QBE Insurance

Cyber threats to the Legal and Professional Services sector

Executive summary

- Including both cyber trends and recommended mitigation steps, this article delves into the risks, challenges and ways to protect your legal or professional services business.
- Ransomware groups frequently target Legal and Professional Services (LPS) organizations, making the sector one of the most impacted globally. These firms are particularly appealing to cyber criminals because they hold sensitive data on numerous clients and are perceived as highly likely to pay significant ransoms.
- The LPS sector has been particularly affected by zero-day vulnerabilities (e.g. MOVEit), and it is highly likely that this attack-type will continue to impact organisations in 2025.
- Criminal actors are also adapting their tools and techniques to counter advances in technical defensive tools like Endpoint Detection and Response (EDR).
- Nation State Actors are increasingly collaborating with criminal actors, adopting the same tools and techniques, and blurring the lines between state sanctioned and financially motivated activity.
- Given the complex supply chains of LPS firms, there is a significant risk of third-party compromises, which could lead to data breaches or potentially cause sector-wide disruption.
- Cloud adoption, increasingly complex supply chains, and cyber criminals' focus on third party technology supply chains is creating new threats for firms.
- Artificial intelligence (AI) has enhanced attack and social engineering tactics, allowing groups to scale their activities and increase the chances of successful compromise.
- Business email compromise, driven heavily using AI, remains a significant threat to most organisations.

Introduction

This paper explores cyber threats to the Legal and Professional Services (LPS) sector, examining the latest developments in the threat landscape and their implications for this industry. This analysis follows our initial report, "Cyber Threats to the Financial Services Industry," which can be accessed here.

Ransomware and extortion

Unsurprisingly, the frequency of ransomware attacks remains high, with numbers of victims being posted onto dark web leak sites being higher in 2024 than 2023.

However, a recent analysis suggests that the total amount paid out to criminals decreased in 2024, from USD $1.25 billion in 2023 to USD $813 million in 2024. This suggests that some organisations may be less willing to pay ransoms and/or that law enforcement is having an impact on the ransomware landscape.[1]

In 2024, other key trends included:

- **Ransomware actors focusing on vital supply chain targets.** Ransomware incidents like Change Healthcare in 2024 by the Blackcat crew[2] and Synnovis by Qilin[3] demonstrated the second order impact that can be caused by attacks on key service providers. In these cases, the impact on the broader healthcare sector was significant. The interdependencies that exist between organisations is not lost on these threat actors, and the Professional Services sector faces a similar threat due to the network connections they have with their customers. For UK law firms, this type of supply chain attack manifested in the 2023 ransomware attack against CTS, an MSP for the broader UK legal sector[4].
- **Increased security capabilities have forced threat actors to develop their toolsets.** The adoption of advanced cyber security technology, such as EDR solutions, has made it more difficult for threat actors to compromise systems and perform post-intrusion activities. In the ransomware space, many threat actors have been forced to adapt and in 2024, there has been a notable increase in the adoption of malicious tools that tamper with security tools. Specifically, groups have adopted tools known as "EDR", allowing the actor to run their malware with a reduced chance of being detected or blocked. Examples of tools observed in 2024 are EDRSilencer[5], AvNeutralizer[6], and EDRKillerShifter.[7]
- **Blurring of lines between criminal and nation state actors.** Microsoft and others have noted overlaps between nation state and cybercriminal actors in their intent, tools, and techniques. Most concerningly, this crossover has been in the use of ransomware by nation state actors who initially perform traditional nation state activities such as intelligence gathering but subsequently deploy ransomware to monetise their access.

North Korean actors have embodied this blurring of lines for years, with reporting in May 2024 on the North Korean actors using the FakePenny ransomware on firms after exfiltrating sensitive data from target firms. This year, intelligence agencies also warned of Iranian actors collaborating with prominent ransomware operators during their attacks, encrypting systems of organisations they had targeted for espionage purposes.[8]

Firms in the LPS sector should map security controls to the TTPs of certain nation state actors as well as criminal groups.

