# RANSOMWARE

## Security Tips for SMBs


ESET®

Digital Security
**Progress. Protected.**

# TABLE OF CONTENTS

# INTRODUCTION

## RANSOMWARE IS ON THE RISE

In the past few years, criminal gangs creating this type of malware and running ransomware as a service have been developing a different, more targeted approach to these types of attacks – one for which metrics are much harder to obtain.

Cybercriminals are becoming more aggressive and show persistent efforts to discover any weakness in your IT security systems – attacking databases, web servers and smartphones. Brute-force attacks on the remote desktop protocol (RDP), or DDoS attacks against a company's website, are only a mere snippet of what is happening now.

## RANSOMWARE AS A THREAT TO SMALL AND MEDIUM BUSINESSES

SMBs are increasingly becoming attractive targets for ransomware attacks. Why? Because these businesses accumulate more valuable data than individual consumers, and at the same time, they lack the robust security measures employed by large corporations or institutions.

When it comes to SMBs, these factors act as a "sweet spot" for cybercriminals, and they elevate the risk of ransomware attacks.

In addition, because SMB managers often don't see their companies as potential targets, they may not regularly back up their vital data, leaving them less prepared for ransomware attacks.

# HOW DOES IT WORK TECHNICALLY?

**A ransomware attack can be defined as an attempt to extort money from an organisation by denying it access to its data.**

Realising that you have become a victim doesn't take long. Ransomware will usually inform you soon after affecting your devices, by displaying a ransom note on your screen, adding a text file to the affected folders, or changing the file extension of the encrypted files.

## Ransomware Types

### Screen locker ransomware

Blocks access to your device through a screen locker, allowing you to use only a malware user interface.

### PIN locker ransomware

Changes your device's PIN code, rendering its content and functionality inaccessible.


### Disk coding ransomware

Encrypts the MBR (Master Boot Record) and/or critical file system structures, preventing you from accessing your operating system.

### Crypto ransomware

Encrypts the files on your disk.

# HOW DOES IT WORK TECHNICALLY?

The scope for ransomware has expanded throughout the COVID-19 pandemic. Repeated lockdowns have brought more phishing emails, largely targeting employees who've moved to working from home and are accessing internal company systems and services via remote desktop protocol (RDP) – this has become a wildly popular vector for delivering ransomware.

In addition, cybercriminals who are running ransomware as a service (RaaS) schemes often leverage vulnerabilities to gain access to a machine, and then they move laterally to a server and to the wider network, only later deciding whether they will use ransomware.

Cybercriminals can also conduct supply-chain attacks, to access entire IT ecosystems. By commandeering popular, managed service provider (MSP) platforms and productivity tools, threat actors can unleash ransomware across multiple networks at scale. Another trend is that network-attached storage (NAS) devices, which provide data to different users and are commonly used to share files to make backups, have also earned the attention of ransomware gangs.

# HOW DOES IT WORK PSYCHOLOGICALLY?

Ransomware operators employ pressure as their core tactic. The pressure points multiply when individuals or organisations see real-life reputational damage, business outages, or even legal and financial penalties.

Manipulation is highly likely to follow. Victims often see multiple facets of their digital touchpoints affected, from DDoS attacks on their websites to obnoxious demonstrations of criminal presence on a network. Some of these include the following shock-inducing approaches:

- Print bombing, in which multiple printers on a network are commanded to print a ransom note — this threatens management's ability to control internal and external comms.
- Accessing a business's customer data, and then getting in touch with, or possibly even cold-calling, its customers with further threats, and publicly shaming the victims, while their IT departments struggle to mitigate impacts of the attack.

## INCREASING PRESSURE ON VICTIMS

To ensure that cybercriminals receive the sum they've asked for, they often multiply the methods of extortion.

### Double extortion

This combines data encryption with data exfiltration. Cybercriminals not only prevent access to a victim's valuable or critical files, but can also leak or sell them to other malicious actors. An example of this would be a method called doxing, when cybercriminals comb through their victims' systems to discover sensitive data, which they will then threaten to release, unless an additional fee on top of the ransom is paid.

