systems

If you have an external backup available, then you can reset your system to factory settings and restore the original files. The backup should go back to a date before the ransomware attack to avoid a new infection. It is important to note that removing the ransomware does not necessarily involve decrypting the files or restoring the original files. This can only be done using a ransomware decryptor, if one is available for the infection variant. Also, remember to change all passwords.

In addition to these steps, IT managers and developers should conduct a post-mortem analysis to determine how the ransomware attack occurred.

In short, answer these 3 questions:

- What didn't work?
- What was the weakness?
- How to update the disaster recovery plan?

The goal is to establish a new prevention strategy to minimise the impact of future incidents and ensure that systems and data are adequately protected.

Please note: The 7 steps listed above are critical to a proper response to ransomware incidents. However, sometimes even IT managers do not have an up-to-date backup (or the backup itself has been encrypted by ransomware). The following section provides a simple step-by-step process to restore files encrypted by ransomware.

How to decrypt ransomware

If you do not have an up-to-date backup, you will have to deal with the ransomware and decrypt your files. Here is a 6-step procedure:

Step 1: Identify the type of ransomware

The first step in recovering files encrypted by ransomware is to identify the type of ransomware that has infected your system. This can be done by examining the malware's ransom note and file extensions. A website such as ID Ransomware can help identify the type of ransomware. Sometimes decryption tools may be available for specific strains of ransomware.

Step 2: Remove the ransomware

After identifying the type of ransomware, removing it from the infected system is critical to prevent further damage (and to prevent the files you recover from being encrypted again). This can be done using antivirus software or by following the instructions provided by other tools such as No More Ransom Project.

Step 3: Make backups of the infected files

Before attempting to restore files encrypted by ransomware, it is essential to back them up in case something goes wrong during the decryption process. It is recommended to make a copy of the encrypted files and store them on an external device or in the cloud.

Step 4: Use a ransomware decryptor

If a decryption tool is available for the specific type of ransomware, download it from a trusted source such as an antivirus software vendor's website or the No More Ransom Project. It is critical to make sure the tool is compatible with the specific ransomware variant.

Step 5: Run the ransomware decryptor

After downloading the decryption tool, follow the instructions provided by the device to restore the files. This may involve selecting the encrypted files, entering a decryption key, if provided, or selecting a folder to save the decrypted files in. It is essential to follow the instructions carefully, as the wrong settings or options could cause the decryption process to fail (hence the importance of backing up the encrypted data before beginning this process).

Step 6: Check that the files have been restored correctly

Once the decryption process is complete, check that the restored files are working properly. Inspect the files with an antivirus program to make sure they are not infected with residual malware. Also, save the decrypted files in a safe place.

If the files still do not work properly, try using another ransomware decryptor or contact a professional cybersecurity company.

In conclusion, decrypting and recovering files encrypted by ransomware can be very technical and there is no guarantee of success. It is essential to back up the encrypted data, identify the type of ransomware, download a reliable decryption tool, follow the instructions carefully, and remove the ransomware from the infected system.

Top 15 tools for decryption and removal

Before going any further, it is essential to specify the difference between a ransomware decryptor and a ransomware removal tool.

1. Ransomware decryptor: allows you to restore files encrypted by ransomware.
2. Ransomware removal tool: removes the ransomware virus.

So, if you use the “ransomware decryptor”, the virus will continue to encrypt files. On the other hand, if you remove the ransomware and do not have an up-to-date backup, you will no longer be able to access your data.

Top 10 free ransomware decryptors

Victims of ransomware can use decryption tools to recover their files without paying the ransom or restoring the backup. Here are some of the best ransomware decryptors available.

1. Bitdefender decryption tools

Bitdefender offers a ransomware recognition tool and decryptor for ransomware such as GandCrab, REvil, and Darkside.

2. Trend Micro

If you need to decrypt files hit by Petya, Jigsaw, CrySiS, Teslacrypt, and other insidious ransomware, give it a try.