- **Some groups have specialised in social engineering and impersonation for initial access.** Scattered Spider (aka Octo Tempest) has received increased attention in 2024. They have adopted relatively novel methods of acquiring credentials and breaching accounts. They have, for example, impersonated employees and IT helpdesk staff with the intention of resetting credentials and/or MFA, sometimes supplemented by SIM swapping. They have also registered domains that imitate the organisation they are targeting to harvest credentials. After initial access, they have shown a high degree of capability to move around cloud environments, disable security tooling, exfiltrate data, and launch ransomware, likely partnering with prominent RaaS operations.[9,10]

Extortion and Professional Services

In 2024, the LPS sector was ranked sixth in publicly reported ransomware and data theft and leak attacks. It followed the technology, manufacturing, construction, healthcare, and consumer services sectors, with approximately 400 organizations publicly named by ransomware groups.[11]

This includes the targeting of LPS organisations by prominent ransomware operations, including **Black Basta, RansomHub,** and **BianLian.**

- According to a report in mid-2024, LPS was the most affected sector by Black Basta affiliates since their inception.[12]
- For RansomHub, who ended 2024 as the most active RaaS, LPS was in the top 5 affected sectors.[13]
- According to a 2024 joint advisory on the BianLian extortion group, the group has shifted to conducting data theft only. They have primarily targeted US organisations with a focus on LPS, as well as manufacturing, healthcare, financial services, construction and engineering sectors. The advisory also mentions the targeting of an Australian Professional Services organisation.[14]

Threat actor snapshot

RansomHub

Overview: RansomHub emerged in early 2024 and has quickly risen to being one of the most active RaaS operations currently. Affiliates are typically offered 90% of extortion profits and have reportedly included Scattered Spider as one prominent group that has leveraged the ransomware.[16]

Targets: Professional services is one of the topmost targeted sectors by affiliates of RansomHub, along with manufacturing, retail, technology, and healthcare.[17] US organisations comprise around half the victims on their leak site, with Europe not far behind.[18]

Initial access techniques: RansomHub intrusions have started with a series of tactics ranging from valid credentials to access VPN systems, malware (known as FAKEUPDATE) infections, social engineering of helpdesk staff to obtain credentials, to vulnerability exploitation.

Actions on objectives: RansomHub have used compression tools, remote access software, and widely used tools like Rclone, MEGAsync, WinSCP, and WinRAR to perform data theft. To deploy the ransomware, they have used manual execution, self-propagation techniques and scripting. In some intrusions, affiliates have disabled various security tooling to ensure the ransomware runs.

Intent analysis: Why are extortionist actors targeting LPS?

Key factors that contribute to the targeting of the LPS sector are likely:

- The central role LPS organisations play in organisations' business operations
- The high number of customers they may have,
- The sensitivity of the information they store on their customers.
- The potential for the actors to subsequently target their customers using the access they have in the LPS organisation.

For these reasons, there is likely to be a perception from cybercriminals that LPS firms are more likely to pay a ransom demand to protect customer data and avoid downtime caused by the encryption of their systems and subsequent business disruption for their customers.

The targeting of larger, high revenue LPS organisations is considered **big game hunting**, something that affiliates of Black Basta, RansomHub, and others are known to do. In CrowdStrike's 2024 Threat Hunting Report, they observed a 141% increase in 'targeted intrusions' year-on-year, along with a 152% increase in access broker advertisements for Consulting and Professional Services entities.[19] This suggests a marked increase in the level of intent from threat actors that adopt a more targeted approach to their attacks.

Overinflation

Conversely, it is common for some threat actors to overinflate the severity of their attacks. This has been observed frequently within the LPS sector. While an actor may claim to have breached a major consultancy, they may have only compromised a third-party platform, hosting relatively innocuous data. Due to LPS organisations often leveraging a large number of third-party providers themselves, the likelihood of this is high. In December 2024, a ransomware group called Brain Cipher claimed to have compromised Deloitte, stating on their leak site that they have taken one terabyte of data on a number of customers. Deloitte later responded to the claims, saying it was limited to one client and the impacted systems fell outside their network.[20] Another example is Lockbit who, in a bid to remain relevant after law enforcement action against them, published a lot of recycled data (from old breaches) or fabricated claims on its leak site.[21]

While it is important to address the threats to third parties, claims made by threat actors must be treated with caution while they are thoroughly investigated. This is also potentially why we have seen the total number of ransom payouts drop, as some organisations increasingly doubt the sensitivity or value of data being leaked.

