Tech Informed

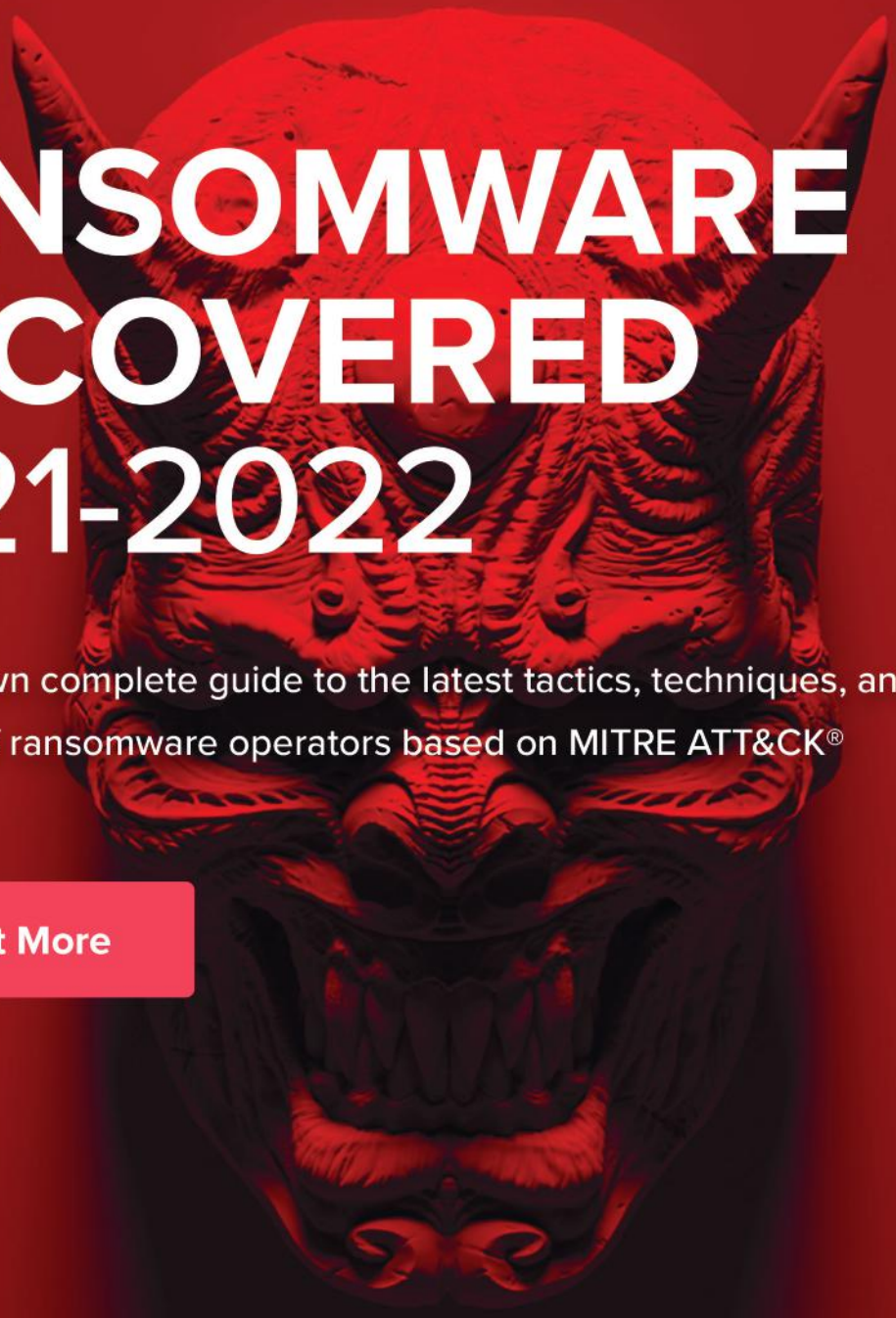
The frontier of tech news

Special Report

@TechInformed

www.techinformed.com

GROUP-IB



RANSOMWARE UNCOVERED 2021-2022

The well-known complete guide to the latest tactics, techniques, and procedures of ransomware operators based on MITRE ATT&CK®

Find Out More

THREAT RESEARCH

GROUP-IB.COM

James Pearce
Editor
TechInformed

Facing the threat head on

It is not an exaggeration to say that cyber security continues to top the agenda for most global enterprises. Since TechInformed launched less than a year ago, no subject has elicited a greater response than cyber threats, with the number of attacks recorded in the first half of 2022 up 15.1% on the previous year, according to ThoughtLab.

I don't write this to be alarmist, but pragmatic. Without trying to sound like a cliched advert for a cyber security firm - who provide an invaluable service to enterprises - but it is almost certain, in this most uncertain of times, that your business is more likely than not to come under threat.

Of all the cyber threats out there, one of the most prominent and nefarious is ransomware - when attackers take your data or systems hostage, with the promise of returning access in exchange for a fee.

TechInformed can't claim to produce a report that prevents this from happening, but we can introduce you, through conversations with over 50 cyber security specialists, to your enemy, the ransomware attacker, which may help you make more informed decisions about which technologies and strategies to deploy.

In this special report - pulled together by the brilliant TechInformed editorial team - we dive right into what ransomware actually is, how it happens, and what you can do to both prevent it or,, in the worst case scenario, when you fall victim to it.

The key thing to remember: Don't panic. This report is not about bigging up the threat to your business - though that threat is a very real one. It is a practical intro to the world of ransomware.

Please let us know what you think on the social handles below.

Follow TechInformed on Twitter: @techinformed

Follow TechInformed on LinkedIn: @techinformed

CONTENTS

A quick thank you

To create this report, TechInformed reached out across the industry for key insights into ransomware, and the response was overwhelming. We'd like to thank all of those who contributed, whether quotes were used directly or as part of our research. Please see a list of organisations that contributed below – and thanks to them for their input.

