V11 ISSUE 03

Ransomware Report 2025

Building Resilience Amid a Volatile Threat Landscape

Akamai

State of the Internet/Security

Contents

02 **Introduction**

04 **Key insights of the report**

05 **Overview of attack patterns and the impact on customers**

06 **Evolving extortion tactics**

13 **Inside the RaaS ecosystem**

23 **Putting the RaaS in hacktivism**

26 **Security spotlight: A malicious treat with TrickBot** (Guest contributor: Or Zuckerman)

27 **Industry trends**

30 **Security spotlight: Cryptominers** (Guest contributor: Maor Dahan)

37 **The impact of ransomware attacks on operational continuity**

39 **Security spotlight: Ransomware and the law** (Guest contributor: James A. Casey)

42 **Building ransomware resilience around the world**

46 **Mitigation**

47 **Conclusion**

48 **Methodology**

49 **Guest contributors**

50 **Credits**

Introduction

The ransomware landscape has grown even more complex and volatile in 2025. Groups like FunkSec and Black Basta have reportedly used generative artificial intelligence (GenAI) and large language models (LLMs) to create ransomware code and enhance their social engineering attacks, respectively. Although adversaries are using multiple extortion techniques — sometimes even quadruple extortion — double extortion remains the attackers' favored method. Despite high-profile law enforcement takedowns, threat actors show strong resilience — regrouping, rebranding, or forming new groups to quickly fill any vacuum created by the dissolution of a dominant group.

How attackers are harnessing AI and LLMs

Adversaries are rapidly integrating AI and LLMs to increase the scale, sophistication, and efficiency of their operations. Ransomware groups such as FunkSec use GenAI to generate malicious code, create new ransomware variants, and deploy chatbots to negotiate with victims. Attackers also employ AI to craft convincing phishing emails and conduct voice phishing ("vishing") attacks that impersonate company personnel. Advanced persistent threat groups have also begun using GenAI on a limited scale. Forest Blizzard (aka Fancy Bear) and Emerald Sleet reportedly leveraged LLMs to mimic official documents in phishing campaigns and to conduct vulnerability research, respectively, and emerging tools like WormGPT, DarkGPT, and FraudGPT are helping cybercriminals increase both the scale and effectiveness of their attacks.

Adding distributed denial of service to the extortion mix

Beyond traditional encryption, attackers are also deploying sophisticated multi-extortion methods that create compound pressure points. Simultaneous encryption, data theft, and distributed denial-of-service (DDoS) threats give attackers more leverage against organizations. To maximize profits, some ransomware groups auction off stolen "crown jewels" or confidential company data to the highest bidders on dark web marketplaces.

The fading line between cybercrime and hacktivism

While the majority of ransomware groups primarily pursue financial extortion, traditional boundaries between profit-driven cybercrime and ideologically motivated hacktivism are dissolving in troublesome ways. Ransomware as a service (RaaS) relies on a wider criminal ecosystem that consists of developers, affiliates, the zero-day market, and initial access brokers who are key to orchestrating attacks. The broader criminal ecosystem has become a service industry, with criminal groups building their brands or specializing in functions like money laundering. RaaS groups with hacktivist motivations are using ransom payments to fund their campaigns to advance ideological or political objectives. Moreover, hacktivists such as Head Mare, Twelve, and NullBulge have adopted ransomware tactics to cause greater disruption in the countries they are targeting, which further complicates the threat landscape.

Partners join the fight against ransomware

As organizations become more cyber resilient by putting a Zero Trust architecture and other security controls in place, they are better positioned to proactively mitigate ransomware. But they need more help, and it's beginning to arrive. Public—private partners of defenders and law enforcement are sharing threat intelligence and best practices and making a difference. Since 2022, FBI-provided decryption keys have saved victims more than US$800 million in payments. Governments are also introducing legislation aimed at banning organizations from paying threat actors. These policies benefit organizations since paying the ransom does not ensure the return of their data. Finally, cyber insurance providers are incentivizing organizations to strengthen security programs and offering their negotiating skills to lower ransomware payments.

Akamai's thought leadership and research

Akamai security research is committed to shining a light on the cybercriminal ecosystem by analyzing the emerging techniques used by adversarial groups. In this State of the Internet (SOTI) report, we spotlight two key threats:

- TrickBot malware, which is leveraged by certain ransomware groups, including Ryuk, Conti, and Diavol
- Cryptominers, which our researchers have identified as one of the critical intersection points within the ransomware landscape because their goals and strategies are similar to those of ransomware groups

Additionally, our threat experts provide strategic, actionable insights that empower security leaders and defenders to fortify organizational resilience, deploy robust protection, and proactively counter today's increasingly sophisticated ransomware threats.

Key insights of the report

Ransomware extortion tactics have been evolving. **Quadruple extortion is the newest tactic**, while double extortion is currently the most common tactic. And ransomware groups continue to seek additional ways to generate profit, such as by pressuring victims and weaponizing compliance.

More than US$724 million in cryptocurrency was extorted from strains linked to the TrickBot malware family, which is used by ransomware groups. The Akamai Hunt Team recently observed this malware in connection with four malicious scheduled tasks on five customer assets.

GenAI and LLMs increase the frequency and scale of ransomware attacks by enabling individuals with less technical expertise to launch sophisticated campaigns, as demonstrated by groups like FunkSec.

The emergence of hybrid ransomware hacktivist groups that are leveraging RaaS platforms to amplify impact (e.g., CyberVolk, Stormous, KillSec, Dragon RaaS, and DragonForce) demonstrates a significant shift in the ransomware landscape in which **political and ideological motives are becoming more intertwined with financial crime**.

The hacktivist groups Head Mare, Twelve, and NullBulge often use LockBit ransomware (built from leaked or publicly available builders) for political disruption. NullBulge specifically uses it to **target online communities and platforms that are operating with AI and online gaming tools**.