Snapshot use cases:

Threats to the Legal and Professional Services sector

In addition to consistent ransomware attacks on LPS firms, there were other incidents and campaigns in 2023 and 2024 that reflect a wider threat to the sector:

Zero-day exploitation: In 2023, several LPS firms were affected by the widespread exploitation of the MOVEit file transfer application. This included Ernst & Young, Deloitte, PWC, Crowe LLP, WTW, Aon, Sovos, and Kirkland & Ellis.[22] The exploitation of zero-days and newly published vulnerabilities (n-days) remains a highly effective method of gaining initial access to organisations. The UK's NCSC and its allies released data on the vulnerabilities that were actively exploited last year, showing that many of them were exploited as zero-days, meaning that there were no patches available and little organisations could do to mitigate against it. The trend has been observed as we have progressed through 2024 and differs considerably from 2022 where half of vulnerabilities were exploited as zero-days.[23]

Third party compromise leading to sector-wide disruption. The ransomware attack on CTS in November 2023 affected several UK-based law firms. CTS is a managed service provider (MSP) for the sector and was reportedly compromised via high impact vulnerability known as Citrix Bleed, which was being weaponised by several threat actors including ransomware actors. The attack meant that a significant number of law firms could not access critical case files and client data.[24] This incident, along with incidents like CrowdStrike, demonstrate the risks to key service providers where they act as single points of failure in sectors or geographies. More discerning threat actors can identify these single points of failure and given the opportunity (like access to a zero-day), will look to target them to cause as much disruption as possible.

Nation state espionage: On March 2024, the US DOJ released an indictment against several hackers that were performing cyberattacks against multiple sectors and geographies on behalf of the Chinese Ministry of State Security (MSS) as part of a threat group known as APT31. The espionage campaign involved the targeting of suppliers and managed service providers that had links to their primary targets. Targets included multiple (unnamed) global law firms based in the United States as well as a provider of software for the legal sector.[25]

Data exposure: The business services giant CBIZ Benefits & Insurance Services (CBIZ) disclosed that in June 2024, an actor had exploited a vulnerability in one of its websites enabling them to steal personal information relating to 36,000 individuals.[26]

In September 2024, a hacker posted on a dark web forum that they had stolen 20 GB of data from Capgemini, a major French consultancy firm. They claimed to have stolen source code, credentials, and virtual machine logs relating to one client T-Mobile (who later said their machines weren't caught up in the breach).[27]

Initial access malware: Gootloader, which is a long-standing and prominent malware has typically used compromised websites and lure documents that typically revolve around legal agreements, documents, and similar.[28] In previous years, law firms had been directly targeted by Gootloader.[29] The Gootloader malware is particularly dangerous as it often serves as an initial malware foothold which is passed onto ransomware actors such as INC or Blacksuit.[30]

Global threat spotlight: cloud exploitation and cross-domain attacks

Threat actors are increasingly becoming "cloud", meaning they are developing more effective techniques to compromise cloud environments and leverage them to achieve their objectives. This involves the abuse of the interaction between 'on-premise' and cloud accounts and systems. Given the centrality of cloud systems in almost all corporate environments, threat actors are developing capabilities to gain access to often overly permissive cloud service accounts, perform reconnaissance, maintain persistence, identify sensitive cloud systems and data storage repositories, exfiltrate this data, and potentially deploy ransomware conventionally, or using cloud encryption techniques.

Cloud encryption has emerged as a notable threat, where threat actors are developing techniques to encrypt and delete critical data stored in cloud hosting services like AWS, Google Cloud, or Azure. For example, researchers have observed threat actors abusing native AWS features like AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data in an S3 bucket and extort the organisation. All the attackers need to perform these attacks are valid AWS account credentials. In this case, the attackers give the compromised organisation 7 days to pay a ransom or the files are deleted.[31]

Reports on cloud targeting by groups like Scattered Spider[32] and Storm-0501[33] for example, reflect a growing shift in how some threat actors are carrying out targeted intrusions. The attack chain below provides a high-level view of some of techniques being used to perform attacks in the cloud.