Akamai, Adarma, BlueVoyant, Canon, Censornet, Central Networks, CheckPoint, Cyberproof, Cybersmart, Cyber Risk, CYFOR, DigitalXRAID, Drawbridge, eSentire, Enpass Technologies, Exiger, Forcepoint, Forescout Security, Hamilton Barnes, Intercity, KnowBe4, KPMG, Kroll, Netacea, Nonname Security, NormCyber, Nozomi Networks, Otka, Open Systems, Psybersafe, Privacy Compliance Hub, Qualys, Quostar, Searchlight, Secure Age, Splunk, SureCloud, S-RM, Trend Micro, Threat Quotient, Thales, Trelix, University of Nottingham IEEE group, Vectra, VIPRE, Yubico

Editorial
James Pearce *Editor*
Nicole Deslandes *Reporter*
Ann-Marie Corvin *Report editor*
Emily Curryer *Editorial Assistant*

Design
Sajeev Alangode *Sr.Graphic Designer*

For advertising enquiries email contact: @techinformed.com

iResearch™
research to relationships

Green Pioneer or Greenwasher? The Tech Industry and Sustainability

Our two-part report on sustainability in the technology sector focuses on **proprietary global research** and **first-hand insights** from **sustainability specialists**, **consultants**, **technology leaders**, and **decision-makers**.

You will gain insights on:

- Which **technologies** and **business strategies** are **driving sustainability**.
- What **challenges and opportunities** the technology sector faces in becoming more sustainable.
- How innovation is **driving cross-sector partnerships** to bring about green tech and sustainable change.
- Is **greenwashing** really as much of an issue for the technology industry as it appears?
- And much more...

How Sustainable is the Technology Sector?

Discover by downloading our two reports today.

iResearch Services, a global B2B thought leadership and marketing agency.

Contact us about your thought leadership campaigns
thoughtleadership@iresearchservices.com

www.iresearchservices.com

“Know thy enemy”: The hackers and their marketplace

By Ann-Marie Corvin and Nicole Deslandes

Who are the bad actors threatening your business, and why is it important to know your enemy, and how they operate, so you can protect yourself?

Know thy enemy and know yourself.” So goes Sun Tzu’s ancient proverb from Chinese opus The Art of War. It is wisdom that rings true today for enterprises looking to tackle the threat of ransomware.

The full quote says when you’re ignorant of the enemy but know yourself, your chances of winning or losing are equal. If you’re ignorant of both your enemy and yourself, you are sure to be defeated.

With ransomware, it is important to start there - with getting to know your enemy.

By ransomware, we mean malware that encrypts data, demanding payment in exchange for a decryption key, given in return for a ransom usually paid in Bitcoin or another digital currency.

Ransomware’s cost to business can be immense – according to Sophos’ 2022 State of Ransomware report, the average total cost of recovery from a ransomware attack in 2021 was $1.4 million.

The subsequent data loss can cause a business to be down for 10 days or longer, meaning factors such as product sales and business productivity are also affected. And it’s hard to quantify the kind of reputational damage a breach can cause a firm.

Once the data has been encrypted by ransomware, the hacker usually demands a ransom using Bitcoin or another digital currency to decrypt and regain access to their files.

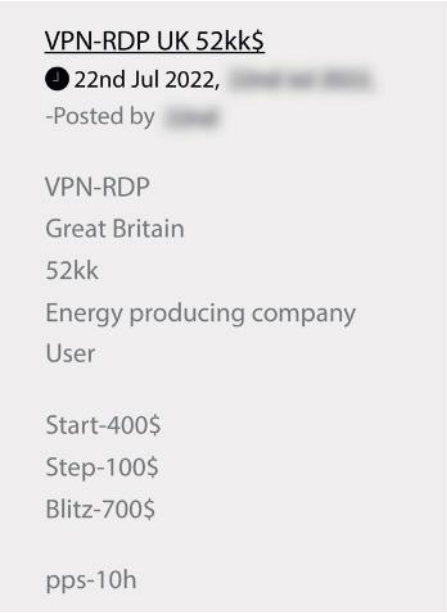
The growing threat of ransomware has caused some enterprises to acquire Bitcoin solely for the purposes of attacks – although whether a ransom should ever be paid or not is something we’ll discuss in part three of this series.

The dark web

So who are the hackers and how do they operate? The stereotypical image of the malevolent hoodie-wearing hacker is in urgent need of an update: no longer are single players the only threat at the table. Nor is cyber warfare merely available to nation states looking to flex their digital muscles or harm their political enenmies.

Digital transformation has swept

through the criminal underworld – turning a cottage industry into a multimillion-dollar criminal racket with software-as-a-service offerings similar to most legitimate tech businesses.
Conversely, because it's never been easier for the have-a-go-cyber-criminal to don a hoodie and inflict some serious damage, to some extent this stereotype persists – albeit one that now operates within a much more complex framework.
According to Roger Grimes, a data driven defence evangelist at Know-



A user selling credentials relating to a UK-based energy company. Figure from Searchlight Security

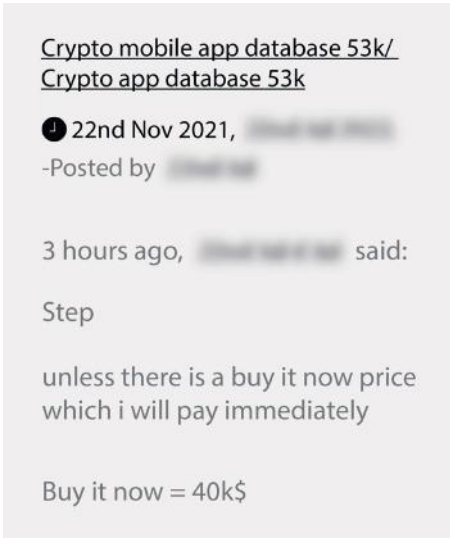
Be4, today's ransomware criminals run the gamut from lone individuals to criminal gangs, cartels and nation state sponsored attackers.
Most operate via the dark web – that encrypted alcove of the internet which is not indexed by search engines and requires a specific configuration or authorisation to access – over a peer-to-peer connection, or by using an overlay network such as the Tor browser.
While this anonymous part of the internet can be used by people who require privacy for legal reasons – the exchange of proprietary business data or for political activism for instance – these networks have contributed to the dark web's reputation as a hotbed for criminal activity.
Technology, training and ransomware-as-a-service kits (or all three bundled in together) can be accessed cheaply and anonymously on the dark web.
A recent HP Wolf Security Report analysed 35m hidden dark web sites, noting that cybercrime is being supercharged through 'plug and play' malware kits that are making it "easier than ever" to launch an attack.
As a result, only 2-to-3% of today's criminals are high coders