Although cryptominers pose a unique danger, their goals and the strategies they employ are similar to those of ransomware groups. Notably, nearly **50% of the cryptomining attacks we analyzed targeted nonprofit and educational organizations**, likely because they possess substantial computational resources and are less secure than other industries.

Overview of attack patterns and the impact on customers

Akamai research has observed a concerning trend: Multiple ransomware groups are increasingly targeting the same organizations simultaneously, heightening the risks to those organizations. Additionally, our research revealed significant fluctuations, with noticeable peaks and valleys in the number of global customers targeted by ransomware during 2024 (Figure 1). These fluctuations may also be evidence of volatility within and among the major ransomware groups, which frequently dissolve into smaller operations or rebrand in an effort to evade law enforcement and remain undetected.

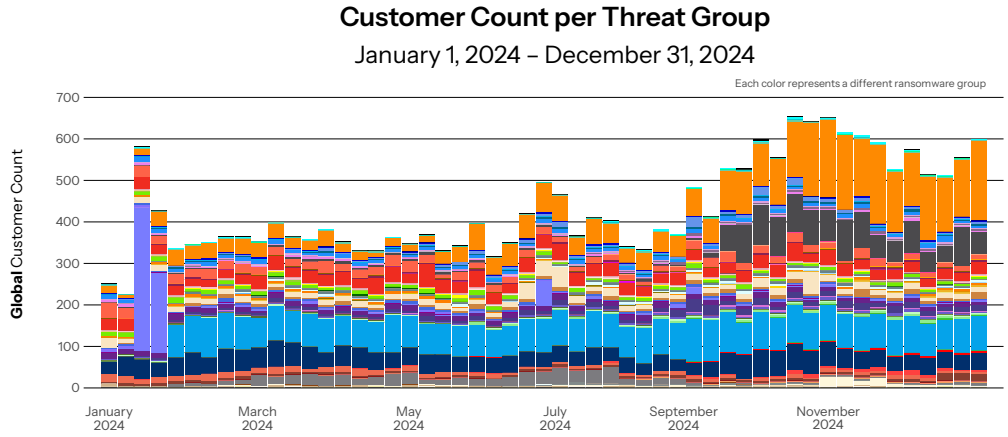

Fig. 1: The number of global customers targeted by ransomware attacks

The ransomware activity and trends we see regionally (Figure 2) mirror the global patterns in Figure 1.

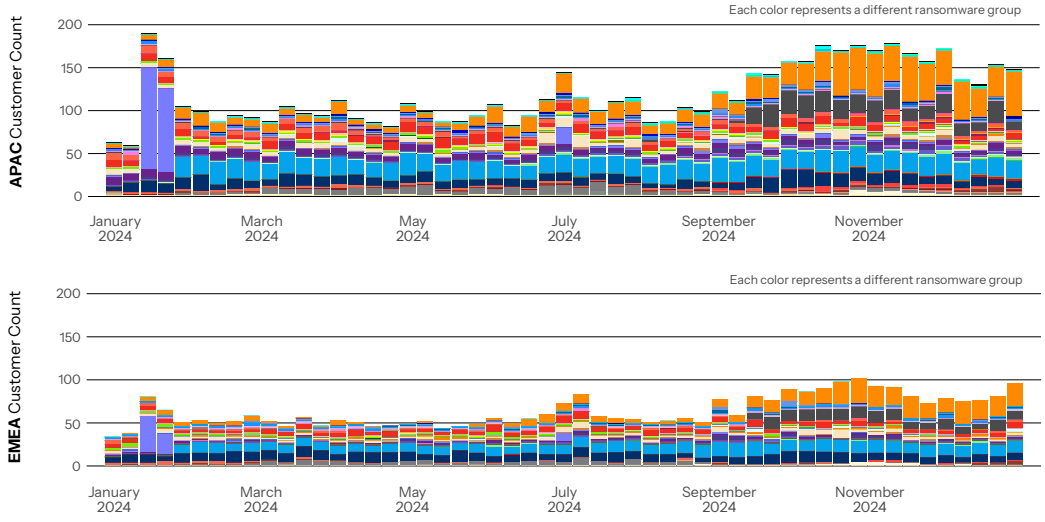

Fig. 2: The number of customers in the Asia-Pacific (APAC) and Europe, the Middle East, and Africa (EMEA) regions targeted by ransomware attacks

In 2024, ransomware spiked by 37%, accounting for 44% of the data breaches globally and for 51% in Asia-Pacific (APAC), according to the Verizon 2025 Data Breach Investigations Report. In Europe, the Middle East, and Africa (EMEA), the proportion of enterprises that experienced a ransomware attack grew to 27% in 2024. And in Latin America (LATAM), 29% of enterprises reported an attack in 2024, with a growing wave targeting small and medium-sized businesses.

To mitigate these risks, companies should prioritize strengthening their cyber resilience. This includes implementing segmentation to contain the attack and prevent threat actors from moving laterally within the network to compromise sensitive data.

Evolving extortion tactics

Ransomware extortion tactics have been evolving from single extortion (which is intrinsic to all traditional ransomware operations) to double extortion (e.g., the Maze ransomware group in 2019) to triple extortion (notably with the ALPHV/BlackCat in 2021) to quadruple extortion (e.g., CL0P in 2024; Figure 3).

