
FORINT
digital investigations
RANSOMWARE
EXPOSED!

MEET RANSOMWARE, THE STAR OF THE SHOW

The villain in many of today's cybersecurity tales of woe is ransomware. This multifunctional weapon can be wielded to great effect by savvy cybercriminals, enabling them to carry out operations that can bring companies to their knees. It is also the favored weapon of nation-state threat actors.

It's no accident that ransomware is the star of the show in cybercrime today. A complex web of influences and an unexpected wealth of opportunity has given cybercriminals a golden ticket to profit from ransomware attacks - and they're not wasting it.

Go behind the scenes of the ransomware landscape to learn more about its smashing success and see what you can do to secure your systems and data before it's too late.

THESE 10 BLOCKBUSTER STATISTICS TELL THE STORY OF RANSOMWARE RISK

Ransomware has been a smash hit for cybercriminals, breaking records in an unprecedented wave of cybercrime. These 10 statistics illustrate the epic success of ransomware and how it has evolved to become the cybercrime superstar that it is today.

1	About 61% of organizations worldwide experienced a damaging ransomware incident in 2020.
2	Ransomware demands are already up by more than 40% in 2021.
3	About 85% of all ransomware attacks target Windows systems.
4	Ransomware impacted two in five SMBs in 2020.
5	Ransomware incident downtime has expanded to 23 days in 2021.
6	The average ransomware payment in the third quarter of 2020 was $233,817.
7	The average ransom demand has increased by 47% over 2020.
8	Ransomware accounted for 41% of cyber insurance claims filed in 2020.
9	More than 80% of reported security incidents are phishing related.
10	Hackers attack every 39 seconds or at an average of 2,244 times a day.

What the Critics Are Saying:

Microsoft Incident Response:

Ransomware has remained the most common reason behind this team's engagements since 2019.

IBM Security X Force:

Ransomware accounted for one in four attacks that the team remediated in 2020.

CISA:

The agency opened a new one-stop resource center to help stem the rising tide of ransomware attacks in January 2021.

RANSOMWARE RISKS SURGE WHEN INDUSTRIES ARE IN THE SPOTLIGHT

The need for adequate preparation cannot be emphasised enough; however, it is also important to note that some forces are outside your control. Ransomware risk often ebbs and flows, based on an industry's current relevance.

Desirability of data is a powerful influence on a sector's likelihood to attract bad actors.

Sectors that are especially stressed are prime targets because cybercriminals know that organizations in those industries are likely to pay them to resume operations quickly.

The COVID-19 pandemic is a perfect example of how risk changes as different industries find themselves in the spotlight. At the beginning of the pandemic, hospitals were firmly in cybercriminals' sights. However, as the world traversed the path from treatment to vaccination, risk shifted from hospitals to university laboratories to research facilities to drug manufacturers and finally cold storage transportation companies.

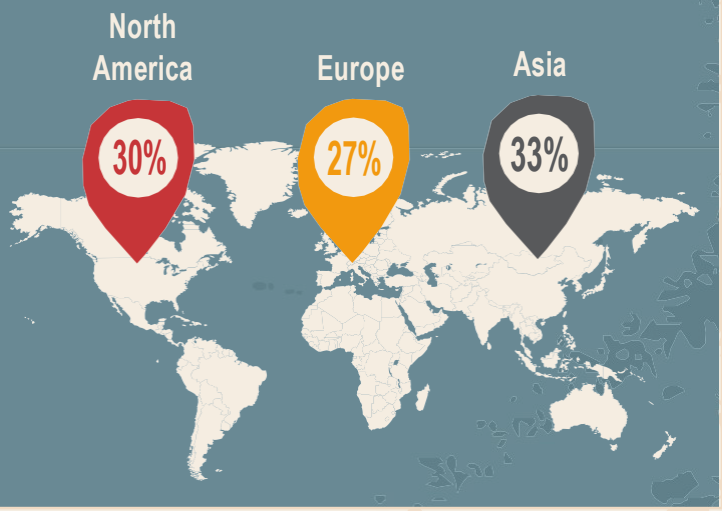
The IBM Security X-Force published a breakdown of their 2020 ransomware incident response activity by industry and the percentage of total calls that they represented. Companies in these three sectors were at the top of the list:

25%	17%	13%
Manufacturing	Professional Services	Government Entities

Source: IBM Security Intelligence

On Location: Prime Spots for Attack

Ransomware attacks in 2020 are broken out by geography as follows:



THE CAST OF CHARACTERS

Ransomware has many variations, but most of it conforms to one of two profiles when doing its dirty work.

Crypto Ransomware

Crypto ransomware encrypts data, like files on a computer, making it inaccessible. Cybercriminals then offer to sell the victim the decryption key. This type of ransomware does not impact the machines it is used on, just the data.

Locker Ransomware

Locker ransomware makes devices, like computers or machinery, unusable. Cybercriminals will offer to unlock the affected devices on payment of the ransom. This type of ransomware is typically used in infrastructure attacks or attacks against manufacturing targets.