3. Emsisoft

From Jigsaw to Wannacry, Emsisoft offers decryption tools for several ransomware types.

4. No More Ransom

Another flexible tool to decrypt files infected by Maze, Teslacrypt, REvil, GandCrab, and others.

5. Avast Ransomware

This tool can decrypt victim data of several ransomware strains, such as Babuk, CrySiS, GandCrab, TeslaCrypt, and many others.

6. Kaspersky's No Ransom

Kaspersky offers 7 free tools to restore files encrypted from ransomware such as Coinvault, Shade, and others.

7. AVG Ransomware

AVG offers 7 free ransomware decryptors for Apocalypse, BadBlock, Bart, Crypt888, Legion, SZFLocker, and TeslaCrypt.

8). Netwrkspider/WannaDecrypt

A free tool on GitHub to decrypt 5 ransomware from the WannaCry family (including the WannaCry ransomware).

9. Maureen Data Systems

This company provides decryption tools for numerous ransomware such as TeslaCrypt and Dharma.

10. Quick Heal

CrySiS, Troldesh, DeriaLock, GandCrab, and others: Quick Heal offers 20 free ransomware decryptors.

Didn't find what you were looking for? In this article, Heimdal Security provides one of the most comprehensive lists on the internet.

Top 5 tools for ransomware removal

Let us now consider the top 5 ransomware removal tools of 2023:

1. Avast Ransomware Removal Tool ***(100% free)***

This tool scans and removes ransomware on Windows, Android, Mac, or iOS devices.

2. Bitdefender Antivirus Plus ***(30-day free trial, from $23.99 per year)***

This behaviour-based detection system eliminates all types of ransomware, according to PCMag.

3) MalwareBuster ***(Free trial | $35.99/year)***

A software that scans your entire PC and removes all ransomware it finds.

4) Webroot SecureAnywhere AntiVirus ***(14-day free trial, from $23.99/year)***

Webroot is an antivirus that takes up very little space on the PC and scans very quickly. In testing by PCMag, it eliminated all ransomware and restored encrypted files.

5) Zscaler ***(30-day free trial, from $28.80 per year)***

A cloud-based platform offering malware removal tools.

Ransomware incident response plan checklist

Ransomware attacks can be catastrophic and cause significant downtime, data loss, and reputational damage. To deal with this threat without stress, organisations must have a comprehensive incident response plan that addresses all aspects of a ransomware attack.

That is why, in 2023, it is essential to have a proven ransomware incident response plan ready.

Below are the key checklist points that IT managers, CTOs, and developers should consider when creating a ransomware incident response plan:

#1 Before the incident

Before you prepare for the worst, make sure you have done everything you can to prevent the attack. Follow digital hygiene practices such as software updates, employee training, and the principle of least privilege. In addition, it is critical to test and verify your full backup (and disaster recovery plan).

To facilitate impact analysis, you can develop a risk assessment framework that considers the likelihood and potential impact of ransomware attacks on your organisation (e.g., downtime, data loss, reputational damage, regulatory fines).

After following the ransomware prevention checklist, you should prepare a ransomware incident response plan. The steps for doing so are outlined below.

First, it is essential to know what to do during a ransomware attack. Then, you need to create a table of roles and responsibilities: from IT to legal communications and crisis management teams. In addition, you need to know who to notify about the breach (e.g., internal teams, external stakeholders, and law enforcement).

Establishing advanced regulatory, insurance, and business policies is critical. Make sure your company's insurance policies cover ransomware incidents (and the negotiation process!) and that the terms and conditions of the policy are clear.

Finally, label and protect critical data. This last step helps you define the resources you will need to prioritise for recovery in order to maintain business continuity. In addition, you can mark sensitive resources that need advanced encryption to prevent exfiltration.

#2 During the incident

Ransomware is not a matter of "if" but "when." Sometimes the worst happens even though we have followed all the best prevention practices.

If your company is under attack or you notice something wrong, you need to act immediately.