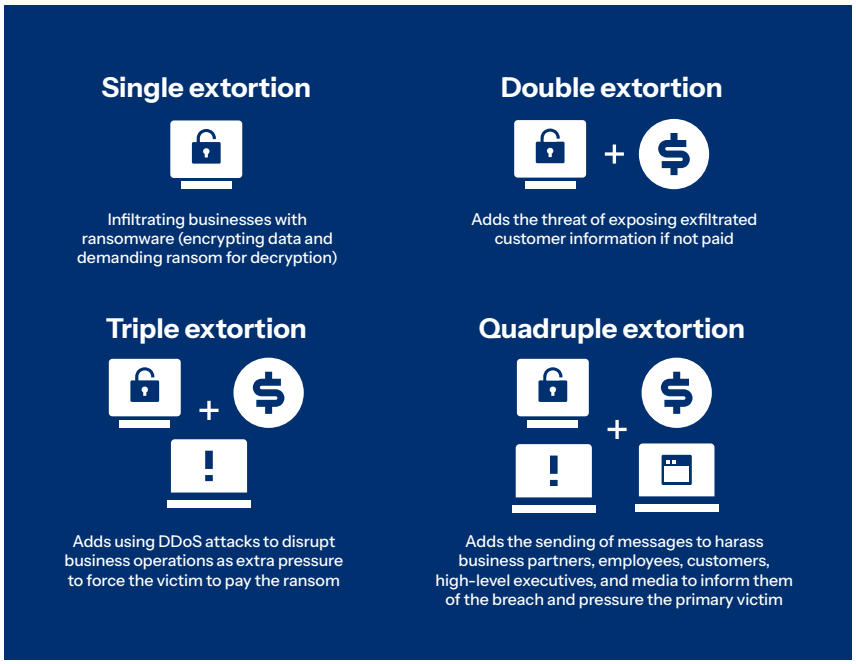

Fig. 3: Ransomware extortion tactics

This evolution of tactics has proven effective for ransomware groups, resulting in escalated average ransom payments. While triple and quadruple extortion are growing more frequent, double extortion still appears to be the most common tactic (Figure 4). And a new trend among ransomware groups that are using double and quadruple extortion tactics is the use of government regulations as leverage.

Ransomware	Double Extortion	Triple Extortion	Quadruple Extortion
Abyss Locker	⚠		
Black Basta	⚠		
FunkSec	⚠		
HellCat	⚠		
Interlock	⚠		
Lynx	⚠		
Morpheus	⚠		
Nnice	⚠		
RansomHub	⚠		
XELERA	⚠		
Akira	⚠	⚠	
Medusa	⚠	⚠	
ALPHV/BlackCat	⚠	⚠	⚠
CL0P	⚠	⚠	⚠
LockBit 3.0	⚠	⚠	⚠

Fig. 4: Akamai researchers have observed these ransomware groups employing various extortion tactics

The three groups that have historically been among the most prominent ransomware groups — ALPHV/BlackCat, CL0P, and LockBit — have all conducted quadruple extortion. And in February 2025, CL0P claimed responsibility for 385 attacks in just a few weeks, setting a new record for the most attacks ever attributed to a single group in one month. CL0P remains the most stable group of the three, given last year's shutdowns of ALPHV/BlackCat and LockBit. This is despite LockBit's return, which later led to the fragmentation of the group, its code being widely reused by others, and, most recently, the group being hacked.

Yet, the ransomware landscape has been shifting significantly over recent months with new and emerging groups becoming major threats. Similar to ALPHV/BlackCat, CL0P, and LockBit, many of these newer groups are also weaponizing compliance regulations as part of their tactical approach, whether implicitly (e.g., double extortion) or more explicitly (similar to ALPHV/BlackCat). Regardless, organizations need to be vigilant of such tactics and remain aware and in compliance with specific regulations regarding ransomware attacks.

Notable groups within regions

The most active groups in regions outside of North America include the top variants reported to the FBI's Internet Crime Complaint Center (IC3) in 2024 — Akira, LockBit, RansomHub, and Play — which underscores their global dominance. As an example, from 2024 through early 2025, Akamai researchers confirmed that LockBit was a persistent threat in APAC (surging in October 2024) and EMEA, despite having experienced various disruptions (Figure 5).

