



UK RANSOMWARE TRENDS: LESSONS FOR 2023

www.jumpsec.com

Content

Introduction	03
Other influences	08
The UK's most prevalent threats	12
UK Sector-by-Sector Analysis	20
What can we expect in 2023?	26



SEAN MORAN

Researcher - Sean is a researcher and writer with a keen interest in geopolitics and its impact on the cyber security industry.



DAN GREEN

Head of Solutions - As Head of Solutions at JUMPSEC, Dan is responsible for shaping the solutions that JUMPSEC offer, working with our clients to ensure we deliver the outcomes they need.



JOHN FITZPATRICK

CTO - John is respected as one of the foremost researchers and leaders in the field of super computing and cyber security.

JUMPSEC threat intelligence analysts track global ransomware activity using a mixture of manual investigation and automated bots to search or 'scrape' the public-facing domains of ransomware threat actors. The raw data is then enriched by investigating the geographic location, industry sector, size, and financial profile of each targeted organisations.

Introduction

Ransomware has been a major cyber threat globally since late 2019 and is a top concern for just about every organisation regardless of industry or business model.

After year-on-year increases in ransomware attack figures, competing sources have provoked debate on whether ransomware rose or fell as a risk in 2022.

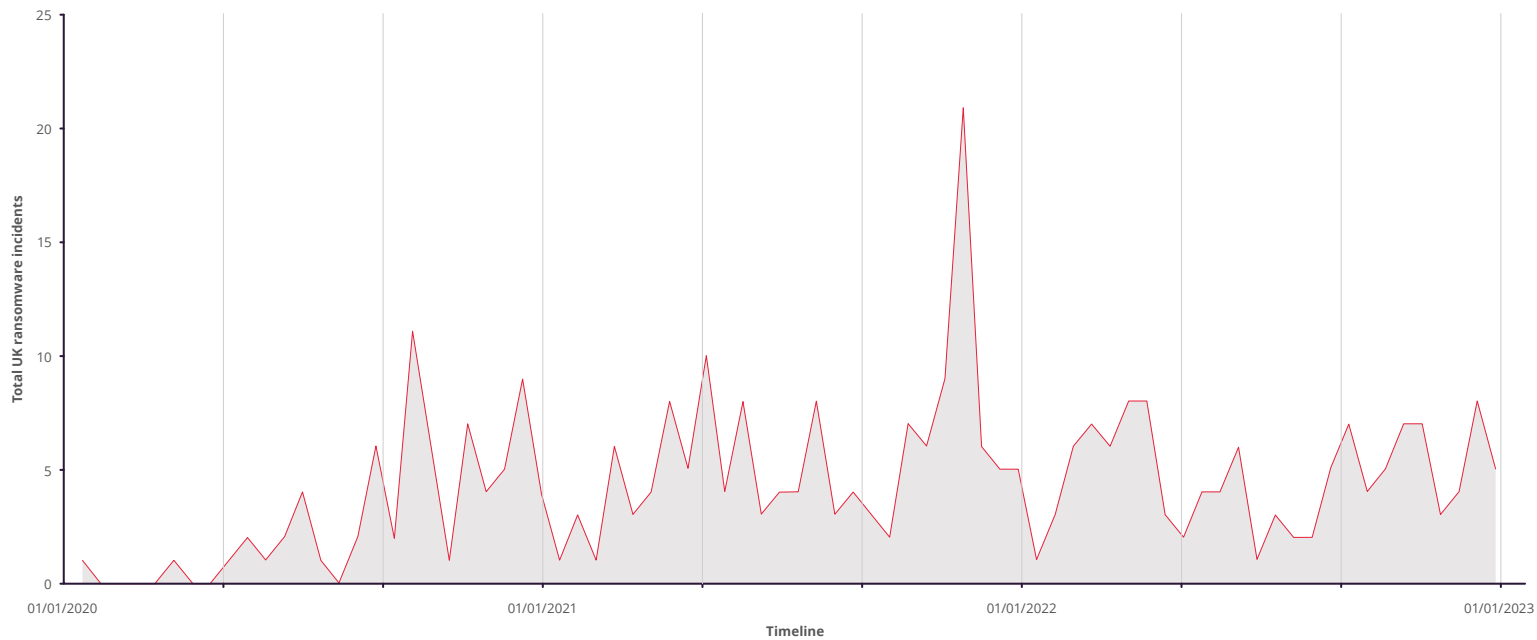
From one perspective, there is a growing consensus and evidence to suggest total attack rates may have lessened, substantiated by falling reported cryptocurrency revenues for ransomware groups.

Conversely, the narrative of exponential growth which has accompanied ransomware since 2019/20 still carries significant momentum, with announcements that 2022 was a 'breakout year'¹ for ransomware – despite evidence that 2022 showed a less dramatic rise in activity.²



Globally in 2022, JUMPSEC's data shows that attacker reported ransomware rates experienced diminished growth compared to previous years. However, **attacker reported incidents in the UK specifically have increased by a further 17% in 2022**, meaning that from a UK perspective at least, any statements about the diminished threat of ransomware should be met with a degree of caution. Furthermore, the initial data for 2023 shows signs of an uptake in UK ransomware activity.

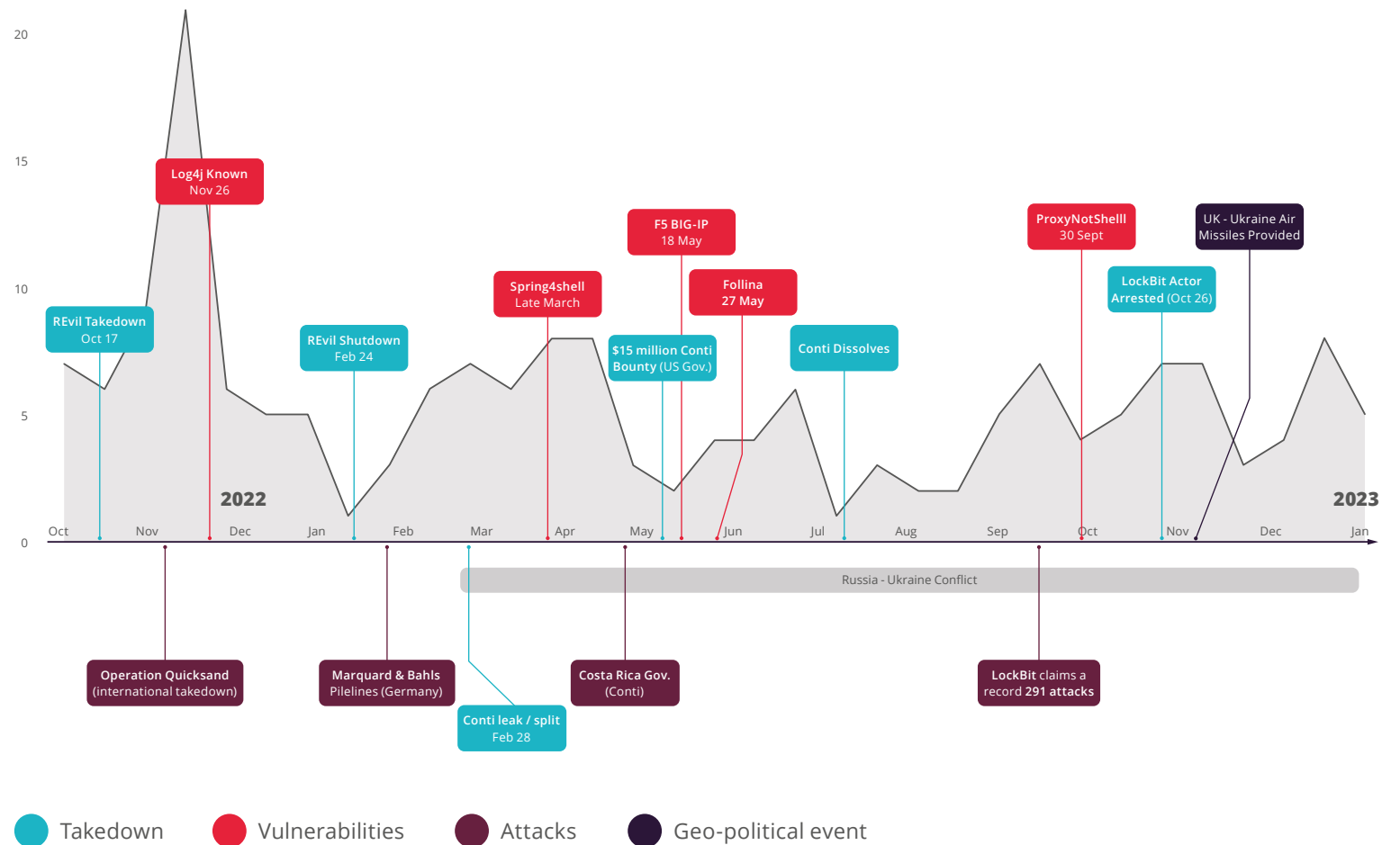
Total UK ransomware incidents (2020-July 2022)