RANSOMWARE SUBTYPES

Double Extortion

This is the ransomware du jour in circulation, accounting for 50% of ransomware attacks in 2020. In a double-extortion ransomware attack, cybercriminals deploy ransomware that creates two adverse effects for the victim — encrypting data and locking machines at the same time. The gang then demands payment to unlock machines and decrypt data.

Triple Extortion

This up-and-coming variety of ransomware causes immense trouble for the victims and has the potential to earn cybercriminals high profits. Going one step further than a double-extortion attack, this variety produces three adverse effects for its target. For example, the ransomware could lock machines, encrypt data, and deliver a distributed denial of service (DDoS) attack against the hapless victim. Thecybercriminals then demand payment to undo all three negative effects.

BEHIND THE SCENES:
THE IMPACT OF RANSOMWARE

The effects of ransomware on an organisation can vary wildly — from minor disruptions in service to a full shutdown — as remediation and recovery take place. In companies that maintain high cyber resilience with strong incident response planning, the effects will be blunted. Unfortunately, only about half of all businesses have a cybersecurity incident response plan ready to swing into action in the event of a cyberattack. For companies that aren't quite as ready to handle trouble, the impact can be catastrophic.

Companies impacted by ransomware lost an average of six working days.

An estimated 37% of companies experienced downtime that lasted one week or more.

About 60% of companies that suffer a cyberattack like ransomware go out of business.

TO PAY OR NOT TO PAY?

It would seem the most direct path back to normal operations would be to simply pay the ransom, and indeed many companies choose to go that route. In fact, 52% of ransomware victims chose to pay the ransom in 2020. But that's a bad idea for many reasons.

- It's illegal to pay in many regions, but NOT in the UK
- Ransom payments are growing increasingly unlikely to be covered by cyber insurance.
- Paying carries no guarantees that stolen data won't be sold or copied.
- Payment does not ensure that the cybercrime gang won't leave a backdoor in the victim's systems.
- Only 1 out of 3 organisations that paid a ransom got what they were promised.

FOLLOW THE MONEY

How do cybercriminals profit from ransomware? The money a ransomware operation generates travels all over the dark web. Major cybercrime gangs that claim responsibility for most ransomware attacks aren't the only players that get paid handsomely. Ransomware money also trickles down to a galaxy of affiliates, specialists and freelancers that support the major gangs - and everyone has a good chance of walking away with substantial profit.

Major gangs often run their scams through affiliates, so the actual attacker is very likely an independent contractor of sorts.

An affiliate may be a smaller gang or just a group of freelancers getting together for one job.

or

Freelancers may be specialists in a particular technique or technology like PowerShell scripts.

If the operation is a win, the attackers will then notify the umbrella gang that they've succeeded.

Usually, the umbrella gang will handle the process of informing the victim that they've been hit and negotiating payment in cryptocurrency.

AND

The umbrella gang will take its cut, usually 10% – 20% of the take, and the rest goes to the affiliate.

The affiliate then pays out to any freelancers and keeps the rest of the loot.

Most umbrella gangs maintain their own dark web sites where they recruit affiliates and announce their victories. Typically, when an attack is successful, perpetrators use these websites to claim responsibility for the attack, display a sample of the stolen data and announce the ransom demand. Attempts to shame organisations into paying by publicly exposing the company's cybersecurity failure are a time-honored tactic, especially if the victimised organisation denies the attack.

Publicity is also an essential component of the ransomware racket. Just like any other business, ransomware gangs attract talent and demonstrate their strength through their reputations. Some major cybercrime gangs are also in regular contact with industry experts and journalists. The REvil organisation, a leading Russia-based gang, has a formal communications staff that handles press releases, announcements, and interviews with journalists just like any other business.

COMING SOON TO AN INBOX NEAR YOU:

MORE RANSOMWARE RISK

Most businesses aren't ready to handle a ransomware attack touching down inside their environment. About 50% of IT professionals don't believe that their organisation is ready to defend against a ransomware attack. Today's volatile threat landscape is a minefield of danger for those hapless businesses as they contend with risks like these.

Nation-State Cybercrime

Ransomware is the favored tool of nation-state cybercriminals, especially when used against strategic targets that serve as linchpins between multiple economic sectors like power plants or pipelines. These extremely sophisticated organisations are typically propped up by hostile governments, and they are very good at choosing strategic targets, often reaching into their target's supply chain to find an easy way to slip inside the target's security.

Supply Chain or Third-Party Risk

No business is an island. Every company maintains relationships with manufacturers, distributors, service providers and other organisations that enable them to do business together. Those relationships create records with proprietary information, account credentials and other data that's ripe for the picking by cybercriminals. An estimated 22 billion new records poured onto the dark web in 2020, ready to fuel future cybercrime and raise risk for every business.