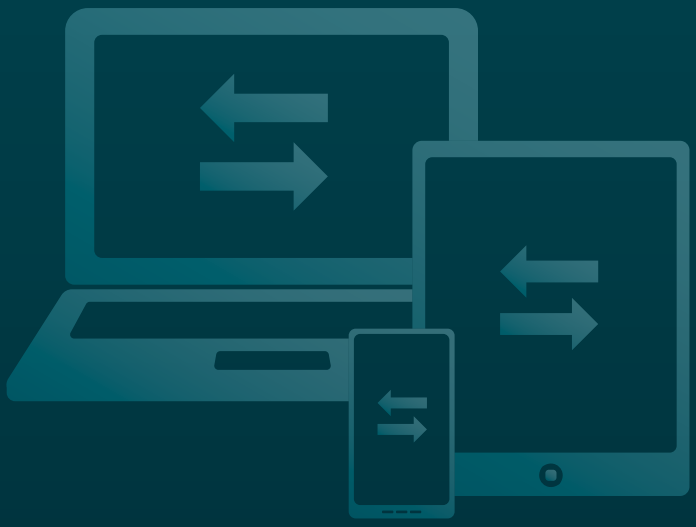
# HOW DOES IT WORK PSYCHOLOGICALLY?

## Triple extortion

Some ransomware operators contact business partners or customers of victims that have not paid the ransom, to inform their partners that their sensitive data has been accessed as part of the ransomware attack. They go on to suggest that these partners pressure the victim organisation to pay, in order to prevent this data from being released, or demand payment directly from the partners.

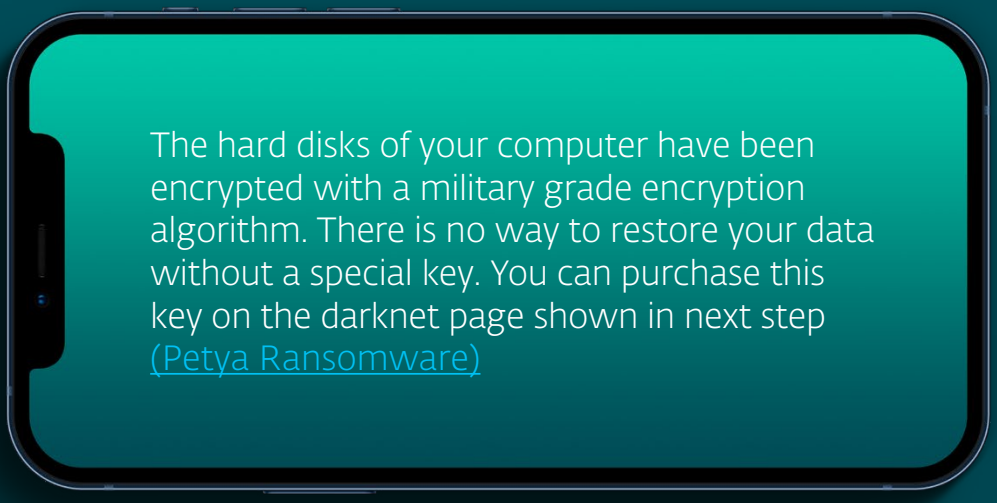
In other words, ransomware can turn an unfortunate malware incident into psychological warfare that aims to force victims to act against their own will and best interests. These attacks don't have to come via custom malware, zero-day exploits, or long-term persistence campaigns. They can simply be the result of poor security practices by employees, poor configuration of RDP and other remote access tools, or gaps in practices and processes, both within your organisation and that of your service providers and other actors in your supply chain.