Total UK cases 2020-2023. Total UK reported attacks increased by 17% in 2022 compared to 2021, although the rate of attacks broadly followed a similar pattern to the previous year.

New and emerging vulnerabilities are likely to increase the damage ransomware groups can inflict on organisations following discovery and exploitation. New vulnerabilities such as Spring4Shell, Follina and ProxyNotShell were identified and exploited in 2022, however, not to the same degree as Log4j in 2021.

In 2022, at no point did total attack rates reach the record high of November / December 2021, which saw a total of 20 attacks in the UK over a two-week period – primarily due to the widely exploited Log4j vulnerability.



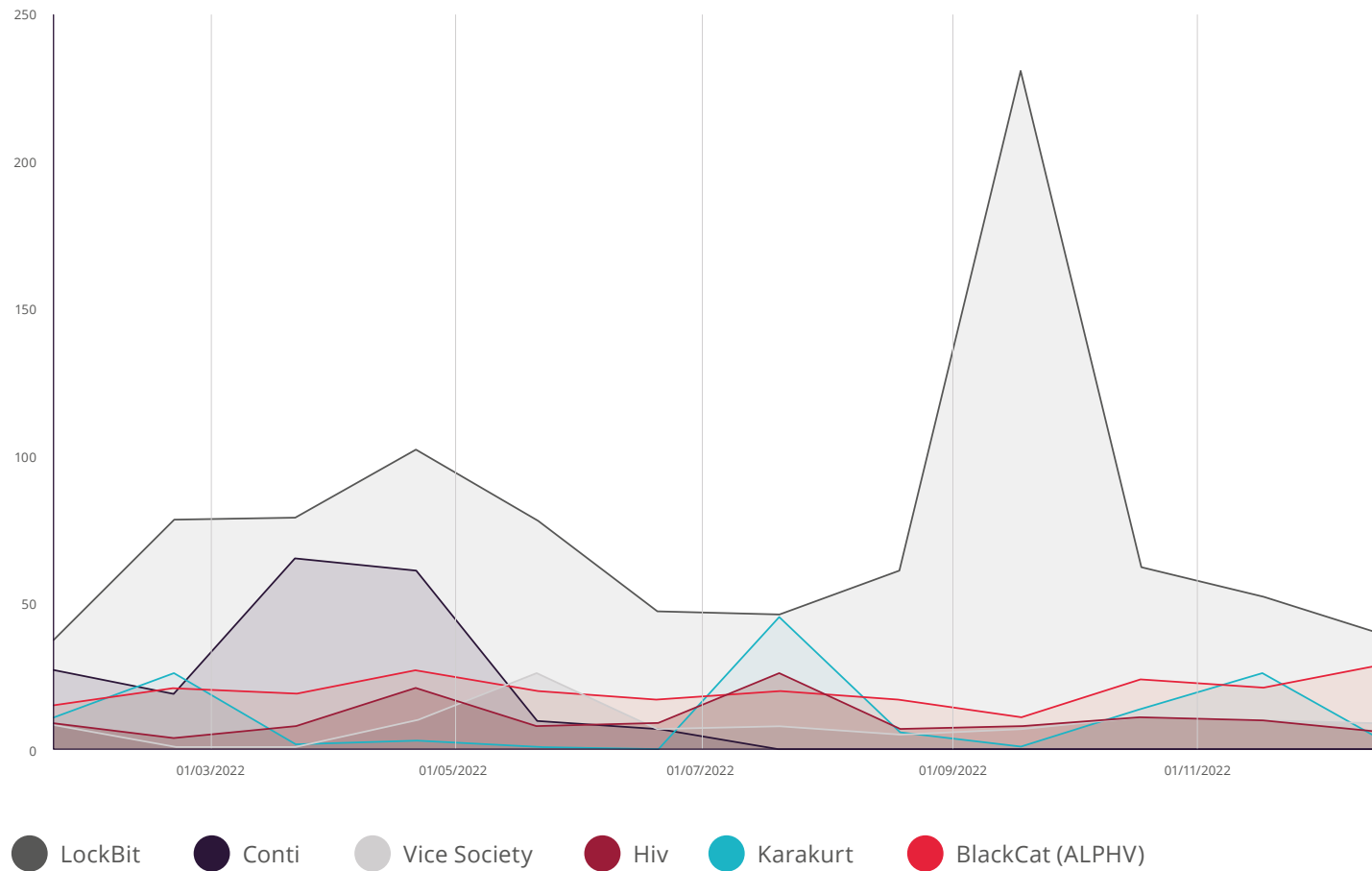


Total activity in the UK overlaid with a timeline of major cyber security events.

Perhaps more influentially in 2022, **new threat actors** have become more prominent in the ransomware space following the disintegration of Conti and REvil, formerly the largest ransomware players, and key actors in the December 2021 spike.

After the decline of Conti in May, attack rates fell mid-way through the year, before rising again over the Autumn due overwhelming to the resurgence of **LockBit**.

Lockbit have since taken the mantle as the largest ransomware threat by some distance, both globally and in the UK, claiming over 52% of global reported ransomware attacks. In September alone, Lockbit registered a total of 291 total attacks in just two weeks – the most recorded since the ransomware wave began in 2019.



Ransomware groups such as Karakurt and BlackCat have also emerged as more prevalent threats, while others like Vice Society have maintained a consistent presence. Like Lockbit, these groups operate a Ransomware-as-a-Service (RaaS) model which is enabling a greater number of technically unsophisticated cybercriminals to become effective ransomware actors without the skills once required to execute an attack.

The most prevalent threats in the UK in 2022. With evidence that individuals formerly operating as part of Conti likely redeployed to other ransomware groups, this may have contributed to the period of reduced activity mid-year, followed by a subsequent surge.



Other influences

Geo-political events have impacted the evolution of ransomware in 2022. Hactivist groups with allegiances to Russia have emerged and are conducting DDoS attacks which may increase the susceptibility of organisations to ransomware, targeting private corporations, hospitals, government agencies and national infrastructure, with reports suggesting links exist between to known ransomware threat actors and hactivists.³

Pro-Russian Killnet for example threaten action against the UK specifically in November.⁴ Such groups tend to retaliate following geopolitical events deemed unfavourable to their cause, which in November was nominally the UK's support for Ukraine with anti-air missiles.⁵ Although some may be rightly sceptical about whether Russian hactivism translates to real world attacks, nation states also use cyber attacks as a form of retaliation as part of 'grey zone' military tactics.