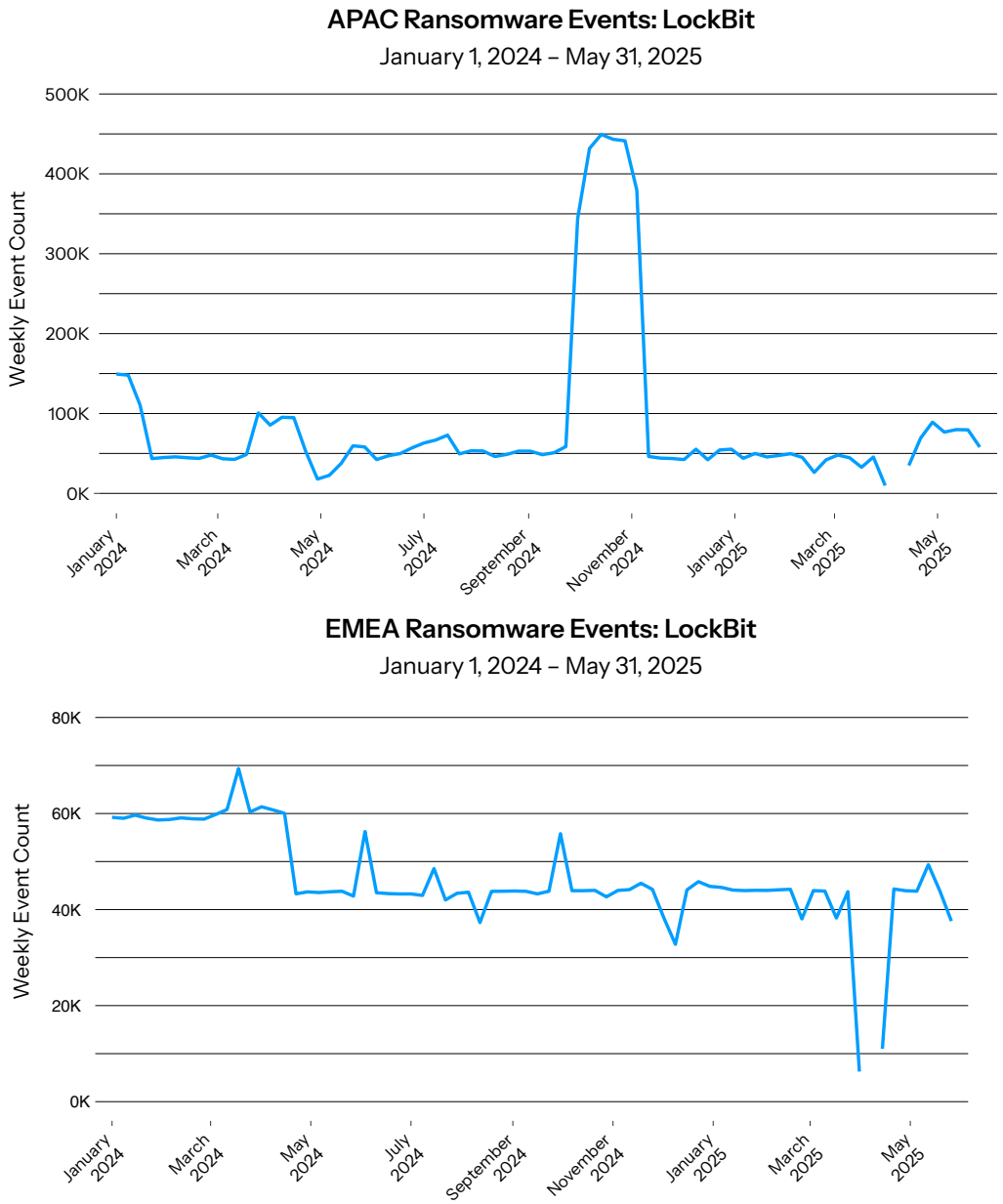

Fig. 5: LockBit remained an active threat in APAC and EMEA from January 2024 to May 2025

(Note: The decrease in April 2025 is not an accurate representation; there was a data collection issue at this time.)

⚠ Active groups in APAC

In APAC, well-known global ransomware syndicates such as LockBit, ALPHV/BlackCat, and CL0P are active, as are newer groups such as Royal/BlackSuit, RansomHub, Akira, Abyss Locker, and Play.

Abyss Locker leaked 1.5 terabytes of data from the Australian Nursing Home Foundation. And a Singapore-based law firm reportedly paid nearly US$1.9 million in a sophisticated ransomware attack by the Akira group.

Other regionally active threat actors also have had an impact across APAC. Termite (a Babuk affiliate) and Anubis actively targeted victims across the APAC region over the past year. Notable incidents include a ransomware attack on an Australian in vitro fertilization clinic in early 2025 by Termite, and Anubis's exfiltration and public release of sensitive patient records from multiple Australian medical clinics.

⚠ Active groups in EMEA

In EMEA, LockBit, RansomHub, Medusa, and Akira are some of the most active groups. January 2025 started with Medusa posting stolen documents from a U.K. government agency on a leak site. Akira published a list of data leakages impacting organizations across the region. Other public reports of specific incidents by these groups include an attack on a German manufacturer, a wave of attacks in Italy, and strikes against the industrial control systems of an energy plant in Spain.

A spate of attacks against U.K. retailers has been attributed to both Scattered Spider, a known affiliate of RansomHub, and DragonForce, which claims to be taking over RansomHub's infrastructure. Additionally, amid various takedowns by authorities and attacks by rival groups, LockBit and Black Basta have used adaptability and shifting tactics to maintain operations.

⚠ Active groups in LATAM

In LATAM, RansomHub, FunkSec, and Akira have been the most active ransomware groups recently. In one month, Akira led the number of LATAM extortion disclosures with six victims in Brazil, two in Argentina, and two in Colombia. Akira was also behind the notable 2024 attack against a LATAM airline. RansomHub activity included an attack against a government office in Mexico. Medusa is also having an impact, with a breach against a financial solutions provider in Brazil.

Regulation violation revelation: A trending threat

Recently, we've seen a growing trend in ransomware groups' threats to reveal that a company is in violation of regulations. This tactic raises the stakes on reputational damage to the brand and the potential cost of the attack (adding fines from regulators and legal fees). But weaponizing compliance is not entirely new. For example, in December 2019, REvil posted on a Russian hacker forum that if companies refused to pay ransom, then their data breach disclosures could lead to severe regulatory fines, potentially 10 times more than the ransom demand itself.* Also, near the end of 2023, the ALPHV/BlackCat ransomware group submitted a formal complaint to the U.S. Securities and Exchange Commission (SEC) against a digital lending solutions provider, alleging that the company failed to disclose a cybersecurity breach within the required time frame.

The Anubis ransomware group (which began operations in late 2024) often highlights regulatory violations, such as for healthcare privacy breaches, to shame organizations publicly (e.g., via the social platform X, a leak site, or direct communication) and thus focuses its efforts on industries in which compliance risks are high (e.g., healthcare and engineering). Also, RansomHub (which was first detected in February 2024) has become a major threat with its high-profile ransomware attacks and rapid growth. This group has explicitly encouraged affiliates to leverage the threat of regulatory penalties (e.g., the General Data Protection Regulation [GDPR], the Personal Information Protection Law [PIPL], and the Personal Data Protection Law [PDPL]) to increase pressure on victims. The ransomware group known as WereWolves (which emerged in May 2023) also weaponizes compliance in addition to using other aggressive tactics (e.g., double extortion, use of LockBit 3.0, and public communication with victims) on their targets.

The impact of these regulation violation threats has been felt worldwide, as Anubis, RansomHub, WereWolves, and ALPHV have explicitly threatened victims by weaponizing compliance (Table 1).