Tools of the trade

On the dark web marketplace, exploit kits, remote desktop protocol (RSP) server access, and attacks that flood a server with internet traffic to block paying customers to have access (DDoS-for-hire) are the most in-demand cyber products and services on marketplaces, according to Smith from S-RM.
A data-stealing Trojan is one of the most popular tools - stealing passwords, cookies and credit card information, it can be bought for as a little as $50-150, according to Jamie Smith, head of cyber at S-RM.
"A ransomware kit can cost from $40 to several thousand dollars a month, depending on the malware strain and whether affiliates share profits with operators," says Smith, adding that "there are also sophisticated malware sellers who offer customers free updates, customer support, and in-depth tutorials."
Additionally, some RaaS groups provide tools and tutorials directly to their affiliates and will trust to receive a split profit of the attack.
Whilst cybercriminals will purchase tools, code, and tutorials to hack into organisations, they can also often simply purchase verified credentials for compromised organisations which could be used as an access point to the organisations network.

The ubiquity of RaaS

Modern ransomware attacks are likely to be deployed by orchestrated businesses or organisations – sometimes even nation states – operating all core elements of a legitimate business, including HR.
Different roles up for outsourcing parts of a ransomware attack include initial access to the organisation; lateral movement through the network and privilege escalation; data exfiltration and clean-up as well as developers to work on bugs or new features for the malware.
As Robert Fitzsimons, a threat intelligence engineer at Searchlight Security explains, these functions might be coupled with "middle management roles, criminals in charge of the PR campaigns to promote the attack, and a negotiator to handle the communication with the victim".
He adds: "The most sophisticated groups manage internal user interfaces and messaging channels so that they can rapidly fire off multiple attacks and thus increase the chances of securing a ransom payment from one of the victims."
The evolution of distinct roles with a ransomware attack has been shaped by the emergence of the Ransomware-as-a-Service model.
RaaS is growing for the very same reasons that software-as-a-service is growing – convenience and access to application functionality without having to install, maintain or even understand the technology itself in order to to use it, alongside the advantages brought by scale.
As Alexandra Willsher, senior sales engineer at Forcepoint, notes: "Criminals now build once and resell many times over."



Credentials from target organisations being sold on the dark web. Fig from Searchlight Security

RaaS also affords criminals the luxury of anonymity: hackers can rotate between renting numerous strains of malware, making it harder to pinpoint who they are as there's no longer a signature methodology. Prolific operators include Lockbit, Blackcat, Hive, Clop and – until recently – Conti.
The Russia-based operator – whose victims have ranged from clothing retailers such as Fat Face to the government of Costa Rica – wound down in May this year, although is reported to be rebranding as several new ransomware groups.
Conti's decision to regroup follows a huge leak of internal documents that revealed details about the inner workings of one of the world's biggest ransomware groups.
The messages revealed that Conti operated much like a regular company, with salaried workers, annual leave, bonuses, performance reviews and even employees of the month.
Whichever the operator, what RaaS has served to do is to lower the entry point for other individuals or groups to perform ransomware attacks, says Jason Illingworth, principal analyst at NormCyber.
"By using tools developed and sold by the main groups, they're able to take a portion of the paid ransom, allowing more cybercriminals to launch ransomware attacks and increasing the scope of companies targeted. The main groups can focus more time on developing new tools while those that have paid for the tools carry out the attacks," Illingworth adds.
It's a trade-off that suits everyone: RaaS also poses less of a risk for malware authors, as they're not the ones carrying out the actual attacks while, Steven Furnell, IEEE senior member and professor of cyber security at the University of Nottingham notes, by using RaaS, would-be cyber criminals are also paying for a tried and tested malware – rather than risk of devising their own solution.
The Big Tech-level of efficiency with which these organisations are run, helps explain the reason why ransomware attacks are currently soaring.
And to hyper charge operations further, there's also been a trend over the last two years for collaboration and partnerships between different ransomware operators: sharing knowledge, stolen data, leaked information and other resources to exhort victims, enhance their capabilities and improve their success rate.
One of the most notable cartels over the last two years has been the Maze-Ragnar Locker- SunCrypt cartel. According to reports, Maze grew so big that it couldn't handle all available field operations and invited other operations such as SunCrypt into the fold on a revenue share basis to help handle attacks.

Forums
Platforms where ransomware tools and newly discovered vulnerabilities in software are discussed, include Exploit, Dread, Nulled and Cracked.

Jason Illingworth, principal analyst at NormCyber

Others, such as Russian speaking forum XSS have banned all topics relating to ransomware in order not to draw attention to themselves.
This followed a raid on RaidForums – a popular English language forum which was taken down by law enforcement agencies in April.
Because forums are now a police target, most active and well-known RaaS gangs communicate directly via their leak sites on the dark web, according to Daniel Dos Santos, head of security research at Forescout.
The dark web is not the only place where ransomware is traded. According to Hugh Raynor, senior cyber security consultant at SureCloud, apps such as Telegram and Signal are also being used to trade ransomware "which is perhaps not surprising given their end-to-end encryption".
There have also been reports of malware being traded on app Discord – which lacks encryption and is said to actively work with the authorities.
However, Raynor explains: "The ease of marketing Discord servers to users of the platform and the huge market of potential buyers for these services has clearly tempted some groups."
As a case in point, researchers at cyber firm Avast recently discovered an online community of children using dedicated Discord servers to build, exchange and sell malware.
Criminal groups lure in by advertising access to different malware builders and toolkits that can be used to code malware without much technical experience.
But how much damage can inexperienced "script kiddies" inflict by purchasing malware or software tooling from forums and indiscriminately targeting various systems and organisations to learn and 'play around' with their tools?
Paul Baird, chief technical security officer UK at Qualys puts it this way: "You could describe an experienced hacker as a smart weapon with precision accuracy, while the novice hacker is like cluster ordinance that creates unimaginable damage over a wide area without any thought for the future."