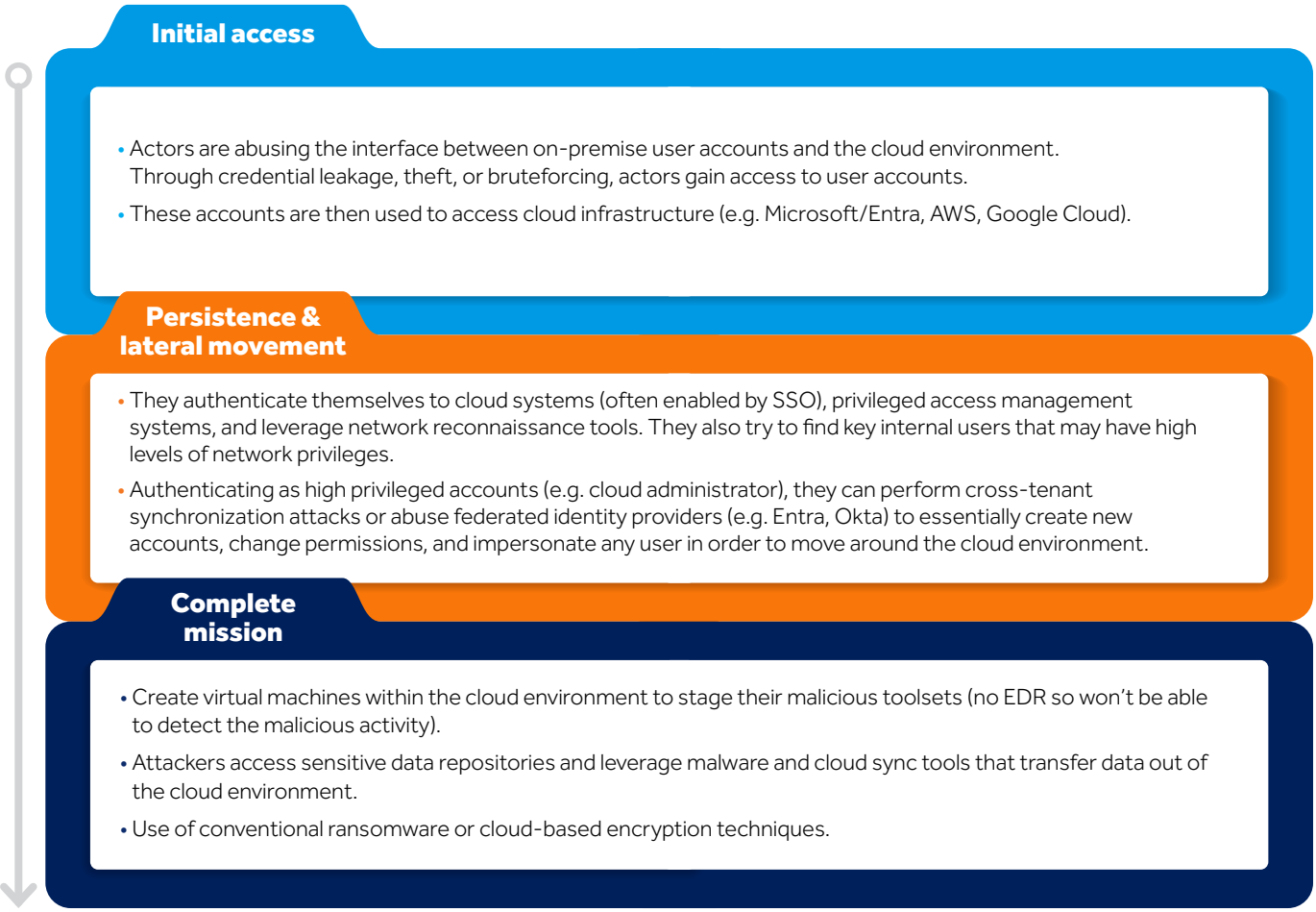

Figure 1: High-level attack flow of how cloud attacks are materialising

Global threat spotlight: artificial intelligence (AI)

AI is an area that requires close attention in how it is developing and being leveraged by threat actors. Primarily, it is being used by actors to enhance their social engineering efforts, specifically by generating text and imagery in phishing emails for example, but also to aid in the reconnaissance on their target, such as harvesting their branding, logo, customers, business areas, etc., leading to higher chances of a user being successfully compromised.

While all threat actors can benefit from the capabilities of AI, the greatest uplift applies to lower capability and opportunistic threat actors, as it allows them to generate more accurate (fewer grammatical and spelling mistakes) content faster and easier. It can also allow them to identify potential vulnerabilities or weaknesses in a target's network, which they can exploit. For more advanced actors, AI is used more to optimize their tools and techniques, for example in writing malware code or scripts used in their attacks.[34]

In November 2024, Google announced that their AI agent identified a previously unknown exploitable vulnerability in SQLite, which is an open-source database engine. Google believe this is the first known example of an AI tool to do so.[35]

Business email compromise (BEC)

BEC has continued to plague businesses in 2024, being one of the costliest forms of cybercriminal activity. AI has almost certainly been a key factor driving BEC scams, given its ability to craft more convincing emails and at scale. According to one email security provider, 40% of all BEC emails observed in Q2 2024 appeared to be AI-generated.[36]

Given the nature of the close engagement LPS organisations have with their clients, the threat from BEC is more acute. BEC actors have ample opportunity to leverage compromised email accounts of, or impersonate, employees at LPS firms to defraud the company or its customers. Attorney impersonation scams are also prevalent in the BEC space, where attackers are deceiving targets to make financial transactions pertaining to legal fees, payment transactions and other confidential business dealings. In 2022, a prominent BEC gang known as Crimson Kingsnake was registering impersonation domain names of major law firms and targeting customers with urgent requests to pay bills claiming to be from the 'Debt Collection Litigation Counsel' for example.[37] AI will only serve to improve the effectiveness and volumes of this type of BEC scam.