Ransomware Group	Regions Targeted	Industries Targeted	Regulatory Exposure (Laws/Regulations Threatened)	Where Threatening to Report
Anubis	Global, especially U.S. and Europe	Healthcare, government	HIPAA (U.S.), GDPR and Data Protection Act 2018 (U.K.), and GDPR (EU)	U.S. Department of Health and Human Services (HHS), U.K. Information Commissioner's Office (ICO), and European Data Protection Board (EDPB)
RansomHub	Global, especially Europe, China, and Saudi Arabia	Spread widely across industries with concentration in IT and critical infrastructure	GDPR (EU), PIPL (China), and PDPL (Saudi Arabia)	EDPB, Cyberspace Administration of China (CAC), and the Saudi Data and Artificial Intelligence Authority (SDAIA)
WereWolves	Russia, Europe, North America, and Africa	Spread widely across industries with concentration in IT, financial services, and hospitality	Not specific but likely to threaten: GDPR (EU) ePrivacy (EU), GLBA (U.S.), SEC rules (U.S.), Federal Law 152-FZ (Russia), Data Protection Act, 2012 (Act 843; Ghana)	Not specific but likely to threaten: National Data Protection Authorities (DPAs), SEC, Roskomnadzor, and Data Protection Commission
ALPHV (ceased operations in 2024)	Global, especially U.S.	High technology and healthcare	SEC (U.S.) disclosure rules and HIPAA (U.S.)	SEC and HHS (U.S.)

Table 1: Ransomware groups that are weaponizing compliance

*The message stated, "GDPR. Do not want to pay us – pay x10 more to the government. No problems."

Note that the list in the table only details specific regulation threats received. It's likely that these groups weaponize other regulations in other regions as well. Even if these groups only engage in double extortion and don't go to the authorities, they are exposing sensitive information that may trigger regulation violations for the victim anyway. That's why we included the other potential regulation violations that may be exposed (such as those triggered by WereWolves) and their associated governing authorities.

Cybersecurity regulations have been beneficial in promoting a more secure digital and operational environment for businesses, and in enhancing data protection, continuity, trust, and compliance across industries. Yet, as cybersecurity regulations continue to tighten across various industries and regions, the playing field widens with more opportunities for cybercriminals to find compliance violations to extort and use as leverage in demanding ransom payments.

Regional pain

Threat actors do their homework and gravitate toward regions where the threat of regulatory exposure could cause the most damage. For example, in EMEA, government-driven regulatory bodies drive compliance within the EU and the United Kingdom, creating greater consistency in reporting time frames, enforcement, and financial penalties. Similarly, in North America, industry councils or associations, federal agencies, and states/provinces actively drive regulations, and enforcement is typically rigorous.

In contrast, LATAM's rapid digital transformation, coupled with the vulnerabilities of increasingly connected systems, makes the region an attractive target for ransomware attacks. However, inconsistent cybersecurity regulations and enforcement across the region diminish the impact of this type of extortion. The same is true in APAC, where the region is a patchwork of new compliance mandates, with stricter enforcement in some areas and inconsistent consequences for failure to report in others. As such, we have yet to see evidence that LATAM and certain areas in APAC have been impacted by groups that threaten regulatory exposure, and some newer regulations such as NIS2 have yet to be leveraged. However, we know how quickly threat actors can shift their focus, so it is worth tracking broader trends.

Our researchers continue to track the evolving use of regulation extortion tactics by ransomware groups. It can be complex for international companies to stay attuned to regional reporting requirements to ensure their security capabilities provide compliance artifacts in a way that supports their audit and crisis management actions. However, it's important to remove this arrow from the threat actor's quiver. Some key pieces of regulation to track in various regions include:

- **APAC:** The reporting time frames range from 12 to 72 hours, depending on the severity of the impact of the attack. Some countries, such as Japan, do not currently impose fines. In other countries, such as Singapore, failure to comply with PDPA can result in fines of 10% of annual revenue. In India, criminal penalties are also possible.
- **EMEA:** The requirements for timely reporting and financial penalties are similar to those in APAC. For example, failure to comply with NIS2's 24-hour reporting deadline can result in fines up to €10 million or 2% of the company's global annual revenue, whichever is greater. Under GDPR, organizations have more time to report (within 72 hours), but the fines can double. Additional ransomware reporting requirements in both the United Kingdom and the European Union are currently under review.
- **LATAM:** Regulations vary from country to country. Brazil has one of the most stringent policies under the Lei Geral de Proteção de Dados Pessoais (LGPD), with initial reporting required within 72 hours and supplemental information due within 20 days. Fines for failure to report can be 2% of annual revenue per infraction.
- **North America:** Failure to report within 24 hours has resulted in SEC fines of US$10 million. Nondisclosure of Health Insurance Portability and Accountability Act of 1996 (HIPAA) breaches can result in fines from US$100 up to US$1.5 million per incident, depending on the severity of the infraction, in addition to criminal penalties. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), expected to go into effect in 2026, mandates ransomware reporting.

Inside the RaaS ecosystem

RaaS has revolutionized ransomware operations, transforming them from highly specialized attacks into scalable, subscription-based services accessible to a broader range of cybercriminals. This pivotal shift eliminates technical barriers that previously impeded ransomware deployment, enabling cybercriminals with minimal technical expertise to execute sophisticated attacks. The democratization of ransomware allows developers in criminal groups to earn steady revenue while enabling less technically savvy threat actors to participate in high-stakes digital extortion campaigns. The proliferation of RaaS significantly increases both the scale and frequency of attacks, compelling organizations to implement more resilient security architectures to withstand this threat.

RaaS platforms like REvil, Ryuk, and DarkSide, which emerged in the mid-2010s, pioneered the concept of providing ready-to-use ransomware kits to affiliates for a share of the proceeds. Beyond financial gain, the real-world ramifications of this business model became evident in high-profile operations like the Colonial Pipeline incident (attributed to the DarkSide group), which disrupted essential services and critical infrastructure in the United States while generating substantial profits for its operators.

Key entities in the RaaS business model

The rapid growth and success of RaaS stems from its accessibility, operational efficiency, and organizational structure that mirror legitimate businesses. These criminal enterprises employ a division of labor with specialized roles that optimize their overall operations. Figure 6 illustrates the primary players in the RaaS ecosystem and their specific functions.