How hackers find their way in

By Ann-Marie Corvin

2022 is shaping up to be a vintage year for ransomware attackers. Deployment of this malware has skyrocketed in recent years, with more attacks reported in the first quarter of 2022 than in the whole of 2021, according to research by cyber security supplier WatchGuard.

Unlike lightning, ransomware attacks are more than capable of striking the same place twice – with a recent Veeam ransomware trends report revealing that 75% of organisations have suffered two or more ransomware attacks in the past. But how do the hackers get in?

The most likely entry point for an attack, according to most of the experts we spoke with, involves phishing emails designed to trick employees into clicking malicious links or downloading infected attachments.

The reason this method is so prevalent, according to SureCloud's Raynor, is because "for all of the benefit of the additional controls, updates, network monitoring and software we apply to the network, humans remain predictable, easy-to-fool bags of flesh."

While humans continue to be the weak link in most firms' security plans, malicious actors are also getting more sophisticated in their phishing attempts and some scams are very hard to distinguish from legitimate emails.

Cian Heasley, security consultant at Adarma, explains that the larger ransomware groups are also shifting away from "scatter gun methods" of phishing, opting for more strategic ways to target victims.

"As such, we're seeing a trend towards spear phishing – which targets high value victims who are more likely to have the type of access ransomware operators seek, perhaps because of their job title," Heasley notes.

While firms can educate their staff to become more aware of these digital social engineering techniques, some other, more aggressive forms of ransomware, can exploit security holes to infect computers without needing to trick users.

Working from home has also exacerbated the number ransomware attacks – in part thanks to the rise in use of external remote services.
According to Ioan Peters, managing director and coleader EMEA of Cyber Risk at security services firm Kroll, in Q2 of 2022 there was a 700% increase in the use of external remote services for initial access by attackers.
Keegan Keplinger at eSentire's Threat Response Unit, notes that stolen Virtual Private Network (VPN), Remote Desktop Protocol (RDP), and AD credentials are now extremely popular ways for cybercriminals to gain access to a victim's IT environment.

Hugh Raynor, cloud security lead at Surecloud

Raynor adds that firms are open to danger when – deliberately or otherwise – they expose their remote desktop protocol services to the internet, to enable connectivity.
"Attackers conduct massive scans of the internet looking for the ports associated with these RDP servers," he warns, "and once they find one, they will send thousands of login attempts to these devices using arbitrary username and password combinations that they have collated from breaches, or had success with before."
KnowBe4's Grimes adds that the biggest surprise for him has been the abuse of unpatched VPN software, both server and the client side – "... the very thing that companies were told they needed to keep them safe is now being used against them."

Patch-and-mouse

Another entry point for attackers which ransomware authors are keen to cash in on is security flaws in software, with many releasing malware and zero-day attacks to exploit software vulnerabilities before vendors and defenders have had a chance to react.
Cyril Noel Tagoe, Netacea's principal security researcher, claims that often with zero day attacks, criminals will reverse engineer critical security updates to identify the vulnerability being patched and exploit unpatched machines. "Many organisations are slow to apply these patches, giving the ransomware authors a decent window of opportunity for exploitation," he explains.
Recent vulnerabilities have been reported in Atlassian's developer tools Confluence; SonicWall's legacy firmware product; in Microsoft Exchange; filetransfer appliance Accellion as well as in VMware's ESXi servers.
Jamie Smith, director and head of cyber security at S-RM adds that he's still seeing well-known vulnerabilities such as Log4Shell (a flaw in popular Java logging framework Log4j) and ProxyShell (an attack chain that exploits three known vulnerabilities in Microsoft Exchange) being actively exploited.
"This indicates that opportunistic threat actors are targeting organisations with gaps in their vulnerability and patch management processes," he adds.
Another reported cyber security concern is the use of macros to automate common tasks in Microsoft Office such as spreadsheets or invoices. In industries such as finance, banking, insurance and retail – being able to control spreadsheets with macros is useful, but, because it's code essentially, it's something that cyber criminals are taking advantage of.
Macro malware (usually delivered via a phishing or spear phishing email or a malicious Zip which the user unwittingly clicks on) hides inside Microsoft Office files.
"Because MS software such as Word and Excel go back many generations the Microsoft suit is vulnerable – and nine out of 10 targets are likely to have this software installed," says Kevin Bocek, vice president of security strategy and threat intelligence at Venafi.
"A Word or Excel doc might target someone in sales but in engineering you might plant code in a PowerShell to execute a code which includes ransomware," he adds.
While it appears that a lot of legacy Microsoft products are to blame for the recent spate of zero day attacks, Qualys UK CTSO Paul Baird believes that the onus should be on firms to update software and keep an asset list.
"It's very easy to point the finger at Microsoft but any software with the right vulnerabilities could potentially allow cyber criminals access to your corporate network. It could be an Apache Web Server, Microsoft Exchange server or an obscure FTP server most people have never heard of," he says.

> "...any software with the right vulnerabilities could potentially allow cyber criminals access to your corporate network"
>
> Paul Baird, Qualys

"Companies must know all the software that they have, and how up to date that software is. With this asset list in place and continuously updated, teams can be sure that they are protected against all potential threats," he adds.
Baird's point hammers home the point that knowing yourself (your own organisations' vulnerabilities and

software inventory) is as crucial as knowing how your enemy (the ransomware attackers) operate.

Supply pains

The SolarWinds supply chain breach proved how suppliers and business partners can also potentially be another weak link in an organisation's security.

Muhammad Yahya Patel, security evangelist at Check Point

It's not unusual for companies to allow third-party vendors or partners to connect to their networks, either in-house or via a secured remote connection. The connection typically only authenticates the external user; once they have proven their identity, communication can flow freely, and ransomware/malware can be delivered.