For a more concrete example, recent research shows that after Finland joined NATO in July DDoS attacks rose significantly. Despite relatively a relatively low volume immediately after joining in July, it wasn't until September two months later that attacks began to increase dramatically.⁶



The changing rate of ransom payments may also influence ransomware trends or alter the strategies deployed by attackers. While close to impossible to completely verify, recent Chainalysis research on the technical side of crypto payments indicates that total payments decreased from \$766m to \$457m in 2022.⁷ However, fewer ransom payments do not necessarily mean less damage to organisations. A survey of affected victim organisation in 2022 showed an increase in respondents who specified lost revenue (56%) and customers (50%) as a result of a ransomware attack – a reminder that direct ransom payment figures are not the only indicator of ransomware’s impact.⁸

Reportedly increased investment in security in 2022, and a shift from denial of cyber security issues to active engagement, may have also impacted ransomware trends. The UK Cyber security sectoral analysis 2022 report shows organisations are investing – total annual UK revenue within the sector reached £10.1 billion in 2022, an increase of 14% since 2021, and the industry saw an increase of 6,000 cyber security employee jobs within the last 12 months (increasing 13% from 2021).⁹



48%



System HACKED

Law enforcement action was diminished in 2022 from 2021's physical shut down of REvil through bilateral action with Russia. The most high-profile efforts from Western authorities' to combat ransomware in 2022 involved threatening action against Conti (setting a \$10 million bounty, contributing to their dissolution), and an arguably more effective remote disruption operation conducted against Hive ransomware (achieved through international cooperation between US, Dutch and German authorities).¹⁰ Although less verifiable, other reports suggested Lockbit were also 'hacked back' on the behalf of a victim organisation in retaliation for an attack, which may indicate a shift in the strategies being deployed to combat ransomware.

That said, additional preventive measures have been imposed on organisations, increasing the threat of prosecution for paying a ransom. The UK's Office of Financial Sanctions Implementation (OFSI) recently released a 'Ransomware and Sanctions' guide which stressed the impact of ransomware payments, and reminded organisations of its power to impose statutory maximum penalty more than £1 million or 50% of the value of the breach.¹¹

Other nations have also pushed more aggressive sanctions on ransomware. For example, the introduction of more stringent reporting regulations across the EU and U.S., and Australia's recent steps toward the outright banning of ransomware payment.¹²

Re-brands and internal splits seen in 2021 and early 2022 have not featured in the same vein in recent months, as Lockbit in particular have demonstrated unparalleled longevity in an often-chaotic landscape generally marked by instability.



New Vulnerabilities

How effectively organisations patch, and how effectively certain industries implement effective controls is likely to impact ransomware trends overtime



Re-brands / Internal splits

Re-branding to evade unwanted attention and internal turmoil disrupts ransomware groups and may limit their ability to execute attacks



Geo-political events

The Russia-Ukraine war has produced new malware and may limit law enforcement. The conflict has also caused problems for ransomware groups (i.e. Conti)



Law Enforcement Action

Further ransom payment and insurance regulations may limit attacker's profits. International law enforcement cooperation also works to disrupt threat actors.



An overview of the factors contributing to changes in ransomware trends.

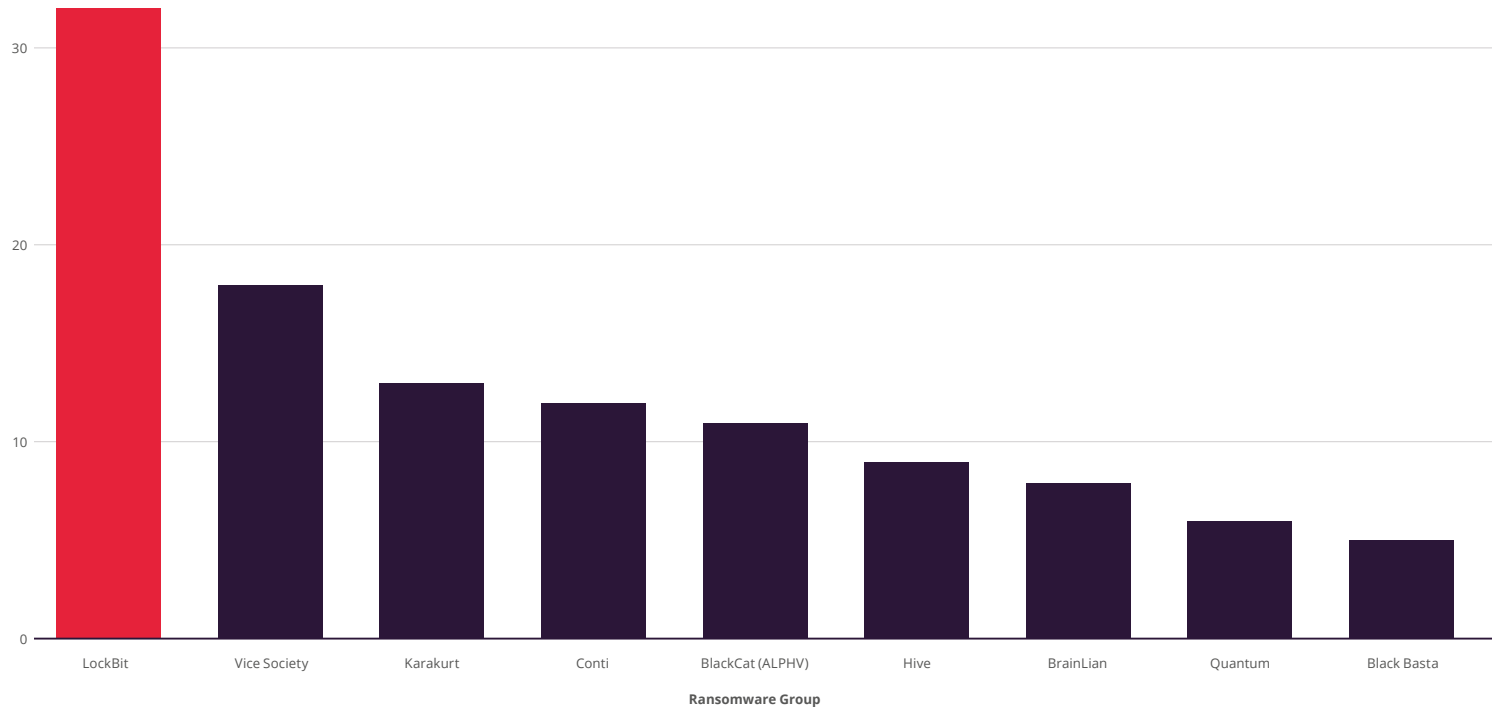


The UK's most prevalent threats

On a global level at least, JUMPSEC's findings appear to conflict to a degree with NCSC's expectation that 'a more diverse and capable ransomware landscape' would emerge in Conti's absence.¹³