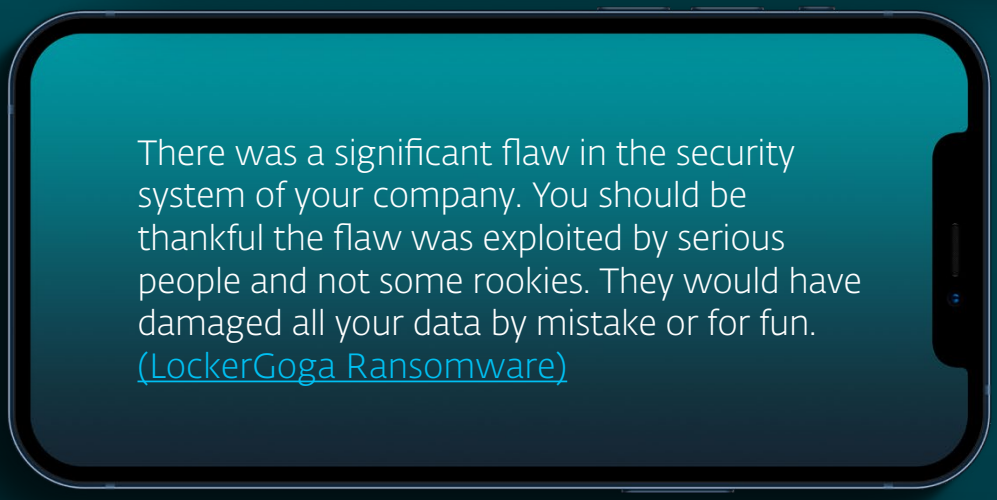
Security is a shared responsibility, which is why your employee cybersecurity training needs to be up to date and reflect the latest trends in cyber threats. You can reduce the number of malware incidents that your company has to deal with, by letting employees know what to look for and avoid, when it comes to phishing and other malicious content.

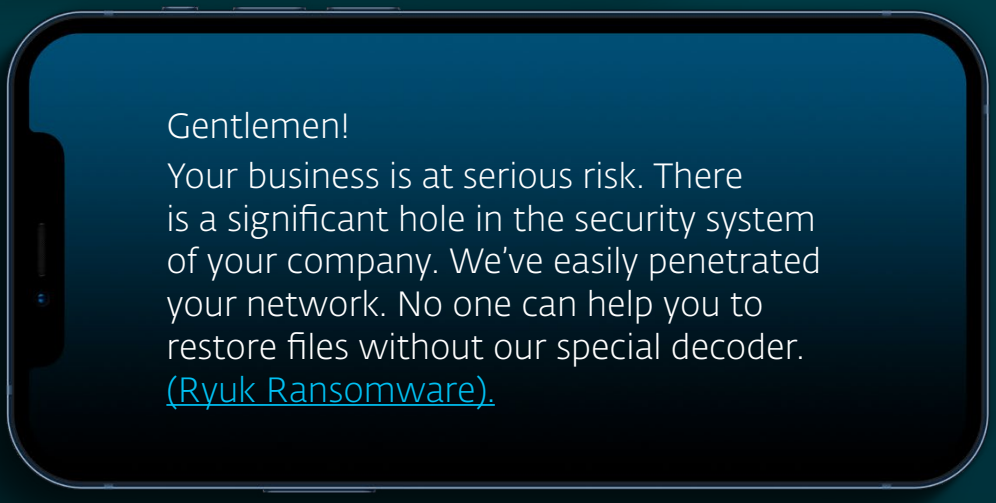


# HOW DOES IT WORK PSYCHOLOGICALLY?

## Examples of ransom notes



# RANSOMWARE VS. IT INFRASTRUCTURE

## REMOTE DESKTOP PROTOCOL

If your company systems need to be accessed remotely by your employees, they must have RDP enabled. This requires that a critical mandate be put into place, both for employees and even Admins to access the platform, via multi-factor authentication (MFA). Following authentication, employees may securely connect to these systems.

infobox

### In what ways can organisations use RDP?

1) To manage programs running on a server; for example, a website or back-end database.

2) To allow remote access to corporate desktops or virtual machines that have access to resources not accessible outside the corporate network. Accessing such systems via RDP means there is no need to directly open sensitive internal servers to the internet.



# RANSOMWARE VS. IT INFRASTRUCTURE

## Why is the discovery of external systems and their abuse so straightforward?

- Vulnerable RDP systems are easy to find (e.g., by specialised search engines like Shodan)
- It is easy for attackers to obtain a foothold on RDP systems if they have poor configuration
- Tools and techniques for privilege escalation and obtaining admin rights on compromised RDP systems are widely known and available

**71 billion**

The number of detections where RDP featured as an attack vector, between January 2020 and June 2021, according to ESET telemetry.