First of all: wait to restore your backup! (Otherwise, the attackers will encrypt it again).

Instead, you must identify the type of attack, analyse its scope and impact, and isolate it from your devices and network. We have explained all the steps to follow in a dedicated article.

Please note: Make sure that there is always a secure environment and that you can restore systems to bare metal. If this is not possible, consider moving applications to the production environment.

#3 After the incident

Even if you have removed the ransomware and restored all critical systems, you need to understand what worked and what didn't. Also, consider implementing tools that allow you to granularly identify the causes of a data breach within minutes. Then, update your disaster recovery plan accordingly.

In conclusion, ransomware attacks are becoming increasingly sophisticated and widespread. Therefore, organisations must be proactive and prepared to handle such incidents. By following the checklist above, you can create an effective ransomware incident response plan that ensures business continuity during a ransomware attack.

Ransomware FAQ

What is Ransomware-as-a-Service (RaaS)?

Ransomware-as-a-Service (RaaS) has become a growing industry lately, generating millions in revenue each year.

Simply put, Ransomware-as-a-Service (RaaS) operates as a subscription-based business model in which cybercriminals offer a complete package of tools, services, and support to launch a successful ransomware attack. This package includes malware, a payment platform, and customer support.

Ransomware-as-a-Service (RaaS) enables a paradoxical model in which ransomware groups often refer to their activities as "businesses." As a result, the victims of their attacks are considered their "customers," toward whom they have "a reputation to uphold."

The RaaS service targets individuals or groups who do not have the technical skills or resources to create their own ransomware, but want to carry out a ransomware attack for profit. RaaS operates similarly to other software-as-a-service (SaaS) offerings, getting a percentage in exchange for their services.

Should you pay the ransom?

In 2021, despite recommendations from FBI and other institutions not to pay the ransom, Colonial Pipeline paid over $4 million to obtain a decryption tool and get back access to its files.

Paying a hacker, in fact, is not the best practice. In particular, you will encourage him to target you and other companies again. Moreover, there is no guarantee that the attackers will provide the decryption key. In some cases, they may even demand additional payments from you.

"If they identify your organisation as one that pays the ransom," says Jeff Lanza, a former FBI agent, at a webinar hosted by Rubrik and IT Web, *"you could end up on a 'known payer list' on the Dark Web and be a target for further attacks."*

Can ransomware steal your data?

Another reason not to pay the ransom is that some ransomware attacks also steal sensitive data, as in the case of a multiple extortion attack.

For example, Ryuk ransomware is known to steal sensitive information, making the attack even more damaging. The threat of publishing sensitive information is a decoy used by hackers to create urgency and encourage the victim to pay the ransom immediately.

Not only that, but new types of ransomware also spy on your credentials and steal accounts.

However, one of the most significant risks is the potential fines under the General Data Protection Regulation (GDPR). Especially if the ransomware victim was handling their own customers' data.

Under the GDPR, organisations can be fined up to 10 million euros for data breaches. This can be a significant financial burden for companies, especially those that handle large amounts of sensitive personal data.

Can ransomware encrypt already encrypted files?

A question often asked is whether ransomware can encrypt files that have already been encrypted and what the implications are for data security.

The short answer is, "Yes, hackers can install their encryption over your security layer and make your data inaccessible."

However, the practice of encrypting files as a preventive measure is still highly recommended. The reason is the spread of a ransomware called 'double extortion' ransomware: a virus that encrypts files and exfiltrates your data. In this way, it will urge you to pay, because if you don't, it will publish all your confidential information.

Recovery Time Objective and Recovery Point Objective

As organisations seek to mitigate the risks of ransomware attacks, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) have become essential for ransomware backup strategies. The RTO and RPO are key metrics that help companies determine the downtime and level of data loss they can tolerate during a ransomware attack.

Simply put, the Recovery Time Objective (RTO) is the estimated time to recover data and systems from the time of the attack. The RTO metric helps organisations set realistic expectations for recovery and ensures the rapid recovery of critical business operations.