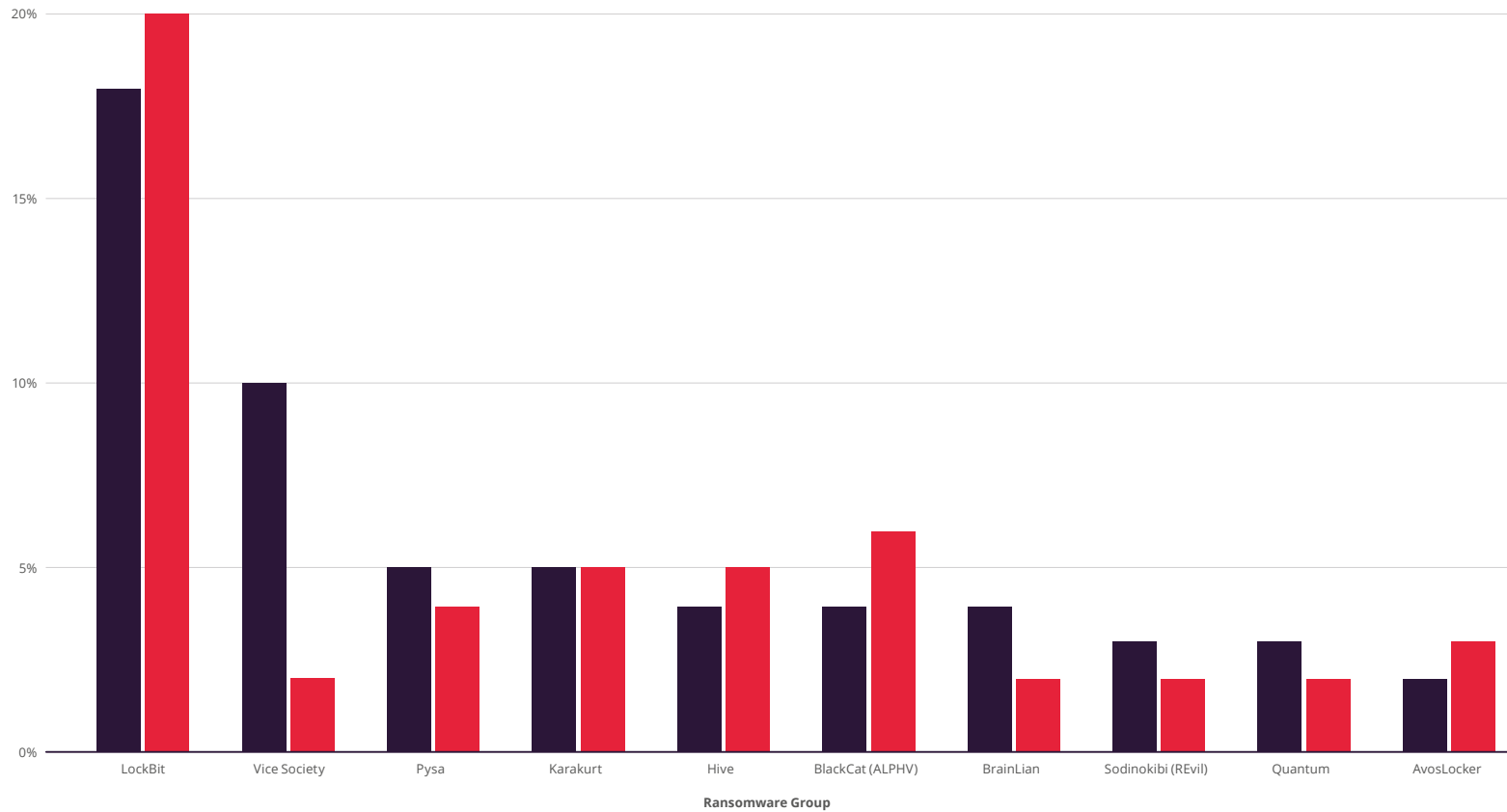
Lockbit have taken the mantle from Conti as the most prevalent ransomware both in the UK and globally, accounting for 52% of attacks. Lockbit's activity sparked globally and in the UK in September 2022. Notable recent attacks on UK organisations include Royal Mail, Ion Trading (the City of London), and Pendragon.

For UK-specific attacks, Lockbit were the most prevalent threat in 2022.



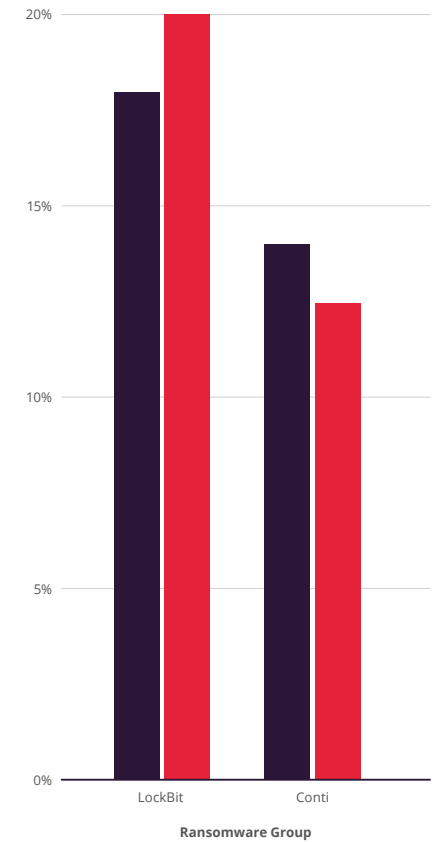


The proportionate impact of the 10 most prevalent ransomware threats on UK and US organisations



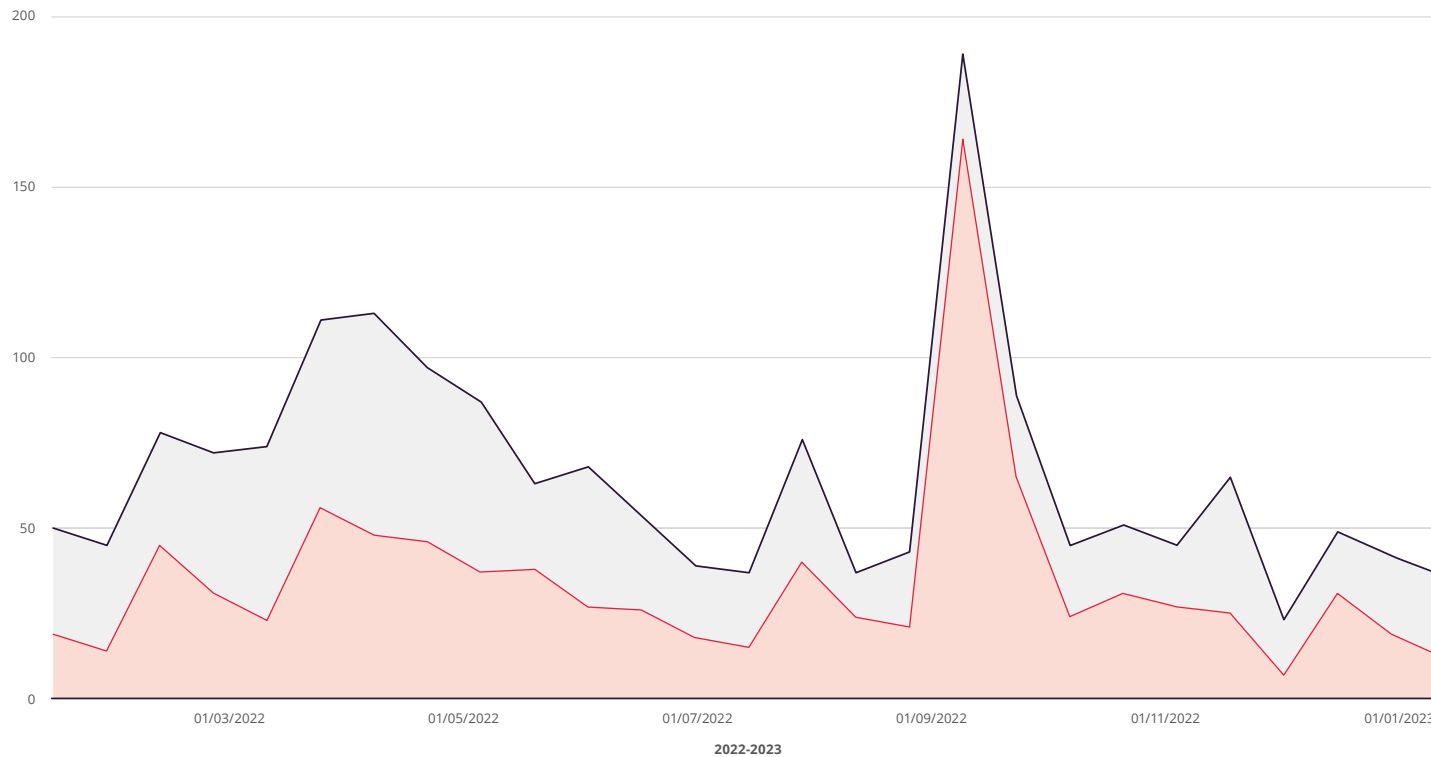
● UK ● USA

How Lockbit compare to the now defunct Conti - the former most prevalent threat globally