The total number of results for default RDP port 3389 open in the Shodan.io search engine

**Over 4 million**

Infographic

# RDP brute-force attack detection trend 7-day average


While the most notable increase occurred in the first half of 2020, 2021 saw the highest figures yet. When comparing H1 2020 and H1 2021, ESET saw sixfold growth in detected brute-force attacks against RDP. Moreover, attacks via RDP can fly under the radar of many detection methods, meaning fewer metrics and less threat awareness.

# RANSOMWARE VS. IT INFRASTRUCTURE

## HOW TO PROTECT YOUR COMPANY AGAINST RDP RANSOMWARE ATTACKS

- Have policies in place to address remote access security. You might have rules requiring all RDP access to be routed over a VPN (virtual private network), secured by MFA (multi-factor authentication), or limited to specific roles, on specific systems that are configured securely, patched promptly, monitored constantly, firewalled appropriately, and backed up regularly.
- Make sure everyone is complying with the rules, while also being prepared to handle an attack that somehow succeeds despite those rules.
- Make an inventory of your internet-facing assets. Based on our research, the following scenario is not that unusual: an organisation is attacked via an internet-connected asset that security staff were not aware of until after the attack.
- Do not allow a contractor or an employee to connect either a physical or a virtual server to the organisation network and the internet, unless that server is securely configured. The configuration must occur before the server goes live, particularly if the server is running RDP with a domain admin account.
- Document which internet-facing assets have remote access enabled and decide if that access is necessary. If access really is essential, require long passwords for the accounts that will have such access and determine the feasibility of limiting those systems to the internal network and accessing them remotely using a corporate VPN.
- If a system needs to be accessible from the public internet via RDP, and using a VPN is not feasible, install multi-factor authentication (MFA), so that you don't rely on passwords alone; however, be sure to use an MFA solution that is not SMS-based. Criminals have plenty of ways to thwart SMS-based authentication. In case you rely on passwords alone, set a threshold of three invalid login attempts, after which no login attempts are recognized for a set period: for example, three minutes.
- Harden and patch all remotely accessible devices. In addition to making sure that all security vulnerabilities are identified and addressed, make sure that all non-essential services and components have been removed or disabled, and that settings are configured for maximum security.

# RANSOMWARE VS. IT INFRASTRUCTURE

## EMAIL

Some criminals are still using email attachments to install malware that serves as the initial stage of being compromised, and which ends with ransomware.

They may use this vector to deliver downloaders that install malware on the email recipient's machine, or to establish a foothold on a networked machine within an organisation. That foothold can be the basis of an attempt to steal valuable data and encrypt files throughout the organisation, prior to making a very large ransom demand, as is often the case with targeted ransomware attacks via RDP.

Email is also one of the primary vectors for botnets, such as Trickbot, Qbot, and Dridex, which commonly use Microsoft Office documents, with malicious macros for initial intrusion and ransomware as the final payload.

Make it clear to employees that they should report suspicious messages and attachments to the help desk or security team right away. Early warning can help the organisation tweak its spam and content filters and bolster its firewalls and other defenses.

example

### From one email to an unusable electronic door at a hotel

Ransomware might not only encrypt your computer's data. A managing director at a four-star hotel in Austria's Alps got a ransomware email that was disguised as a bill from Telekom Austria. After he clicked on a link in the email, his hotel's electronic doors became unusable, and he was not able to issue new card keys to guests. To return to operations, he decided to pay a ransom of two Bitcoins.

Subsequently, this hotel was hacked three more times. It only proves that by paying ransom, you are showing criminals your willingness to pay. So, there is a higher chance they will attack again in the future.

Source: BBC

# RANSOMWARE VS. IT INFRASTRUCTURE

## SUPPLY CHAIN

A supply chain is a network of links between a company and its suppliers to produce and distribute a specific product or service. Attacking the supply chain along any of these points will have consequences along its length.

When supply-chain attacks are digital rather than physical, there are similarly damaging effects. By breaching just one of the participants in the supply chain, bad actors may eventually be able to gain unfettered and hard-to-detect access to large swaths of business partners and the customer base.

example

### What can happen in the case of a supply-chain attack?

In 2017, ESET discovered that a legitimate accounting software was used by criminals to push the NotPetya/DiskCoder.C malware. The attackers penetrated the software company's update servers and added their own code to legitimate application update files. When users of the accounting software clicked to install program updates, they were also installing a malware backdoor, opening the way for what became the most devastating cyberattack in history.