Recovery Point Objective (RPO), on the other hand, is the amount of data loss the company can sustain, expressed in terms of time. In short, it determines how often backups should be performed (e.g., if your RPO is 120 minutes, you should perform a backup every 120 minutes, otherwise, if disaster strikes, you will lose the data created after this time frame).

Another set of metrics closely related to RTO and RPO are Recovery Point Actual (RPA) and Recovery Time Actual (RTA).

Recovery Point Actual (RPA) is the actual time at which data can be restored after an outage (i.e., the time of the last snapshot taken). Recovery Time Actual (RTA) is the actual time it takes to restore systems and data after an outage.

RTO and RTA may seem similar, but RTO expresses the estimated recovery time, while RTA is the actual time.

In conclusion, RTO and RPO are essential metrics that help organisations set realistic expectations for the recovery process and ensure that critical business operations can be restored as quickly as possible. Therefore, for a proper ransomware incident response plan, it is essential to establish appropriate RTO and RPO goals.

Conclusion

In conclusion, ransomware attacks are a growing threat whose impact can cause losses for millions of dollars.

This guide attempts to provide a comprehensive overview of the different types of threats, the main attack vectors, how ransomware infects a system, and the steps that can be taken to prevent and defend against this attack. Facing a ransomware attack can be a nightmare, but paying the ransom only serves to fund the criminal activity and there is no guarantee that you will get your data back.

Remember that prevention is always the best cure.

Cubbit offers a geo-distributed cloud storage that's hyper-resilient, sovereign, and 100% S3 compatible — with no extra cost for redundancy.

Unlike traditional cloud storage, where data is stored in a few centralised data centres, data on Cubbit is encrypted, fragmented, and replicated across multiple locations within a single country.

The service is GDPR compliant and certified with ISO 27001. It supports object locking, versioning and IAM policy.

To learn more about Cubbit's backup solution and how it can help protect your business from ransomware attacks, you can start a free trial — no credit card required. And if you need custom support or advice on storage and cybersecurity, you can book a free 15-minute consultation.

Cubbit

About Cubbit

Cubbit is Europe's first geo-distributed cloud object storage.

Thanks to its groundbreaking technology, Cubbit addresses nations' specific data sovereignty concerns, helping businesses check all the compliance boxes (e.g., GDPR and ISO) while ensuring data control and providing hyper-resiliency against ransomware and disasters.

Unlike traditional cloud storage, where data is stored in a few centralised data centres, data on Cubbit is encrypted, fragmented, and replicated across multiple locations within a single country or geofenced perimeter.

Thanks to S3 compatibility, you can integrate Cubbit in just a few clicks with any S3 compatible stack (e.g., Veeam, Nakivo, Synology,) enabling **immutable backup** lines with maximum security.

Today, Cubbit technology is adopted by 5,000+ customers, partners, and companies in 70+ countries.

The solution is compliant with GDPR and AgID, and certified with ISO 9001 and ISO 27001.

About the authors of this guide

Stefano Baldi is Vice President of R&D at Cubbit. An engineer by training, passionate about software and AI, in the second half of the 2000s he started working on Big Data, and high-reliability storage systems for major Italian telcos. Ten years later he founded and led as CTO two different startups, producing patented hardware and software solutions for cloud object storage, both on cloud and on-premise — solutions which were later adopted in several industries, including space, defence, and healthcare. Today, Stefano is responsible for innovation of products, methods, workflows and know-how in cloud storage.

Blaine Harnack is Head of Technical Services & User Data Management at Cubbit. A Canadian native, Blaine has more than 10 years of experience in IT, communication, and research. Since 2019, he has been responsible for Cubbit's technical services team and software quality assurance processes — a team that works closely with customers and users to ensure the best experience when using geo-distributed cloud storage.

Via della Zecca 1 - 40121, Bologna (BO), Italy

business@cubbit.io

www.cubbit.io