According to Muhammad Yahya Patel, security evangelist at Check Point, it's key that a supply chain can demonstrate how it's making itself secure and this should be a two-way agreement. "Too often it's a one-sided conversation but to work best, both companies need to vet each other to ensure they're as secure as possible," he adds.

Baird points out that small businesses are a target because often they don't have the resources to spend on security, and have weaker defences. "Attacking a weaker supplier or business partner could be an easier stepping stone into multiple targets all from one hack. The potential payout is much higher, so it has become an area of focus," he warns.

> "To work best, both companies need to vet each other to ensure they're as secure as possible"
>
> Muhammad Yahya Patel, Check Point

Remote access

Once they've broken into a company's network an attacker will often go into stealth mode – 'living off the land' – making a silent entry to observe what the business does and what its activities are, before deciding on what course to take.

"They will read financial statements and cyber security insurance policies. They will exfiltrate data and passwords in 90% of all cases," Grimes warns.

Lateral movement can be facilitated by ransomware tools, existing software vulnerabilities or via misconfigured networks where attackers can escalate privileges and obtain more sensitive credentials.

In tandem with escalating their level of privilege, hackers also examine the type of security tools that are in place and how they can best spread ransomware throughout the company's computers. They will try and delete back up files to make decryption harder. They will also seek out other networks they can gain access to.

To remain hidden, hackers might try to disable security tools to some extent and use obfuscation techniques to hide their malicious payloads.

"They tend to use pen testing tools that are explicitly trusted in the environment, such as Cobalt Strike and Ngrok, but also misuse Git repositories," says Filip Verloy, tech evangelist at API security platform Noname.

Cyber criminals are also known to use legitimate services such as TeamViewer to mask their presence in the network. Another detection-avoidance technique is to try and learn the method used for remote access by the admins, and only use that method to log in remotely.

Dwell time before an attack, according to our experts, is now down to several weeks or a month at most (compared to 6-8 months a few years ago) thanks to the way the business models and ransomware gangs have evolved.

"Members of ransomware gangs are paid based on successful attacks, it is in their best interest to get in, secure the access they need, exfiltrate data and then execute their ransomware so that they can move on to the next target and keep chasing those commissions," Heasley explains.

The use of automation in an attack or the ability to deploy a blanket encryption has also speeded things up more.

As new Ransomware-as-a-Service (RaaS) models emerge, it could be that several groups are involved at different points along the way. An initial access broker may gain access to a network, then sell that to a RaaS affiliate that uses a malware dropper from one group and a ransomware from another.

You've been hacked – so what's the plan?

By Nicole Deslandes

So, they're in. The data's been hijacked, and systems are on lockdown. But don't worry, you can get it all back. For a price.

'Don't pay!' plead the cyber security experts and law enforcement, but with your business at risk, you face a dilemma: backups might not work and paying could be cheaper than recovery.

Now the devil is on one shoulder and the angel is on the other, the quandary of whether to pay or not starts to weigh in. The hackers have made their demands – usually payment in the form of cryptocurrency – but do you pay?

Show me the money

"Ransomware is a criminal enterprise, where those who play by the hackers' rules help fund their next attack on an unsuspecting victim," states Jason Illingworth, principal analyst at IT security service firm NormCyber.

It's true that paying the ransom does not guarantee the return of stolen data, and in the worst-case scenario, organisations will simply be out of pocket, on top of being shut out of their systems.

Even when the keys are handed back, it may still take a long time to recover systems.

"Look at Ireland's health service that was hit by Conti – the team there were still attempting to recover from a cyber attack six weeks in, even with the decryption keys," notes Paul Baird, CTSO UK at Qualys.

To add insult to injury, data regulators may dole out fines that could range up to hundreds of thousands of pounds.

As part of a bid to crackdown on ransomware operators, there's an ongoing debate as to whether it should be illegal for businesses or an individual to pay a ransom – or at the minimum, to make it mandatory to report ransomware payments to the authorities – something that the Australian government is currently considering.

Meanwhile in the UK, the government's intelligence arm GCHQ and its data protection watchdog ICO joined forces with the Law Society this summer to launch a campaign to actively discourage lawyers from advising their clients to pay out.

Yet, despite the advice and the pitfalls

involved in paying, the prospect of being handed a decryption key to recover data quickly is tempting for many firms.

More than 80% of British companies that have suffered a ransomware attack paid their attackers, a 2022 Proofpoint study found. Even among smaller firms – around 20% of mid-market businesses end up paying ransoms, according to Code Red's: The State of the UK's cyber security response report, with the average pay-out standing at £144,000.

"It rarely hurts [to pay]," opines Grimes. He adds that depending on the time and survey, the average percentage of victims who pay the ransom varies from 10% to over 60%, with the median percentage being about 40% to 60%.

To all the groups who say it never pays to pay, Grimes counters: why do the cyber security insurance companies always pay?

"Insurance companies know what it costs if you pay or don't pay the ransom, and every insurance company will pay the ransom if they are reassured that paying the ransom will result in the victim getting the decryption keys and those decryption keys and programs working."

Richard Walters, CTO of Censornet

So, while the received wisdom is not to pay out, there are several factors that could push an organisation into paying a ransom.

The financial impact of not paying and recovering systems over a long period of time could be greater than paying up and hoping that the keys will be handed over.

If cyber criminals have hit both the live data and the cold data backups (although these backups should always be segmented), then an organisation may have no choice but to pay if they want to be able to recover their systems and carry on with their functions.

"Typically, organisations must decide whether to pay out on a case-by-case basis. And it often comes down to limiting the reputational and financial damage of a breach, while carefully considering the ethical and legal implications that come with paying a demand," says Richard Walters CTO of Censornet.

Double extortion

Here's the rub: firms that do choose to pay are advised to ramp up security: the business has just caved to the demands of criminals, is now an open target for a second or even a third hit.

"The very act of paying an initial ransom suggests to ransomware groups that the victim may be more open to paying a second or third time when presented with the threat of double extortion, in which data is published or sold online, and triple extortion, in which anyone affected by the data stolen is threatened individually with its publication," warns James Tamblin, UK president of BlueVoyant.