Source: WeLiveSecurity

The growing intensity of supply-chain attacks is also documented by the number of published ESET research articles where this attack vector was used. Between November 2020 and February 2021, there were four supply-chain attack cases discovered exclusively by ESET – a very high number compared to previous years.

Defending against this type of attack involves keeping up with software updates and patches, using endpoint protection software, potentially leveraging EDR solutions, and educating users about unsolicited emails that encourage them to visit unfamiliar websites.

# RANSOMWARE VS. IT INFRASTRUCTURE

## OTHER VULNERABILITIES

While cybercriminals can benefit both from known and unknown vulnerabilities, laying hands on zero-day vulnerabilities generally belongs to the world of APT groups and state-sponsored actors. Saying that, it still provides more than enough headaches for security admins and business owners alike.

Almost all cybersecurity vendors still detect EternalBlue exploit (2017) activity and its many variants, as well as ongoing exploitation based on Microsoft's SMBv1 file-sharing protocol. The long shelf life of vulnerabilities and threats like WannaCryptor (aka WannaCry) usually traces to poor updates and patch management at businesses and institutions.

Lastly, VPNs also demand proactivity by IT Admins who must update the cybersecurity products as required. This focus on timely updates should be paralleled by the use of multi-factor authentication when signing in to VPN services. If suspicions of credential abuse arise, organisation should pursue comprehensive account resets.

example

### Exploiting vulnerabilities via Microsoft Exchange Server

In March 2021, Microsoft rushed out emergency updates to address four zero-day flaws affecting Microsoft Exchange Server versions 2013, 2016, and 2019. Threat actors were observed exploiting the vulnerabilities in the wild, to access on-premises Exchange servers, which allowed them to steal emails, download data, and compromise machines with malware for long-term access to the victim networks.

Source: WeLiveSecurity

# RANSOMWARE DEFENSE STRATEGIES

## CLOUD AND NETWORK SEGMENTATION

Whatever attack vector is employed by ransomware, if it gets into your organisation, there is a fair chance it will try to spread to as many machines as possible and impact all your company's operations.

Limiting the number of machines that an attacker can reach from a single entry point has significant benefits as a defensive strategy. There are several approaches to implementing such a strategy – notably, network segmentation.

A popular system architecture strategy in recent years has been to move data to the cloud. But the cloud provides no automatic immunity from ransomware attacks. In fact, the low cost and relative ease with which new servers can be provisioned in the cloud and connected to the rest of the organisation digital infrastructure has made the cloud a fertile hunting ground for criminals. Clearly, any use of the cloud by any part of the organisation needs to be properly authorized and securely configured. Also, like all other systems, those in the cloud need to be enrolled in an appropriate backup and recovery regimen.

# RANSOMWARE DEFENSE STRATEGIES

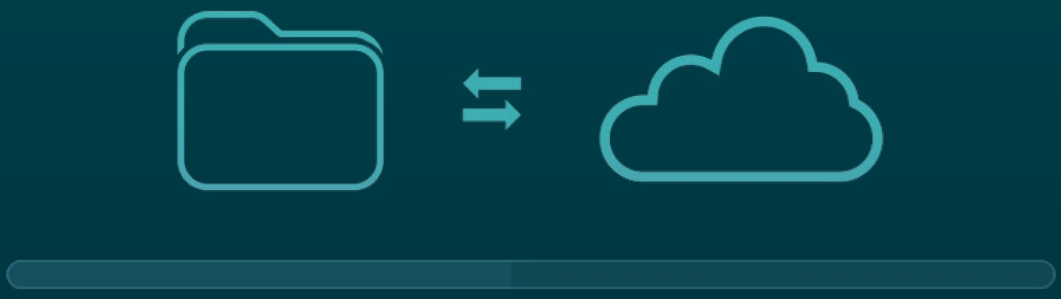
## PATCHING AND BACKUP

Patching and backup are two aspects of operating and administrating systems that play vital roles in defending against ransomware attacks.