LockBit accounted for 52% global ransomware attacks in 2022



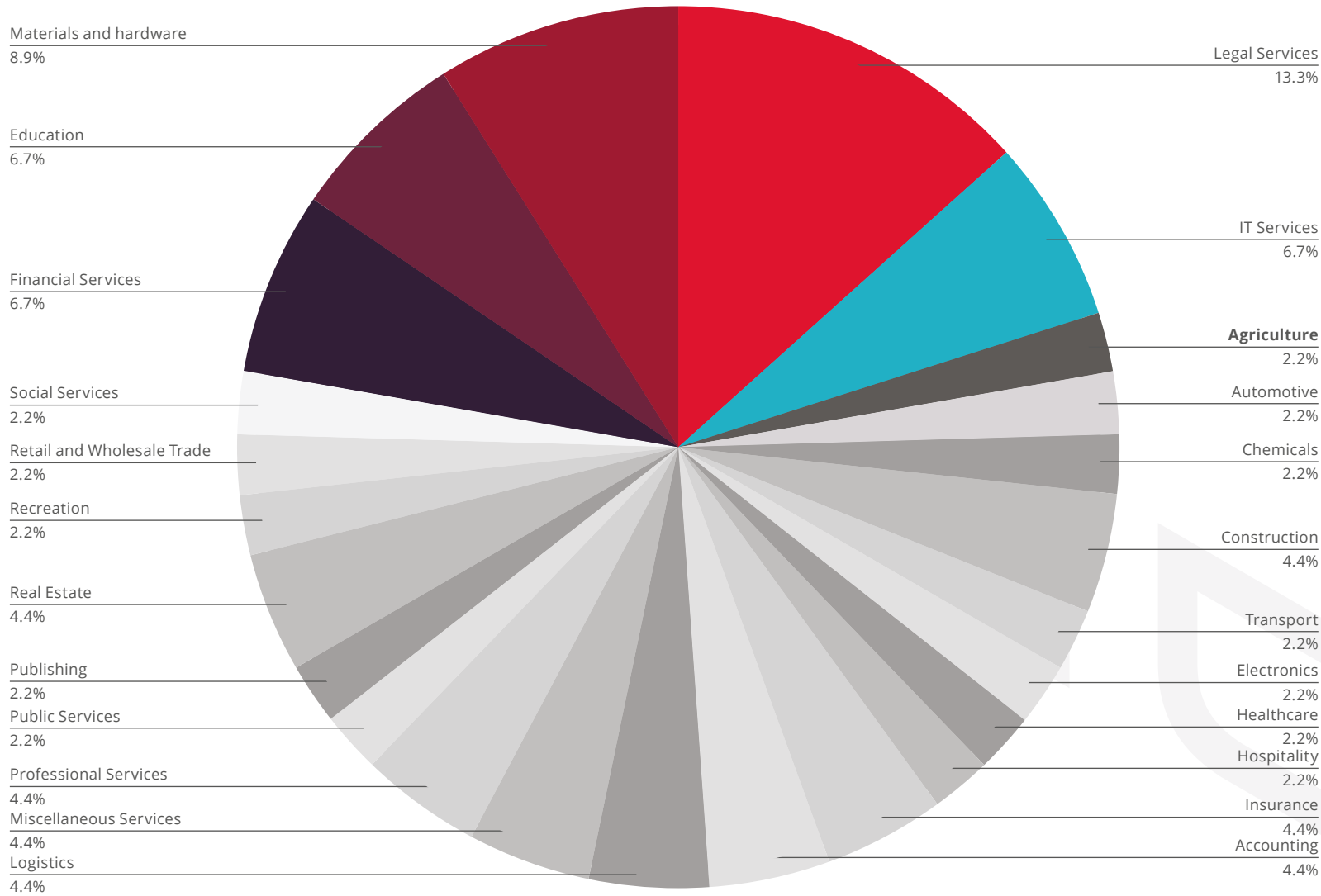
● LockBit Global Total ● Global Total

 The proportionate impact of Lockbit on the global ransomware landscape (52% of global attacks).

However, the total attack figures alone are only part of the story. In terms of the financial profile of targeted UK organisations, Lockbit are not the primary threat to more typically 'cash rich' organisations. Karakurt (thought to be an offshoot or rebrand of Conti) have emerged as a threat both in the UK and globally and have predominantly been responsible for attacks on large UK organisations with Cash in the Bank assets exceeding £20 million.



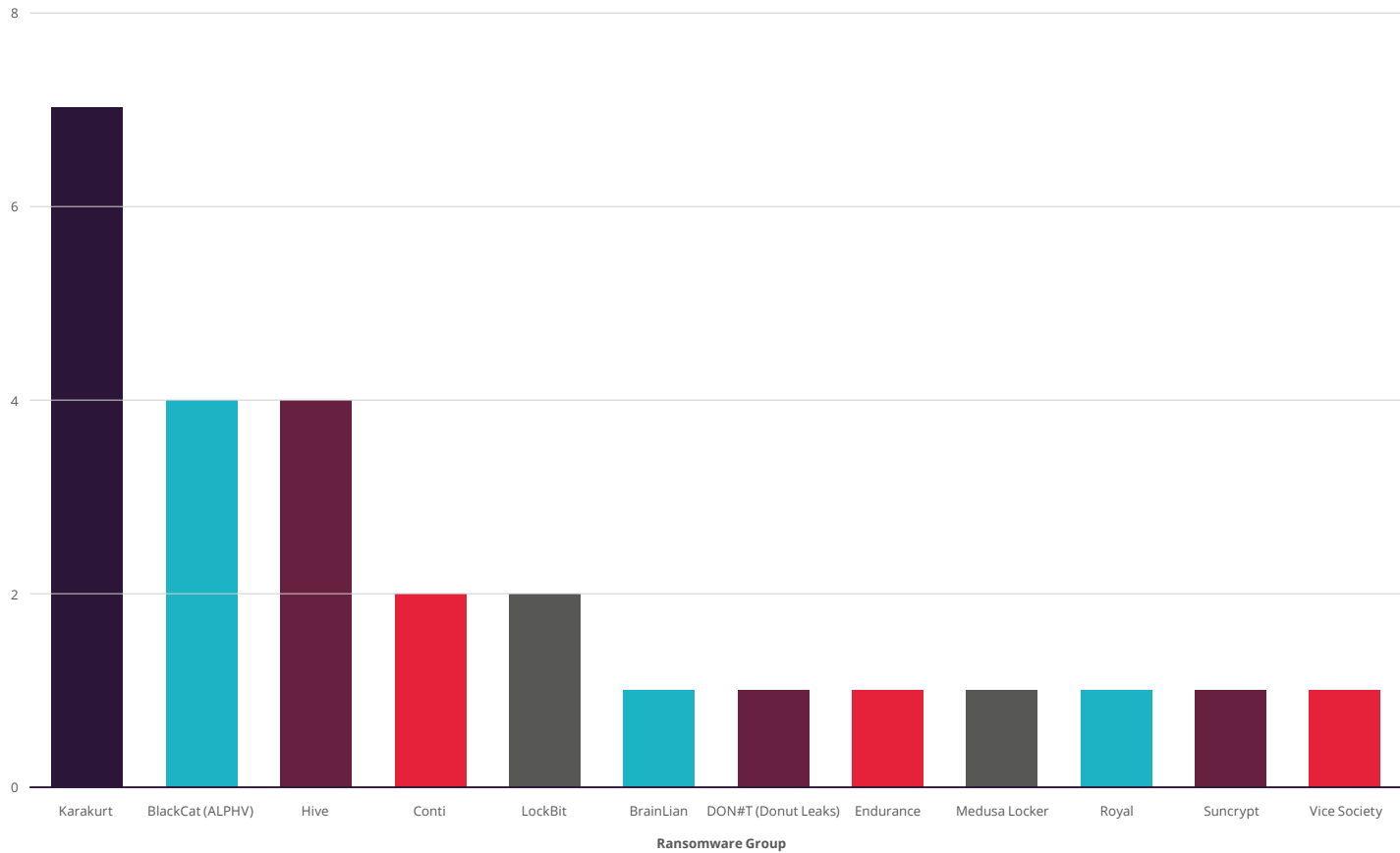
Percentage of UK sectors attacked by LockBit (<5% highlighted)



Sector-by-sector breakdown of the UK organisations targeted by Lockbit in 2022.