Deepfake

Perhaps most concerning, is how advancements in AI are driving the use of deepfake imagery, video, and audio. From socially engineering employees into sending huge sums of money to attacker accounts[38], to impersonating loved ones, it is a growing concern for businesses and individuals. Due to the abundance of material that can be used to train deepfake AI models, such as images and videos on sites like LinkedIn and YouTube of CEOs making public appearances, it has become increasingly simple to craft deepfake attacks.

Notable too, has been the use of AI and deepfake technology to enable North Korean operatives to conduct their brazen campaign of seeking employment at US firms using stolen identities. In July 2024, cyber security firm KnowBe4 provided a first-hand account of how they employed someone impersonating a US citizen using AI and deepfake during the interview process. As soon as they started work at the company, they attempted to install malware on their corporate laptop, which was immediately detected and shut down.[39]

Guidance for organisations

Below are high-level recommendations for organisations to consider when taking steps to mitigate threats. It is not an exhaustive list, and the suitability and applicability of the recommendations will differ depending on the organisational context.

Ransomware

- Create, maintain, and update offline, encrypted back-ups of critical data. Ensure these are as close to "golden images" of pre-configured builds of networks, user devices, and applications.
- Use separate authentication processes for accessing theses critical back-up and data recovery systems.
- Perform regular exercises to test recovery processes and systems.
- Ensure you have incident response playbooks and plans with a focus on technical response and recovery as well as documentation detailing escalation procedures and communications.
- Focus first on initial access vectors such as phishing, credentials, and external facing assets (see vulnerabilities section).
- Ensure you perform regular phishing exercises; implement email filtering or a gateway to reduce the number of phishing emails reaching users or implement DMARC and SPF.
- For credentials, ensure phishing-resistant MFA is enabled for all accounts; leverage conditional access/attribute-based validation (e.g. geo-verification); monitor for leaked credentials; roll-out a common password policy; consider password management solutions; leverage privilege access management; rotate credentials; and disable obsolete internal and external third-party accounts.
- After initial access, assess controls for detecting and preventing post-compromise activities such as privilege escalation, lateral movement, data exfiltration and encryption.
- Monitor for illegitimate use of remote monitoring and management (RMM) tools in your network as they are heavily leveraged by threat actors in multiple kinds of attacks including ransomware.

Vulnerabilities

- Create and follow a patch management process so that high severity vulnerabilities are remediated quickly.
- This should be underpinned by a vulnerability prioritisation process that considers several factors such as whether the system is internet facing, the nature of the vulnerability (e.g. privilege escalation, or remote code execution), whether it is being exploited in the wild, etc.
- Disable unnecessary devices, ports and services for internet facing systems.
- Leverage tools and processes to perform asset discovery and attack surface management to understand your own network and where weaknesses may lie.
- Document secure baselines for configurations of IT, OT, and Cloud systems; monitor for any changes to these baselines and respond accordingly.
- Monitor threat intelligence sources for indications of zero-day exploitation.

Cloud

- Establish consistency in user, administrative, and service account access within cloud environments dependent on roles and responsibilities.
- Strict limitation of access to critical identity management, networking, and storage systems within cloud environments.
- Segregation of critical and non-critical resources within cloud environments. For example, segregating AD domain controllers from the user account plane, internet facing applications, or development environments.
- Credential separation between user accounts and cloud resources, will reduce the opportunity for an attacker to compromise a user's account and move laterally to cloud systems.
- Review cloud logging strategy and ensuring that suspicious activity, such as suspicious logins or data exfiltration, in the cloud is being appropriately monitored.
- Cloud Security Posture Management (CSPM) tools can help to configure secure cloud environments and aid in the prevention and detection of threats.
- Mandiant offers a comprehensive guide to Standardizing Privileged Access for Multi-Cloud environments.