By patching systems, potential avenues of attack are closed off and ransomware can be prevented from getting into your organisation. Or if it does get in, possible damage can be reduced. And a properly managed backup and recovery program is a vital defense mechanism that's crucial for your recovery efforts when ransomware does get into your organisation.

**This can be a lot more complicated than it sounds. Why? Patches and updates need to be tested before they are deployed. Some of your organisation's systems may have software dependencies that are broken by upgrading to the latest version of an application or operating system.**

There is a lot of truth to this, but bear in mind that some ransomware attacks are executed over a lengthy period, during which the ransomware may also be backed up, compromising the potential for a smooth recovery. That is why backup is not a set-and-forget defense; it needs to be monitored and managed, and the recovery process needs to be regularly tested.



# RANSOMWARE DEFENSE STRATEGIES

There are more options than ever for backup and recovery – notably, cloud storage, whether remote, on-premises, or hybrid; however, there is also more data to be backed up, from more places. Unless you have a comprehensive backup strategy, there is always a chance that the purveyors of ransomware will find that one device that you neglected to back up.

According to the backup experts at Xopero, a member of the ESET Technology Alliance, comprehensive backup includes data and system state on all endpoints, servers, mailboxes, network drives, mobile devices, and virtual machines. But there are some caveats specific to ransomware.

For example, when storage is "always on," its contents may be vulnerable to compromise by ransomware, in the same way that local and other network-connected storage is.

infobox

## How to prevent ransomware from propagating

**Opt for off-site storage that:**

- Is not routinely and permanently online.
- Protects backed-up data from automatic and silent modification or overwriting by malware when the remote facility is online.
- Protects earlier generations of backed-up data from compromise, so that even if disaster strikes the very latest backups, you can at least retrieve some data, including earlier versions of current data.
- Protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.

Don't underestimate the utility of write-once media for archiving data. Files stored on media that is not rewritable are immune from the predations of ransomware.

# RESPONDING TO RANSOMWARE

Even if you are aware of the dangers of ransomware and have put in place every possible preventive measure, your organisation still needs to be prepared to respond to a ransomware attack that succeeds in penetrating your defenses. Here, we offer a practical overview that may be useful for planning your response to a ransomware attack.

infobox

## Does your staff understand the policies?

**Questions to discuss within a company:**

- To whom should employees report suspected ransomware?
- What is company policy on paying ransomware demands?
- What steps are the organisation obliged to take in the case of a data breach?
- Who is allowed to pay/negotiate ransom payments?
- What is company policy on powering down affected machines?
- Who makes this call? Powering down machines eliminates potential evidence stored in memory and may be considered as not compliant with regulations.

**Problems to avoid:**

- Employees not reporting suspected ransomware for fear of retribution.
- Network admins paying ransoms because it is easier than recovering systems from backups.
- Unauthorised release of information about actual or suspected ransomware attacks.

# RESPONDING TO RANSOMWARE

## RECOVERY PLAN

It is a good idea to have at least one ransomware scenario in your crisis planning playbook, and to go through it in a tabletop exercise with relevant personnel, including executives.

You can thereby reveal gaps in backup and recovery plans, and better anticipate the impact of not being able to access basic services due to systems being encrypted, like email, VoIP phones, and internet access.

## Example of an effective incident response and recovery plan:

1) At first signs of attack, notify designated personnel.
2) Isolate and analyse affected machines.
3) If isolating affected machines is not possible, take a system image and memory capture, then power them down to avoid further spread of the ransomware attack.
4) Once the attack is confirmed, activate your Incident/Crisis Response Team.
5) Alert legal counsel.
6) Contact vendors who may be able to assist.
7) Remind employees of press and social media policies to maintain control of public-facing communications.
8) Assess attack scope and specifics of ransomware (e.g., determine whether a (publicly available) decryption key is available).
9) Contact law enforcement.
10) Prepare a PR holding statement.
11) If files have been encrypted, determine whether they can be restored from backup.
12) Keep employees updated on status.
13) If necessary, activate your business continuity plan.

# RESPONDING TO RANSOMWARE

14) IT Admin should collect relevant logs and possible indicators of compromise, such as binaries, ransom demand notes, IP addresses, registry entries, or other files.

15) Document the initial investigation of the attack and the steps taken to remediate it.