“Big game hunting” in the UK in 2022 (targeting large-medium sized organisations)

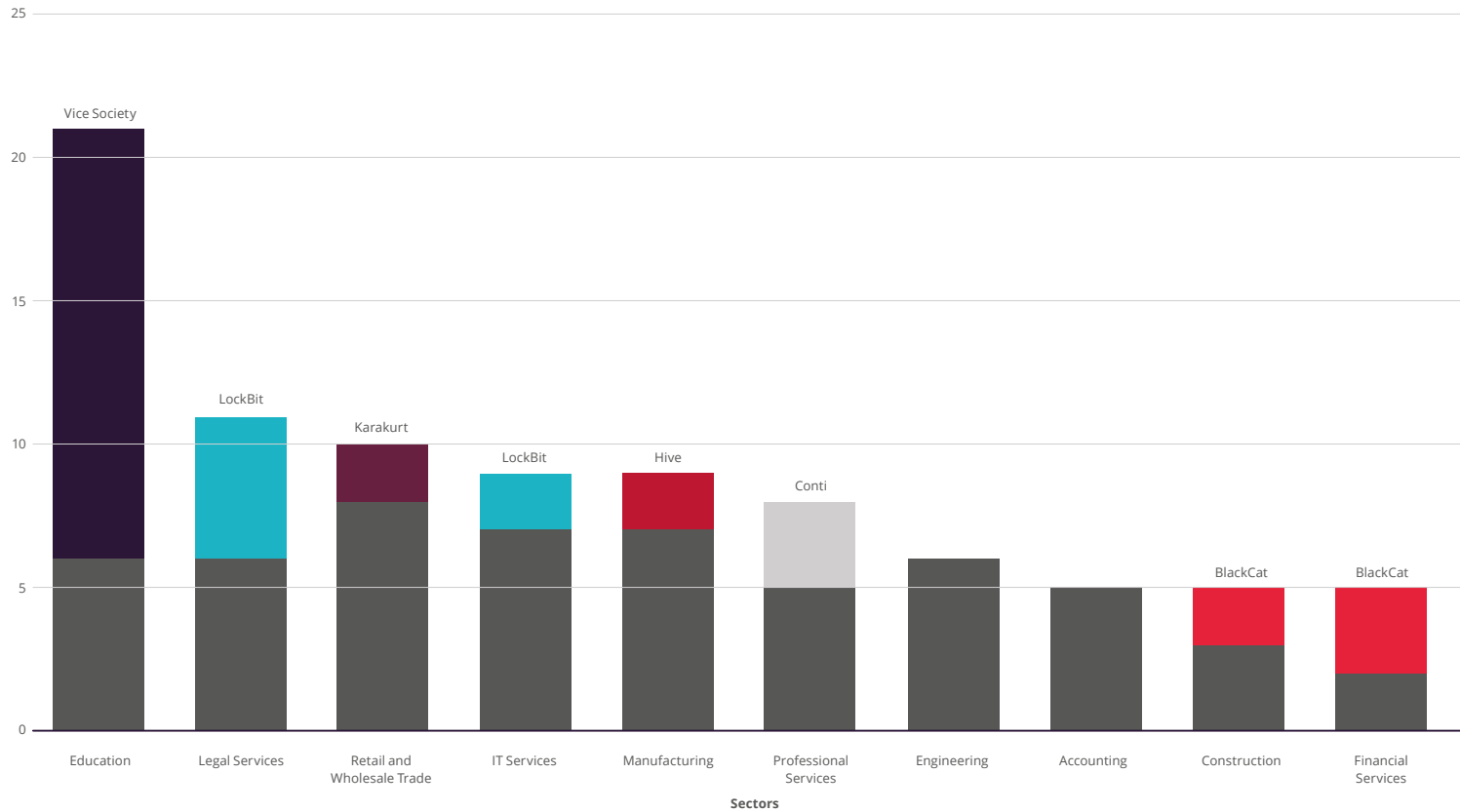


Another group consistently targeting the UK is Vice Society, who overwhelmingly target the UK Education sector. Vice Society is known for an approach that targets less notable high profile and less cyber mature victims by ‘flying under the radar’ to avoid unwanted attention.

In 2022, Karakurt were responsible for the most reported attacks against large and medium UK organisations (by cash in the bank assets). Another indication that Karakurt are linked with Conti (by total reports since 2019, the now disintegrated Conti have reported the most ‘big game hunting’ attacks).



Most prevalent attacker of the most targeted UK sectors



The number of reported attacks by the most prevalent attacker in each of 2022's most targeted UK sectors (not including many attackers (as over 32 known groups reported attacks on UK organisations in 2022)).










Vice Society are not known for their innovation and have been billed as targeting less secure or developed targets.¹⁴ While some have speculated that targeting education is less profitable for attackers than other industries, the fact that groups like Vice Society have now consistently targeted UK schools and universities since 2021 (unlike other sectors that were targeted but are not longer i.e. construction), their attacks are likely yielding a degree of profit.



Other notable threats include:

-  **BlackCat** have begun to target UK organisations in 2022 - all with a turnover of over £10 million. The group were linked to a electricity networks and natural gas pipeline attack in Luxembourg in 2022 and there is evidence that BlackCat are connected to BlackMatter / DarkSide ransomware groups, known for the Colonial Pipeline attack in 2021.
-  **Hive** - Targeted 8 UK organisations 2022 all in the second half of the year, predominantly high value or high-profile large / medium organisations. The group was recently disrupted by the FBI in January 2023, limiting a reported \$130m in ransom demands, however the group continue to operate.¹⁵
-  **BianLian** have emerged as a threat in the UK in Q3 and Q4 and have been active since August.
-  **LV and AvosLocker** - Both show intermittent periods of high activity / inactivity and, while they have been an active globally in 2022, both show disproportionate lack of activity in the UK.
-  **Play Ransomware** have emerged as a new threat in November 2022 and are potentially one to watch for the coming year. The group have attacked major IT provider Rackspace, and a number of government departments in 2022 (but have only begun to attack UK organisations in 2023, (both automotive and manufacturing organisations). This group appears to be pursuing same risk profile / high risk targets similar to the strategy of Conti and REvil in the past.

Threat actors may operate using multiple ransomware strains, and groups can disappear, re-brand and re-emerge often without consequence – making it unwise to put too much weight on the changing fortunes of any individual group. However, understanding the TTPs of ransomware groups and their proclivity to target a particular sector or size of business can help organisations identify potential vulnerabilities and develop effective strategies to mitigate the risk.