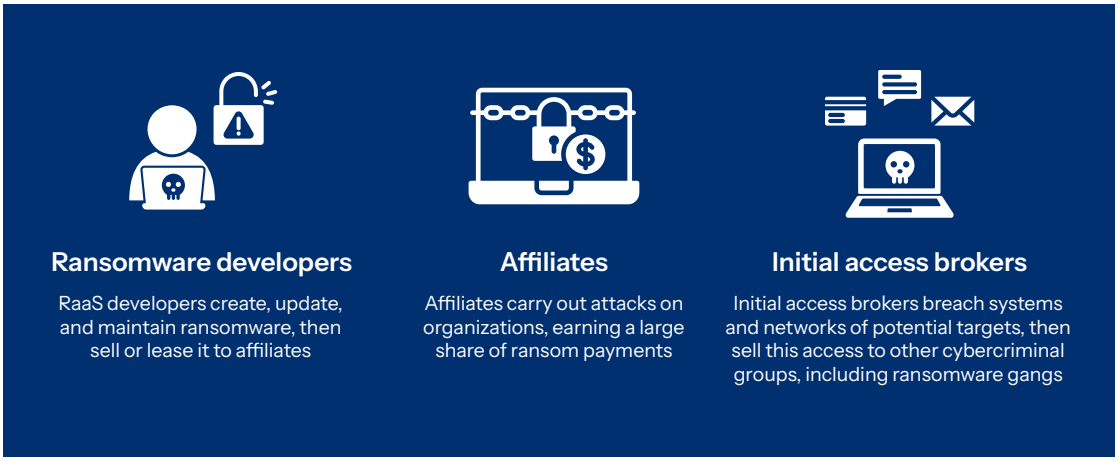

Fig. 6: The critical players that make up the RaaS chain

Ransomware developers

RaaS developers or operators are responsible for creating, updating, and maintaining the ransomware software that they subsequently sell or lease to affiliates. Additionally, they design robust malware strains (many with user-friendly interfaces and 24/7 support for their customers), manage the supporting infrastructure, and establish secure communication channels for affiliates. These highly skilled cybercriminals frequently implement new features and capabilities to remain undetected and to ensure operational reliability.

Financial arrangements typically follow a profit-sharing model, with splits ranging from 60/40 to as favorable as 90/10 — with the larger percentage going to the affiliate who implements the attacks.

Affiliates

Affiliates acquire ransomware from developers through dark web marketplaces and identify targets, deploy attacks, and sometimes negotiate with victim organizations. These cybercriminals may pay a monthly fee to lease the ransomware software, or they may obtain a lifetime license. Unlike developers, affiliates generally possess fewer technical skills, increasing their risk of operational errors and exposure to law enforcement.

Although affiliates select the targets, the developers provide a set of rules that the affiliates need to abide by; for example, target restrictions to certain countries or industries. Breaking such rules could mean expulsion from the group — or, in some cases, the developers will provide the decryptor to the victim for free. For a time, several ransomware groups avoided targeting healthcare organizations, particularly during the COVID-19 pandemic. DragonForce, with code that is an amalgamation of LockBit 3.0 and Conti code, claims to follow a moral code that excludes some types of healthcare targets.

Initial access brokers

To expedite victim identification and reconnaissance, affiliates often engage initial access brokers (IABs) who specialize in breaching targets and selling network access to cybercriminals, including ransomware operators.

IABs have a specific set of skills that allow them to streamline RaaS operations by performing the work of gaining footholds without launching attacks themselves, thus avoiding attention from law enforcement. They sell various access types, including Remote Desktop Protocol (RDP), VPN access, email access, and file share access. Although RDP is the most common type of access sold, it's worth noting that VPN access is also gaining momentum, potentially because it provides stealthier and more direct access to corporate networks.

The price of access depends on the target organization's revenue, with more valuable environments commanding higher prices. In 2024, 86% of access listings were priced at US$3,000 or less.

Major players in the RaaS ecosystem

The following profiles describe some of the most notable RaaS groups active from 2024 through early 2025 and emphasize their innovative tactics. The groups are organized according to the severity of their methods and their impact on companies as of this writing. Their innovations demonstrate how RaaS continues to evolve, and how operators and affiliates continue to adapt, despite increasing pressure from security defenders and law enforcement agencies.

RansomHub

RansomHub, first observed in early 2024, quickly rose to prominence for its multi-OS ransomware that targets Windows, VMware ESXi, and SFTP servers. The group, which uses double extortion, has impacted more than 200 organizations across healthcare, education, and the public sector industries.

Earlier this year, we saw a significant increase in RansomHub activity in our customers' environments, with some periods recording close to 700,000 events and some periods that even exceeded that number (Figure 7).