Steven Furnell, a professor in cyber security at the University of Nottingham, quoted recent evidence that suggested that 80% of victims that paid a ransom were hit a second time, often while still recovering from the initial attack and still in a vulnerable position.

Despite these statistics, other experts refute the idea that double and triple extortion is common.

"Organisations spend an incredible number of resources recovering from incidents, often hiring one or many third-party companies to ensure the incident at hand is remedied, illegitimate access is denied, and steps are taken to prevent similar or worse

Danielle Jablanski, OT cyber security strategist at Nozomi Networks

$160,000 bill for failed security measures

Solutions provider Network Coverage told us of a construction management company (who again could not be named) who suffered a breach, compromising work stations and backups.

The company's ability to function at capacity was compromised, leaving 30 employees unable to work for 10 days while its data was held to ransom.

The company's disaster recovery provider was unable to prevent the attack. The firm also had no back up of its data. The attack led to over $100,000 lost in productivity and business.

The company was forced to pay the $60,000 ransom.

In the aftermath, Network Coverage helped the firm recover its data and put security measures in place to bolster its client's business. It also implemented a secure, automated, reliable backup system to prevent data loss and protect against the impact of future threats.

cases from reoccurring," assures Danielle Jablanski, an OT cyber security strategist at Nozomi Networks.
Whatever decisions are made, in the event of a ransomware attack the first 72 hours after a data breach are critical, according Tamblin. "Every decision an organisation makes can carry financial, legal, regulatory, investigatory, and reputational repercussions," he warns.

Incident response plan

In the era of the zero-trust cyber security framework it is not a matter of if a business is attacked, it's a matter of when. While the experts we spoke with might have been split on the issue of whether to pay up or not, all emphasised the importance of having a robust incident response (IR) plan to run through in the event of attack.
An IR plan is a living document comprising of many different components of a drill to be prepared for in the event of a real-life cyber-attack. The key pillars of any IR plan fall around preparation; detection; analysis; containment; eradication; recovery and post-incident response activities.
The most important step of all is the first one, according to CheckPoint's Muhammad Yahya Patel, as many businesses don't prepare for a ransomware attack thinking that it won't happen to them – a mindset that needs to change.
"Having an IR plan to run through is key to making sure you're able to respond to an attack efficiently. You want to analyse the different streams in your business that need to get started once you are attacked and to make sure that they will be able to function as you deal with the threat," adds Patel.
Planning for an incident typically involves establishing roles and responsibilities; identifying contingency plans; prioritising physical and environmental safety; dictating policies for backups; recovery and restoration; crisis communications and ensuring a thorough post-incident forensic investigation is conducted with lessons learned.
This drill also needs to be routinely tested and revised to meet evolving needs, according to Larry Gagnon, senior vice president, Global Incident Response, eSentire. "An untested IR plan is little more than a list of suggested actions," he says.
"Test, test, test. This is best achieved by testing the plan through tabletop exercises delivered as scenario-based tests of your IR plan, help to identify gaps and inefficiencies in your documented processes," he adds.

Who, what, where?

In the event of a breach, it's important to be able to reach out to the right people quickly and ensure that key players understand their roles and how they can minimise disruption to your operations and customers.
According to eSentire's Gagnon, there are typically two distinct tracks in response to a breach or a malware event – a tech track and an executive track.
"The tech track is where the rubber meets the road. Forensic experts and client network teams work together to deploy and configure tools, contain the active threat, collect relevant data for analysis and remediate any security gaps within the network," he explains.
If it's not your IR provider taking the reins, the responsibility for the tech track usually falls to the IT department. Within the IT team, an IR manager may coordinate the effort, with security analysts undertaking the analysis and threat researchers who can provide context around information gathered.
It's also on the IT team to plan what steps will be taken to secure the environment and mitigate further exposure, identify impacted devices, data and log what sources are available, and engage with the company's disaster recovery program or business continuity plan to restore the impacted devices and keep the business operating.
The executive track, meanwhile, is focused on elements of risk. Damage to reputation, financing the response, business interruption and the potential for future litigation are all considered by the executive team.
According to Qualys' Paul Baird, the responsibility shouldn't just lie with the tech track (although it often does) as more senior department heads in incident management rooms means the information and messaging can be controlled.
"[IR] should involve a broader catchment that includes public relations, HR (If it is a staff data breach), legal and service delivery. Depending on the company and industry, it may also need teams responsible for things like manufacturing processes as well," he says.
Oisin Fouere, head of cyber incident response at KPMG UK adds that it's also important to keep customers, partners, suppliers, investors and regulators in the loop.
In some firms this responsibility falls

Email entry

IT service provider Greystone told TI of a customer who had suffered an email-based ransomware, though the customer could not be named for confidentiality reasons.
In the attack, emails containing malware were received by a member of staff, opened, leading to an infection, resulting in ransomware encrypting a large number of company files across the network.
The customer contacted Greystone and its team tracked and isolated the entry-point user, cutting off their device from the network.
A recovery process allowed compromised files to be restored and, to mitigate future attacks, the firm implement a Software Restrictions Policy and File Server Resource Manager to filter files.

within the comms team, but the main thing to ensure is that you have a spokesperson if an attack occurs and prepare content for a quick response to keep them informed.

Ransomware operators have the upper hand when the authorities are not notified, so it's also recommended to contact law enforcement too – while taking measures not alert the hackers.

Post incident, as soon as the main threat has passed, organisations are advised to conduct a full retrospective audit, "ideally without blame or scapegoats, and share their findings and steps taken with the world," according to Jack Garnsey, security awareness training product managers at VIPRE.

He adds: "Often, many ransomware attacks go unreported – and this is where a lot of criminal power lies. Full disclosure is helpful – not only for customers but also for other organisations – to understand how they can prevent an attack of this type from being successful again."

All at Sea

Scottish marine equipment firm Oceanscan works with the oil and gas, petrochemical, defence, and nuclear industries, serving over 1,000 customers across the globe

In September 2021, Oceanscan was victim of a sophisticated ransomware attack, encrypting multiple file layers and putting the company at risk of potential downtime and lost revenue.