UK Sector-by-Sector Analysis

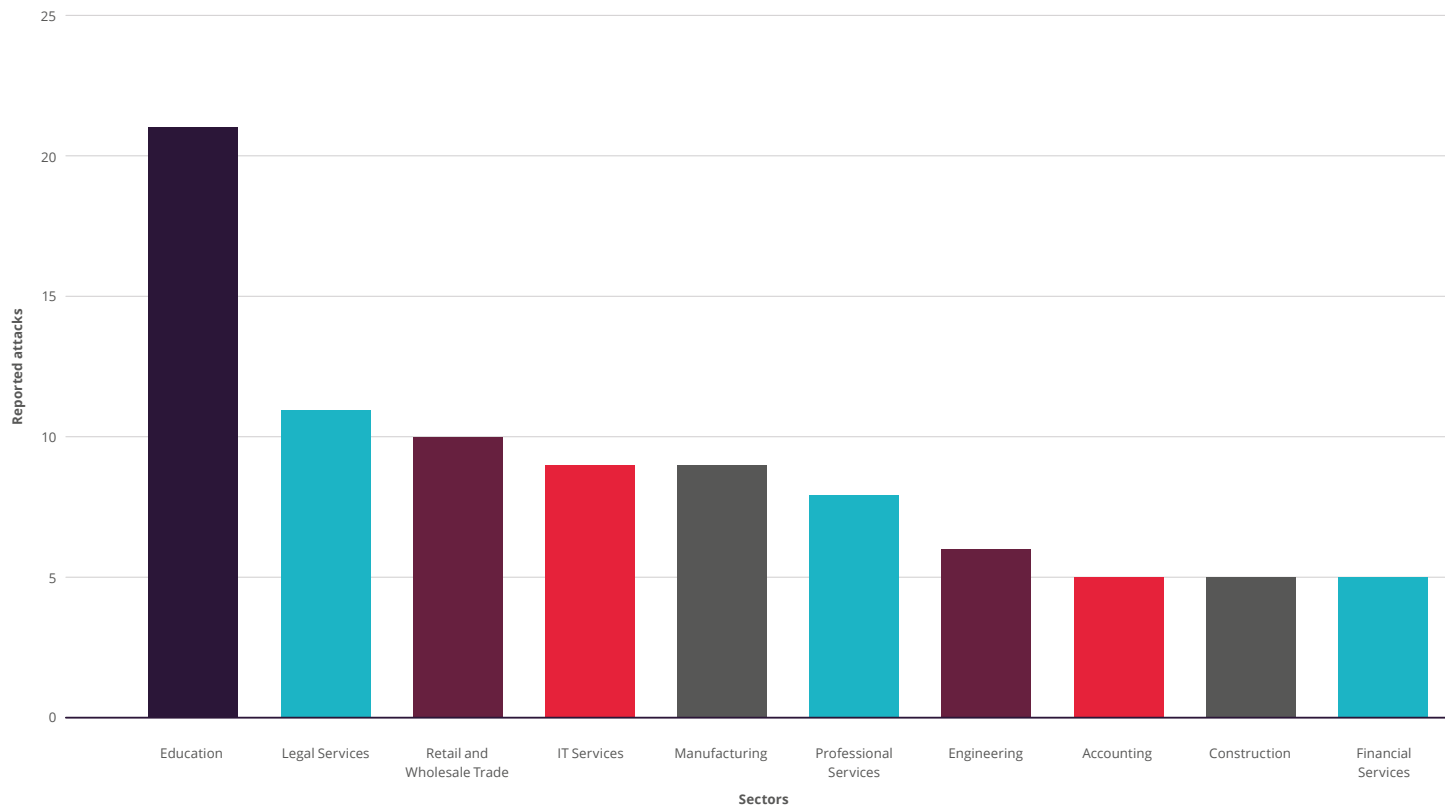
As outlined previous, we know that certain groups do tend to target particular industries (i.e. Vice Society – education). However, most attackers have a far less established target sector and, as outlined in JUMPSEC’s trends report last year, it is difficult to infer whether ransomware groups are influenced by perceived lower levels of cyber maturity, or the promise of a more lucrative potential payoff from cash rich organisations.

Whether attackers have a defined sector-based strategy or not, the data does indicate the degree to which even random ransomware hackers have targeted particular sectors in 2022.

The data suggests that Education, Law, and Retail and Wholesale Trade were the most targeted industries (as they have been considering all attacks since 2019), but we must examine the financial size and capacity of victimised organisation to gain a more realistic insight on the true sector-by-sector impact of ransomware in the UK.



Most targeted UK sectors 2022



The most targeted UK sectors in 2022.

In comparison to 2021 we broadly see similar figures for most UK sectors, with the notable exception of construction, which was targeted far less in 2022 despite being the most targeted sector of 2021.

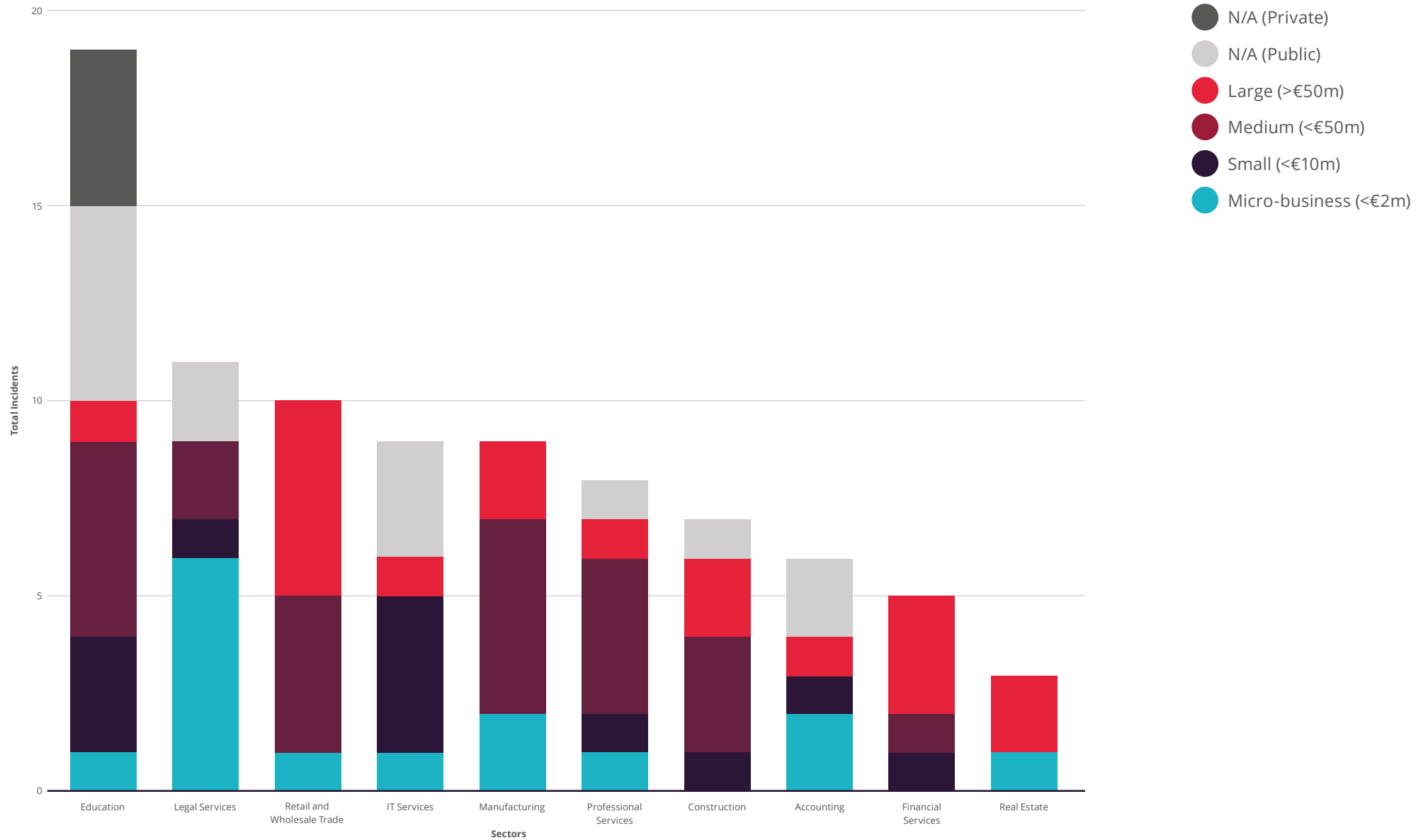
Two primary possibilities contributed to this change. Either the construction industry had a dramatic culture shift and invested heavily in cyber security over 2021 or, targeting construction is simply not that profitable for attackers, and as some have theorised, the fact that the industry is far less reliant on digital infrastructure than other sectors has made construction organisations more difficult to extort.

In this context, the continued attack rates seen the education industry are perhaps an indication that attackers are finding a degree of success by attacking this sector.

As with last year's ransomware trends report, medium and large organisation in Retail and Wholesale trade and Financial Services have been strongly impacted. Smaller businesses were targeted in Law and Accounting.