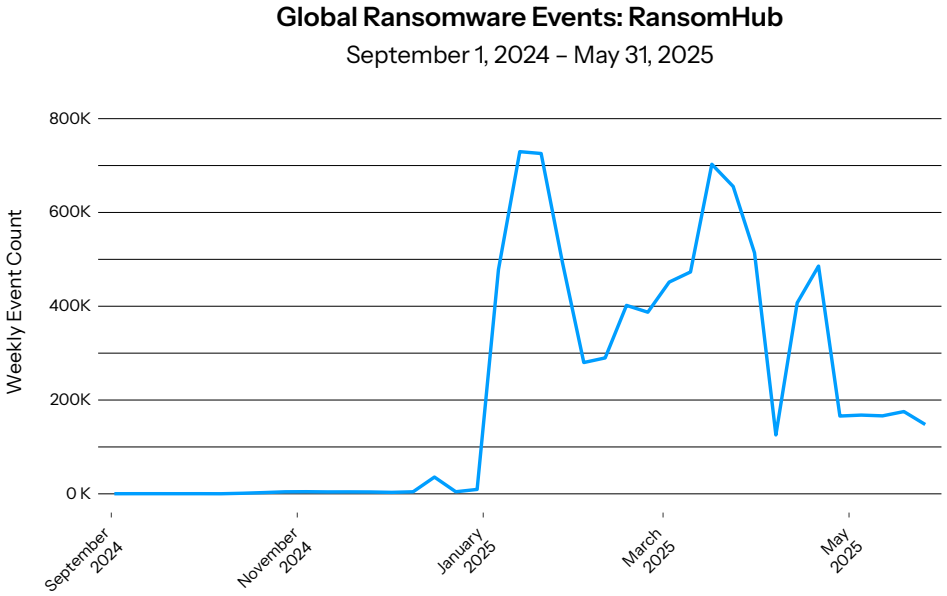

Fig. 7: RansomHub's growing prevalence since January 2025 is evident in the increased traffic observed among our customers

RansomHub's prevalence stems from its use of evasion tools like EDRKillShifter to disable endpoint protections and its exploitation of vulnerabilities such as CVE-2024-1709. Like most groups, RansomHub uses a double extortion tactic, encrypting data and threatening to leak exfiltrated information unless victims pay. As part of its extortion mechanism, RansomHub also instructs affiliates on its leak site to report victims to regulatory bodies, such as the GDPR authorities, to pressure organizations to pay the ransom to avoid regulatory penalties. Additionally, the operators supply affiliates with customized tooling and support, enabling them to steal confidential information as a separate step. In some cases, affiliates re-target previously compromised organizations, leveraging stolen data for additional financial gain.

RansomHub's structure and business model, including a generous 90/10 ransom split, attract both experienced threat actors and novice cybercriminals. RansomHub's infrastructure went offline on April 1, 2025, with several affiliates migrating to groups such as DragonForce and Qilin.

CL0P

CL0P distinguishes itself through the systematic exploitation of zero-day vulnerabilities in file transfer systems. These include attacks targeting a file transfer appliance (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104), GoAnywhere MFT (CVE-2023-0669), and PaperCut (CVE-2023-27350 and CVE-2023-27351). Most notably, CL0P exploited MOVEit Transfer (CVE-2023-34362), compromising more than 2,500 vulnerable servers. Recently, the group claimed to have siphoned and leaked data from a cloud services provider and exploited zero-day vulnerabilities in Cleo-managed file transfer products, enabling remote code execution.

CL0P employs a distinctive strategy: Remain dormant between carefully orchestrated campaigns that coincide with zero-day vulnerability discoveries. This approach effectively enables the group to breach high-value targets while maintaining a relatively low overall victim count, except during exploitation spikes. Additionally, it uses a triple extortion mechanism — and sometimes even a quadruple extortion tactic in which it reaches out to customers and threatens to release their information to further pressure the affected organizations to pay the ransom.

FunkSec

The RaaS group FunkSec exemplifies how GenAI and LLMs are reshaping ransomware operations. Emerging in late 2024, FunkSec, which follows a double extortion model, quickly gained attention by reportedly leveraging AI tools to develop its ransomware code, enhance support chats and communications, and rapidly generate new iterations. Its latest version, still in development, may include multiple extortion schemes, such as auctioning stolen data to the highest bidder, targeting victims' personal networks and families, and launching DDoS attacks to intensify pressure on targets. Researchers believe FunkSec's heavy reliance on AI stems from the group's lack of technical expertise.

FunkSec has moved away from traditional leak sites by employing an auction platform, FunkBID, which allows the sale of stolen data to maximize profits. Their Rust-based ransomware frequently targets organizations that were previously compromised by other groups, using data stolen in prior breaches, which complicates efforts to verify the legitimacy of their claimed attacks. Many researchers question whether FunkSec's activities represent genuine threats or are simply noise to boost their visibility.

The group has formed strategic collaborations with other ransomware threat actors, such as FSociety, to expand its criminal network. Some reports trace FunkSec's activities to Algeria and suggest possible hacktivist motives in addition to financial motives. Despite their inexperience, FunkSec's innovative use of AI in digital extortion could signal an emerging trend in the ransomware landscape.

LockBit 3.0

Prior to the high-profile international law enforcement collaboration in February 2024 (known as Operation Cronos), LockBit dominated the threat landscape. Our previous ransomware SOTI report observed that LockBit accounted for the majority of the victim organizations from October 2021 through May 2023. What has made this group prevalent for a long time is its constant innovation. Its major iteration, LockBit 3.0, offers affiliates customizable payloads as well as double (and occasionally triple) extortion tactics. LockBit 3.0 is known for targeting critical infrastructure and maintaining a sophisticated affiliate structure, complete with bug bounty programs and extortion portals. Its bug bounty program entices hackers to submit information about flaws in the software for rewards ranging from US$1,000 to US$1 million, further amplifying the threat's prevalence.

As a testament to LockBit's resiliency, days after the momentous disruption to their operations, they re-emerged with a new data leak site. Although reports noticed a significant decline in the group's activity in the months following Operation Cronos, LockBit's influence remains undeniable (Figure 8).