"Everyone's initial thought is, 'We are doomed.' If attackers can infect organisations like the Pentagon and the CIA, then what is Oceanscan? Nothing," said head of IT Sukumar Panchanathan.

But the firm was partnered with disaster recovery provider iland in preparation for this very scenario.

Using US-based iland's disaster recovery as a service (DRaaS) and cloud backup system, Oceanscan had the security, replication and failover capabilities it needed to ensure the company's data stayed online and available.

With the company's on-premise environment compromised, but its workloads already successfully replicated to the cloud following the attack, Oceanscan decided to move away from its on-premise production environment entirely following the attack and leverage iland's cloud-based infrastructure, transforming the business.

How to protect your firm from attack

By Ann-Marie Corvin

Due to the sheer volume of ransomware and the efficiency with which attacks are carried out – not to mention the abundance of platforms, apps and IT tools that offer bad actors a way in – most experts believe that firms should take the stance that it's not a matter of if they get hacked, but when.

As a result, the mantra 'never trust, always verify' has become this decade's de facto cyber security approach. This strategy of 'zero trust' assumes that untrusted actors exist both inside and outside the corporate network and every user access request must be authorised. This also means deploying multi-factor authentication (MFA) to access IT systems and updated access lists, according to KPMG's Fouere.

"With a combination of asking all users to authenticate themselves on a regular basis to access a network and only giving people the rights and access needed to perform their role, risks are minimised and any incidents that do occur can be more easily contained."

Besides verification, the other pillars of zero-trust security include validating devices, limiting access to privileged users wherever possible, and then applying machine learning and AI to all these factors to step up the authentication processes where necessary.

Malware detection techniques are also recommended to prevent attacks before they infiltrate a network.

Lewis West, head of cyber security at Hamilton Barnes, broadly outlines three common methods of ransomware attack detection.

"Signature-based ones compare ransomware sample hash to known signatures; the second method compares new behaviours against historical data while the third, a deception-based method, use a 'honeypot' to deceive malicious actors into interacting with a decoy system to expose what the hacker's intentions are."

Ioan Peters, head of cyber risk at Kroll adds that deploying a managed detection and response (MDR) solution, benefitting from curated threat feeds, on-hand expertise and tactical advice can also mitigate some of the threats that are evolving daily.

Addressing concerns over software vulnerabilities, Nigel Thorpe, technical director at Secure Age adds that these can be alleviated in part by controlling and listing permitted

software within your organisation.

"Most business PCs are built to a standard which includes all the software which the user needs to do their work. There's rarely any need to add to this. So, if you deploy an 'application control' system which only allows software within that standard build to run, then any ransomware attempting to execute will simply not work. It's like the bouncer on the night club door – 'if you're not on the list you're not coming in'," he says.
He adds: "This approach avoids all the grey areas around the complicated

Nigel Thorpe, technical director at Secure Age

effort of trying to work out if every application, script or macro is likely to be malicious or not; it's a simple case of checking to see if it's on the list or not."
Given that ransomware attacks are rapidly evolving to counter preventive technologies, experts also believe that firms should also be taking a less static and more strategic approach to defence – which involves looking at recent data and pinpointing the most likely threats.

Securing SMEs

Research from cyber security risk rating firm RiskRecon reveals that data breaches within small businesses jumped 152% globally between 2021 and 2022, outlining a trend that sees hackers moving away from 'big game' and increasingly targeting the mid-market.
"Malicious actors are increasingly targeting SMEs – either to gain access to their sensitive data or to reach larger organisations through the supply chain – but despite the risks, SMEs don't necessarily have the skills or resources to build an advanced security architecture," observes Censornet's CTO Richard Walters.
So, what steps can SMEs take to defend against ransomware? The received wisdom within cyber security used to be that firms should have multiple vendors of firewall technology to prevent a ransomware attack. However, having seven or more different services to manage risk often requires a bigger team of IT security engineers, which SMEs don't typically have the capacity for.
Our security experts agreed that smaller firms would do well to kick start their security by learning to do more with less – consolidating security solutions to a single platform to manage the number of alerts that come through.
"Operating one single platform is easier to manage, eliminates complexity and enables business to respond to more complex threats at faster speed and with greater accuracy," says Walters.
Forcepoint's Willshire advises SMEs to create a unified strategy with a product "that can encompass the entire environment instead of a patchwork of products that can introduce risk inadvertently".
Others point out that there are also plenty of free or inexpensive measures that provide effective baseline protection against known risks. Illingworth of NormCyber, suggests setting passwords to three random words. "Organisations needn't bother with numbers and symbols anymore – cyber criminals can crack passwords like 'BusinessName2020!' almost instantly. Instead, the NCSC now advises organisations to use three random words, made up of upper and lowercase letters."
Illingworth also points out that multi-factor authentication is a free feature built in to most software applications today. "Even if a cyber criminal obtains the password, a unique six-digit passcode is often enough to stop them from gaining access to vital accounts – it's your second line of defence."
Keeping systems updated, rather than ignoring updates and installing antivirus software are other key measures all firms can take.

Training

Given that the weakest link in any organisation is generally agreed to be its people, Mark Brown, a behavioural psychologist and founder of cyber security training platform Psybersafe, believes that arming employees with training is an essential part of ransomware prevention.

> "Cyber security is all about human behaviour. Every individual is a potential target."
>
> Mark Brown, Psybersafe

"Cyber security is all about human behaviour. Our research shows that the biggest issue in developing a cyber secure workforce is target awareness – the realisation that you and I – every individual is a potential target.
"Once a person accepts this and believes it, their motivation to pay attention to cyber security messages increases, as does their willingness to adapt their behaviours and current ways of doing things," he says.
However, Brown adds that taking a 'tick-in-the-box' approach, providing a video or webinar once or twice a year, just doesn't work. "Training

needs to be continuous, engaging and practical for people to take note and implement the desired behaviours."
The psychologist also observes that organisations tend to silo day-to-day cyber security activity and don't involve other staff – which is usually to their detriment, he claims.
On this note, Trend Micro's Duke agrees that security teams need to be brought "into the fold" more so they can help foster good working relationships between teams and improve the speed of response, with established lines of communications making it easier to identify and remove potential barriers to IR before an incident occurs.