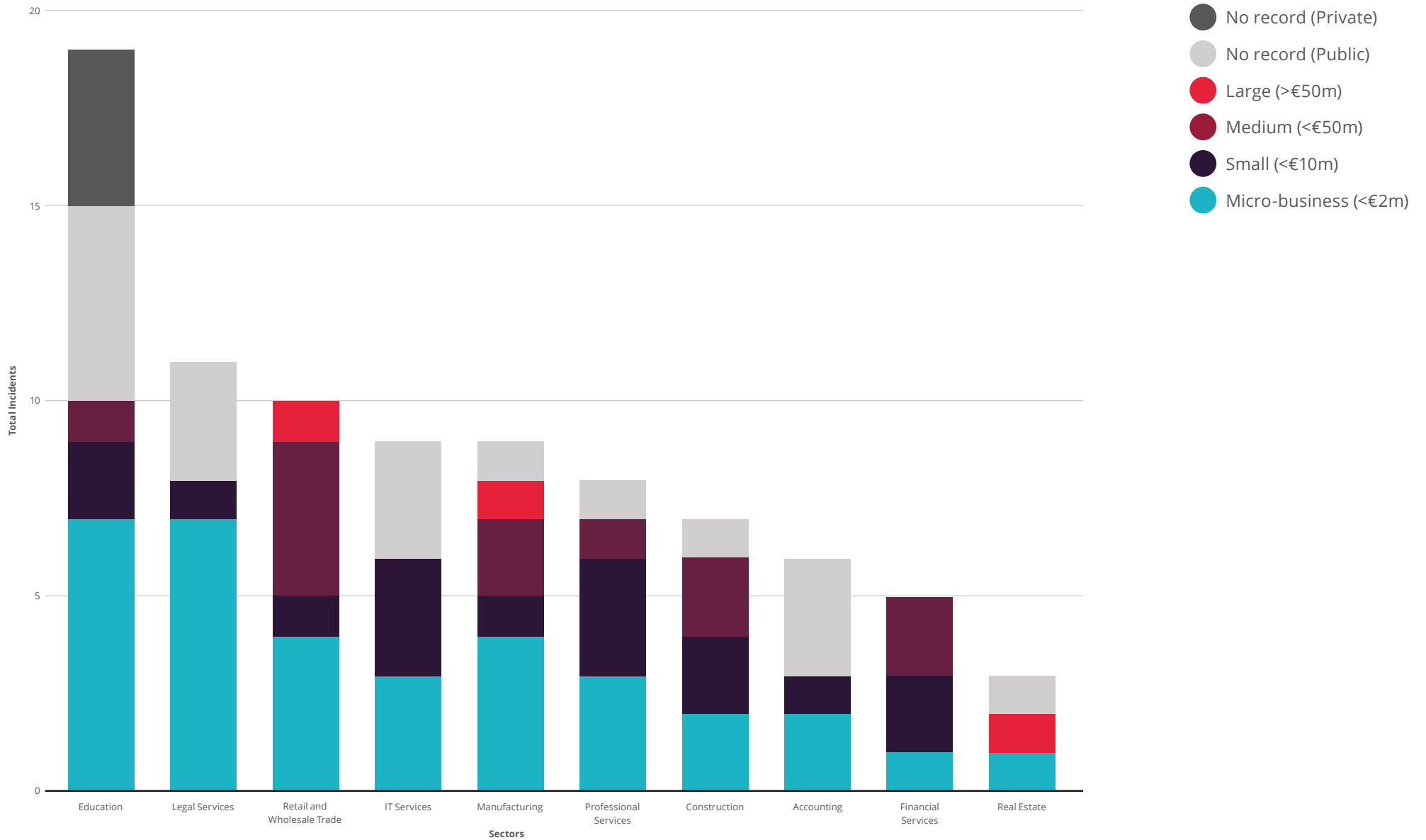


The UK's most targeted sectors, broken down by size (total assets)









The UK's most targeted sectors, broken down by size (cash in the bank assets)





Some key points to consider from the graphs previous include:

-  The most lucrative industry to target hypothetically is **Retail and Wholesale Trade**, owing to its high number of large sized victims (>€50m). This omits Education which has a higher proportion of unavailable public financial data than other sectors.
-  **Financial Services** is potentially a highly lucrative industry to target despite a relatively low attack rate, with a combined total of over £63m cash in the bank assets (second only to Retail and Wholesale Trade despite far less attacks), due to the high proportion of large-sized victims within the sector.
-  **Manufacturing** also presents a highly lucrative UK sector to target, accounting for the third high cash in the bank assets and total assets.
-  There appears to be a high proportion of micro-businesses attacked particularly in the **Legal** and **Accounting** sectors.





Industry Sector	Cash in Bank	Total Assets
Retail and Wholesale Trade	£316,686,040	£2,132,356,370
Financial Services	£63,040,000	£307,700,000
Manufacturing	£52,596,000	£275,047,750
Real Estate*	£46,693,130	£257,310,000
Construction	£39,428,000	£191,910,000
Professional Services	£28,353,820	£145,070,000
Education	£17,361,980	£224,658,000
IT Services	£10,952,910	£224,935,000
Accounting	£5,126,260	£15,990,100
Healthcare	£4,930,000	£17,060,000
Legal Services	£3,280,680	£36,669,390

*One organisation with over £2 billion total assets and £47 million cash in the back assets was attacked in the Real Estate sector in 2022. Otherwise, the sector was not highly impacted (a total of 4 attacks in 2022).



What can we expect in 2023?

As we look to 2023, JUMPSEC's initial attacker reported data show signs of an uptake in reported attacks against UK organisations. However, these figures will naturally fluctuate throughout the year. A number of recent developments may continue to influence ransomware trends:

- **Vulnerability exploitation** will continue to be a key part of the ransomware delivery process and precipitate periods of increased activity. There are early indicators that vulnerabilities affecting VMware ESXi servers are being actively exploited by dedicated ransomware groups seeking to leverage a low-complexity exploit against a prevalent technology, which may be one to watch.
- **Tighter insurance terms** may restrict threat actors' ability to extort organisations, as insurers move to limit their exposure and offer less financial support to victims for ransom payments (detailed by JUMPSEC here). There is evidence that attackers may already be feeling the effects in 2023, as Hardbit ransomware have begun to explicitly request insurance details from victims so that the ransom demand can be adjusted to fall within the victim organisation's policy.¹⁶
- **Further ransomware payment regulations and restrictions** are likely to be enforced in 2023 as the UK have stressed that making a ransomware payment may be in breach of financial sanctions, and therefore must be reported to authorities. The EU and U.S. and Australia have also introduced additional measures to penalise ransomware payments.
- **Grey-zone military tactics** have become a feature of international relations irrespective of individual conflicts, making cyber attacks an attractive means to cause immense disruption without crossing the threshold of overt war. A recent report by Google's Threat Analysis Group (TAG) has suggested increased interconnectivity between ransomware actors and the Russian state, with "tactics closely associated with financially motivated threat actors being deployed in campaigns with targets typically associated with government-backed attackers".¹⁷



- ¹ <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>
- ² <https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/>
<https://www.orange cyberdefense.com/global/security-navigator>
<https://delinea.com/news/2022-state-of-ransomware-report>
- ³ <https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf>
- ⁴ <https://www.hackread.com/pro-russian-killnet-uk-ddos-attacks/>
- ⁵ <https://www.gov.uk/government/news/uk-to-provide-1000-more-surface-to-air-missiles-to-ukraine>
- ⁶ <https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper>
- ⁷ <https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/>
- ⁸ <https://delinea.com/news/2022-state-of-ransomware-report>
- ⁹ <https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022/cyber-security-sectoral-analysis>
- ¹⁰ <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>
- ¹¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135587/Ransomware___Sanctions_guidance__Feb_2023_.pdf
- ¹² <https://www.infosecurity-magazine.com/news/australia-considers-ban-ransomware/>
- ¹³ <https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf>
- ¹⁴ <https://www.wired.com/story/vice-society-ransomware-gang/>
- ¹⁵ <https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/>
- ¹⁶ <https://www.neowin.net/news/hardbit-ransomware-asks-victims-to-provide-insurance-details-to-identify-ransom-demand/>
- ¹⁷ <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>



JUMPSEC

Unit 3E – 3F,
33 – 34 Westpoint,
Warple Way,
Acton W3 0RG

T: 0333 939 8080

E: hello@jumpsec.com

www.jumpsec.com