Supply chain

- Rate the criticality of each supplier with respect to the data they hold and the extent they underpin critical business services, i.e. assess what the likely organisational impact would be of a cyberattack against the supplier.
- Map minimum security requirements the supplier should have based on this impact ranking.
- Communicate these requirements to suppliers and ensure compliance from them.
- Embed this assessment process in all future supplier interactions.
- Tabletop exercises can help to educate the organisation on supply chain risks, provide a mature approach to supplier management, and ensure compliance.
- Less mature suppliers can be supported by experienced security teams to help bolster their cyber security programs.

AI, BEC and deepfake

- Educate users on the threat from AI-generated content including imagery, video, and audio.
- Urge users to treat suspicious payment request or detail changes with a high degree of caution, even when the requests are from trusted internal employees or third parties.
- Create and enforce strict processes for verifying and approving payments, running interviews, and other business functions. Successful AI/deepfake scams often stem from weak processes or processes not being followed properly.
- Educate users of the telltale signs of deepfake content especially those involved in payment processing, as well as performing interviews and other external communications.
  - Strange movement of the face especially not lining up with what they are saying
  - Strange bodily movement.
  - Slow responses to questions
  - Slurred speech
  - Unnatural speech in terms of sentiment and emotion
  - Background noise
- Alternatives to audio-based authentication technology should be considered given attackers' ability to generate deepfake audio from public content.
- Try to limit the amount of personal publicly available content on the internet that can be used to train AI-models and craft deepfake content.
- Implement robust controls around AI and machine learning DevOps when building applications.

[1] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/
[2] https://crsreports.congress.gov/product/pdf/IN/IN12330
[3] https://www.intercede.com/ransomware-assault-on-nhs-a-deep-dive-into-the-synnovis-data-breach/
[4] https://therecord.media/uk-cyberattack-msp-cts-law-firms
[5] www.trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html
[6] https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/
[7] https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/
[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
[9] https://blog.sekoia.io/scattered-spider-laying-new-eggs/#h-eggspedition-scattered-spider-s-exfiltration-tactics
[10] https://www.reliaquest.com/blog/scattered-spider-x-ransomhub-a-new-partnership/
[11] This ranking was determined from Ransomware.live, which actively scrapes known data leak sites and presents the data on the site. The data is unlikely to be completely accurate as incorrect sector classification and other factors may skew the figures. Important note: the data is also not reflective of the number of actual ransomware attacks, as those companies that paid a ransom will not have appeared on the leak site.
[12] https://blog.barracuda.com/2024/05/18/black-basta-nasty-tactics
[13] https://www.zerofox.com/intelligence-feed/ransomhub-extortion-attacks-on-sharp-upward-trajectory/
[14] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
[15] https://www.reliaquest.com/blog/scattered-spider-x-ransomhub-a-new-partnership/
[16] https://www.group-ib.com/blog/ransomhub-never-sleeps-episode-1/
[17] https://www.zerofox.com/intelligence-feed/ransomhub-extortion-attacks-on-sharp-upward-trajectory/
[18] www.trendmicro.com/vinfo/gb/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub
[19] https://crowdstrike.com/explore/crowdstrike-2024-threat-hunting-report/crowdstrike-2024-threat-hunting-report
[20] https://www.securityweek.com/deloitte-responds-after-ransomware-groups-claims-data-theft/
[21] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/
[22] www.trustwave.com/hubfs/Web/Library/Documents_pdf/2024_Trustwave_Professional_Services_Sector_Threat_Landscape.pdf
[23] https://www.ncsc.gov.uk/news/uk-allies-warn-shift-in-cyber-attackers-exploiting-zero-day-vulnerabilities
[24] https://www.totalityservices.co.uk/cts-citrixbleed/
[25] https://harfanglab.io/insidethelab/apt31-indictment-analysis/
[26] www.bleepingcomputer.com/news/security/business-services-giant-cbiz-discloses-customer-data-breach/
[27] https://www.theregister.com/2024/09/12/capgemini_breach_data_dump/
[28] www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Detecting-GOOTLOADER-with-Google-Security/ba-p/823766
[29] https://www.esentire.com/blog/gootloader-identified-at-legal-services-firms-in-drive-by-attacks
[30] www.bleepingcomputer.com/news/microsoft/microsoft-vanilla-tempest-hackers-hit-healthcare-with-inc-ransomware/
[31] https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c
[32] blog.eclecticiq.com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries
[33] www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/
[34] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
[35] googleprojectzero.blogspot.com/2024/10/from-naptime-to-big-sleep.html
[36] https://vipre.com/wp-content/uploads/2024/07/vipre-q2-2024-email-threat-report.pdf
[37] www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf
[38] edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[39] https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

QBE Insurance