## WHY YOU SHOULDN'T PAY THE RANSOM

Paying the criminals who have encrypted your files by no means guarantees that you will get the decryption key. There are numerous reasons why paying may not get your files back:

1) Some of the data might have been corrupted in the encryption process and are thus not recoverable.
2) The provided decrypting tool might be bundled with other malware, not work properly, or be much slower than recovery from backups.
3) The process for delivery of the decryption key might fail.
4) The attacker might be acting in bad faith and might have no plans to provide decryption keys.
5) Paying ransom can be illegal. For example, in October 2020, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) declared it illegal to facilitate the payment to individuals, organisations, regimes and, in some instances, entire countries that are on the sanctions list.

On top of that, there are ethical reasons not to pay the demanded ransom. Because if you do, you ...

... are validating the business model behind the crime.
... are encouraging further criminal activity.
... are allowing ransomware gangs to research zero-day vulnerabilities and develop new exploits.
... may be hit with future attacks and further demands for money.

infobox

Typical arguments for paying ransom

## "It's cheaper than restoring from backups."

If this statement is based solely on time and labour calculations, it might be technically correct; nevertheless, the decision to pay is deeply flawed for the reasons stated earlier. Also, removing active ransomware with security software is by no means the same as recovering data. Removing the ransomware and then deciding to pay up means that the data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is often part of the malware.

## "We cannot restore the encrypted information from backups."

This could be because backups do not exist, or they exist, but are incomplete or damaged in some way; however, there are real alternatives to paying up. First, check with your security software vendor to see if there is a decryption tool available, making recovery possible without paying the ransom.

# FUTURE RANSOMWARE SCENARIOS

Ransomware leverages an organisation's dependence on technology. Therefore, we can expect ransomware to persist and evolve in the future, barring unforeseen shifts in global politics and economics.

Based on our experience with malicious code, since the late 1980s, we can say that malware threats tend to evolve along these lines:

- Vulnerabilities in a new technology/software are discovered and their potential for criminal abuse is discussed.
- Attempts at criminal abuse of the latest technology are, at first, rare, because criminals are making easy money from established strategies.
- Efforts to remediate and mitigate those vulnerabilities begin.
- Absent widespread criminal abuse, remediation and mitigation efforts lose steam.
- Eventually less-skilled criminals discover that this "new" technology is ripe for exploitation.
- A new malware trend emerges.

These evolving ransomware scenarios have multiple implications for SMBs. It's time to start addressing these potential threats within your own risk management strategy and planning.

Start getting a handle on "ransomable" assets now: IoT devices, SOHO routers, robots, control systems, and autonomous systems. Track vulnerability reports related to these assets and keep up with patches and firmware updates for these assets. Also, segment IoT devices and other new technologies from production networks.

Due to the increased effectiveness of extortion techniques and new ransomware distribution channels, hundreds of millions of dollars are estimated to have ended up in the accounts of these technically skilled cybercriminals, allowing some of them to build a ransomware as a service business model (RaaS) and onboard numerous new affiliates (criminals with lesser skills and experience). Moreover, it is assumed that some cybercriminal gangs have begun acquiring zero-day vulnerabilities and buying stolen credentials, further expanding the pool of potential victims.

# CONCLUSION

With money, ambition, and focus mostly on the side of ransomware gangs, learning from the nightmare stories and analyses reported daily in the media has become a must for any IT Admin, security professional, and business leader. It has been demonstrated time and time again that enforced policies, proper configuration, and strong passwords, combined with multi-factor authentication, can be the decisive elements in the fight against ransomware.

To counter zero-day vulnerabilities, botnets, malspam, and other, more technically advanced, techniques, additional security technologies are needed. These technologies start with a multi-layered endpoint protection solution, able to detect and block incoming threats in emails, via web links, RDP, and other network protocols; and endpoint detection and response tools to monitor, identify, and isolate anomalies and signs of malicious activity in an organisation's environment.

**Keep your endpoints secure from ransomware with ESET solutions.**
**To discuss further, please contact us at sales@eset.co.uk.**

## ABOUT ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services, to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multi-factor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com/uk/ or follow us on LinkedIn, Facebook, Twitter and YouTube.



Digital Security
**Progress. Protected.**