Call for backup

The reason a ransomware attack can be so devastating is because a business can find itself with no alternative but to pay to restore its data. However, if a company knows they can restore their data to a clean state due to a backup, they will have greatly minimised the disruption and pain associated with an attack.
According to Lawrence Perret-Hall, director at CYFOR Secure, when it comes to data backup, enterprises should follow the rule of three: smaller, more frequent and incremental back-ups for business restoration, alongside full back-ups, encrypted and stored on an entirely separate network. Finally, create a third set of long-term back-ups separately, and store them on tape.
"Ultimately, while it may sound excessive and expensive, having three lots of back-ups will be far more cost-efficient than falling victim to ransomware unprepared," he says.
"What's more, keeping separate back-ups will avoid the issue we see time and time again in ransomware recovery, where back-ups themselves are infected because they are stored on the same network in order to reduce recovery time," Perret-Hall adds.

WFH risks

As more of the workforce transitions to working from home or hybrid working models, it's also vital that firms identify the vulnerabilities that external remote services present, particularly ones that were set up hastily, as a reaction to the pandemic.
"The traditional 'castle and moat' approach to cyber security no longer works since we're no longer barricaded inside the 'castle'," explains Hamilton Barnes' Lewis West, who adds that investment needs to come in three areas.
"Improving the tooling in place; improving the attitude of employees to security risks and investing in the right expertise that can support a

Lewis West, head of cyber security at Hamilton Barnes

business's cyber security. Businesses should also use web security solutions that manage web activity of remote employees by inspecting all SSL (encrypted) traffic to expose threats," West adds.
Todd Moore, VP for encryption products at French aerospace firm Thales's cyber security division, believes that data encryption can act as an essential line of defence against ransomware attackers targeting remote networks.
"When cyber criminals infiltrate the home or remote network, it's essential that any data that's stolen is properly protected so that it can't be read by unauthorised actors. The keys used to encrypt data should be centrally managed through multi-level access controls to ensure that encryption cannot be "undone" by hackers," he says.

Cyber Insurance

While cyber security insurance cover falls under the mitigation category rather than prevention, most insurers will look for evidence of a well-funded and well managed cyber security programme.
According to Jennifer Mulvihill, business development head at cyber-Insurance and legal firm BlueVoyant, the severity and frequency of ransomware attacks has meant that cyber insurers are increasing their premiums and designing stricter and more technical underwriting guidelines.
"If your company can demonstrate its well-prepared for a cyber-attack, cyber insurance premiums may be reduced, or at least barred from a significant increase," she says.
These requirements may include basic cyber security best practice such as the implementation of MFA across the enterprise and a robust MDR that provides 24/7 monitoring.
"Carriers are also seeking evidence that the business has dedicated experts that allows them to effectively respond to a cyber-attack, or at least have an IR retainer in place to partner with outside forensic experts," Mulvihill adds.
When shopping around for insurance, to select the appropriate cover, businesses should consider the importance of each system or data set to their operations and check whether losses to third parties are covered, as well as looking at what other services the insurer offers in an event of an attack to response.

Future threats and how to face them

By Ann-Marie Corvin

We asked six security experts how the threat landscape is likely to evolve.

"Ransomware incidents in Europe are likely to stabilise but will continue to grow dramatically in other EMEA regions. As these move towards a more digital economy, they are increasingly exposed to attacks. Cyber criminals are taking what they have learnt from Europe and are applying these lessons to a new ground."

Quentyn Taylor, Canon EMEA information security and global incident response senior director

"With attacks still generating so much money for criminals, the number and impact of ransomware attacks will increase but this could lead to increased cybersecurity regulation and prevention guidance.

However, the reality is that the future of ransomware is very much here already. The number of hacks on IoT devices, reusable third-party software and OT will only continue to grow, given the success bad actors have seen in recent years."

Daniel Dos Santos, head of security research, Forescout

"Ransomware gangs are becoming hack-everything-gangs. They will do whatever it takes to get money. The "gold" ransomware gangs have is not the ransomware. It's the access to the victim's passwords and systems. With that they can do anything they want to do (steal data and passwords, install crypto mining trojans, create botnets, do DDoS attacks, send out phishing attacks to name but a few examples). The ransomware gangs of the future therefore will look to every compromised victim as a potential bag of money and ask themselves how they can maximise their potential revenue. Eventually it will be' good guy bot versus bad guy bot' and the best bots with the best AI-algorithms will win."

Roger Grimes, data driven defence evangelist at KnowBe4 (knowbe4.com)

"As defenders got better at doing backups and "simply" restoring lost files, ransomware writers also adapted. Now they exfiltrate files and threaten to release them unless the ransom is paid. They also message the victim's customers and threaten them unless they pay. I've personally been on the receiving end of that after a data breach of one provider, receiving emails that have my name and home address and threatening to perform a home invasion and kill my family unless I pay them."

Michael Smith, field CTO, Neustar Security Services

"Given the history of ransomware and how the threat has developed in recent years, it's likely that we will see smaller franchise-style ransomware operations which will either switch to pure exfiltration and abandon encryption of devices entirely or use ransomware software purchased from developers on criminal forums. Exfiltrating data from specific machines is easier than spreading ransomware across a whole network. It's less noisy and there is no complicated or unsuccessful process of trying to restore encrypted files upon a successful negotiation, a frequent issue."

Cian Heasley, security consultant, Adarma

"As fuel bills continue to be a growing concern for businesses and consumers at present, threat actors will weaponise operational technology environments more successfully than ever before, striking when energy providers are otherwise preoccupied. Given the global energy industry is already facing a turbulent time, we are most likely to see a major energy supplier taken offline, with threat actors tapping into these vulnerabilities and holding the service to ransom for their own gains."

Todd Moore, VP for encryption products, Thales