Unsuspecting Targets

Attacking organisations that aren't normally in the line of fire has proven to be a bonanza of opportunity and profit for cybercriminals. Ransomware strikes against targets that aren't historically known to maintain high security like trucking companies, sports clubs and even a flavor manufacturer started ramping up in early 2020 and that trend is still on the rise. These small companies also have valuable, exploitable connections to the bigger, more secure companies that they do business with, giving cybercriminals an easy way to open a backdoor that allows them to infect a high-value target with ransomware too.

MAKE EVERY EMPLOYEE PART OF THE ENSEMBLE

Protecting businesses from phishing must be a top goal of any security plan - and one of the best ways to do that is by increasing employee security awareness with a powerful training solution like BullPhish ID.

In a volatile risk atmosphere, companies need every employee to feel invested in maintaining security. Security awareness training that includes phishing simulation exercises recruits everyone to the security team, reducing an organisation's chance of experiencing a damaging security incident like ransomware by up to 70%.

BullPhish ID is loaded with features that make training a breeze for both employees and administrators and includes:

Access to our extensive library of engaging training videos in eight languages, and dozens of plug-and-play phishing simulation kits that are ready to deploy immediately.

A personalised training portal where users can access their assigned courses at their convenience, watch training videos and take testing quizzes. Our built-in learning management system makes it easy for admins to assign, track and report on training.

The option to customise every aspect of a phishing simulation campaign, from emails to URLs and attachments, enabling administrators to simulate real threats that employees face daily.

Learn more about our Phishing Solution BullPhish ID in this video:
Charge Into Cyber Safety With BullPhish ID Security Awareness Training

DON'T LET CYBERCRIMINALS BEHIND THE VELVET ROPE

One of the biggest goals of any cybercriminal who comes phishing around in a business is to obtain credentials that allow them to penetrate systems, steal data and deploy ransomware. The more powerful the credential, the deeper into an organisation a cybercrime gang can slip, enabling them to do catastrophic damage. Sometimes, that credential can also empower cybercriminals to penetrate a business partner's network, creating a devastating ripple effect.

That's what makes secure identity and access with a dynamic solution like Passly a clutch performer. It takes the power out of a phished password, making it easy for IT teams to stop an intruder at the door with built-in functionality that protects business systems and data automatically.

Passly includes every tool that businesses need at their fingertips to seamlessly control who accesses their systems and data, at what level, at any time, from anywhere.

Multi-Factor Authentication (MFA)

This is the single most powerful tool in a company's arsenal to keep unwanted visitors out of their systems and data, stopping 99% of password-based cybercrime cold. MFA with Passly also offers multiple options for token or code delivery for convenience.

Single Sign-On (SSO)

Create a stronger defense by lowering the number of access points to the heart of businesses. Giving every user their own personalised launch pad to access business applications not only enables techs to easily add and remove permissions, it also enables them to quickly isolate accounts that may be compromised to minimise damage in case of emergency.

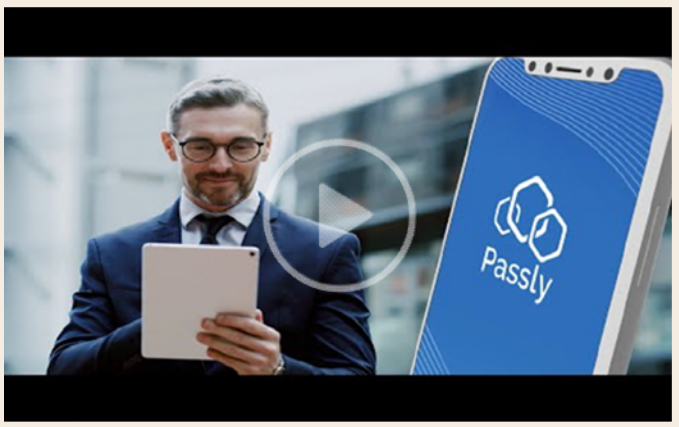
Automated Password Resets

Why wait until a tech can address a trouble ticket to reset a password? Immediate, automated password resets make it easy for employees to quickly change a password themselves whether they believe that it's been compromised or if they've just forgotten it.

Secure Shared Password Vaults

Store especially powerful passwords, like privileged credentials and essential hardware passwords, in a secure vault that every tech can access, reducing the time it takes to track down a much-needed password to adjust permissions or perform defensive actions in case of trouble.

Learn more about Passly in this video: Secure Identity and Access Management



THERE'S NO COMEBACK FROM RANSOMWARE

Ransomware devastates the companies that fall prey to it. Thriving dark web data markets and a wide array of eager freelancers make running a ransomware operation both easy and profitable, ensuring that it won't go out of fashion anytime soon. The sad truth is that piloting a successful ransomware attack is all too easy for cybercriminals in a world where many businesses haven't taken action to reduce their attack surface.

ID Agent can help reduce the risk of a disastrous encounter with ransomware through the strength of our digital risk protection platform. Contact one of our solutions experts and let's start putting affordable, effective cybersecurity protection in place to stop threats like ransomware dead in their tracks.

Learn more about Forint: https://www.forint.co.uk/

Book a personalised demo: https://www.forint.co.uk/contact