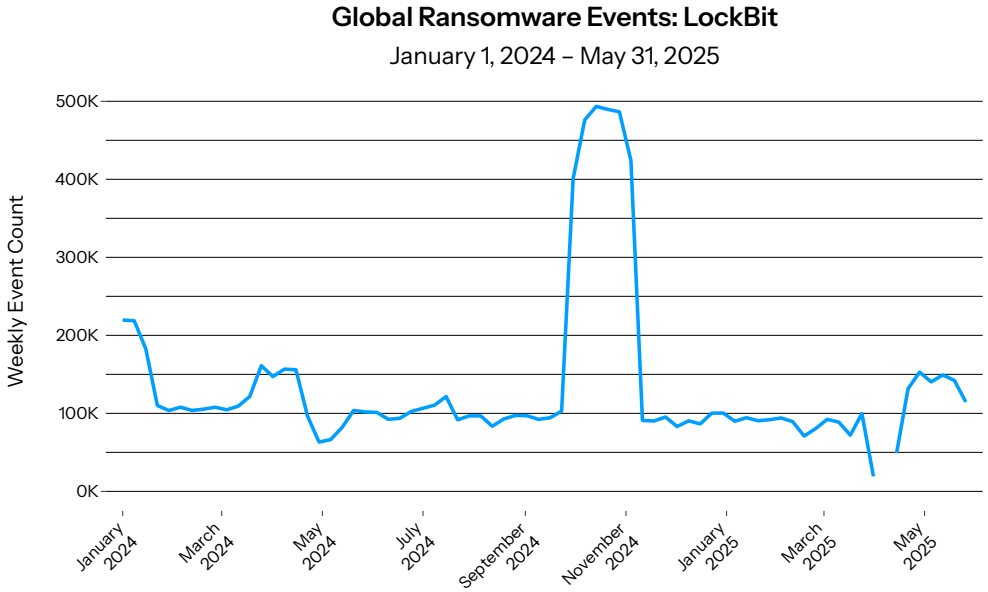

Fig. 8: LockBit's activities across Akamai's customer environments spiked in October 2024, correlating with the uptick in victims published by the group on their data leak site

In May 2025, LockBit suffered a major breach from unknown perpetrators, which led to data leaks from December 2024 to April 2025 that included bitcoin wallet addresses used in ransom operations, negotiation messages between LockBit and its victims, and others. LockBit's dark web affiliate panels were defaced and left with the message shown in Figure 9, which included a link to download a leaked MySQL database dump.

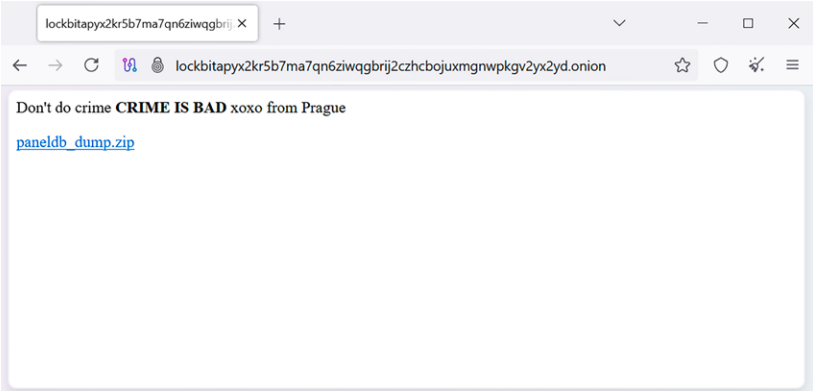

Fig. 9: LockBit's data leak site was defaced in April 2025 by unknown perpetrators (Source: Bleeping Computer)

Black Basta

Black Basta follows a double extortion approach and has been linked to attacks of more than 500 organizations globally, including healthcare providers, manufacturers, and financial institutions. In our customers, we saw a peak of more than 120,000 attack attempts in one week (Figure 10).

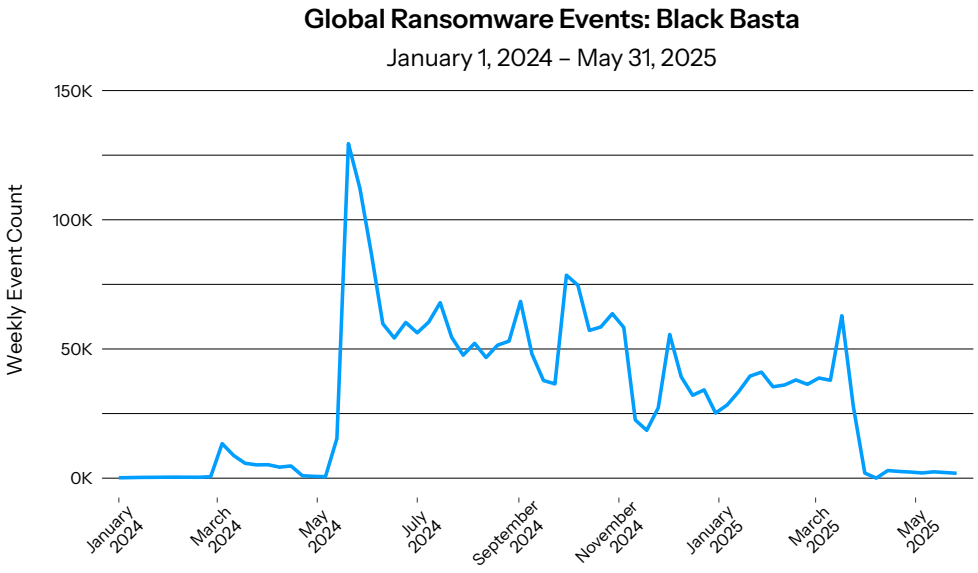

Fig. 10: Black Basta's ransomware activity peaked at more than 120,000 in one week

The group has been associated with former Conti operators and is known for disabling security software and exfiltrating sensitive information before deploying ransomware. In February 2025, the group's chats were leaked, which revealed insights into their operations, tactics, techniques, and procedures (TTPs) — including brewing discord within the group— which provided defenders with valuable intelligence to enhance their security posture.

In addition to having an opportunity to purchase a zero-day vulnerability targeting Ivanti Connect Secure for US$200,000 (it is unclear whether that purchase was ever made), Black Basta actively uses BRUTED, a brute-force tool that targets edge devices such as VPNs.

Medusa

Since emerging in 2021, the Medusa ransomware has impacted multiple industries — healthcare, education, legal, technology, and manufacturing — and has continued attack attempts on our customers' networks from January 2024 through May 2025 (Figure 11).

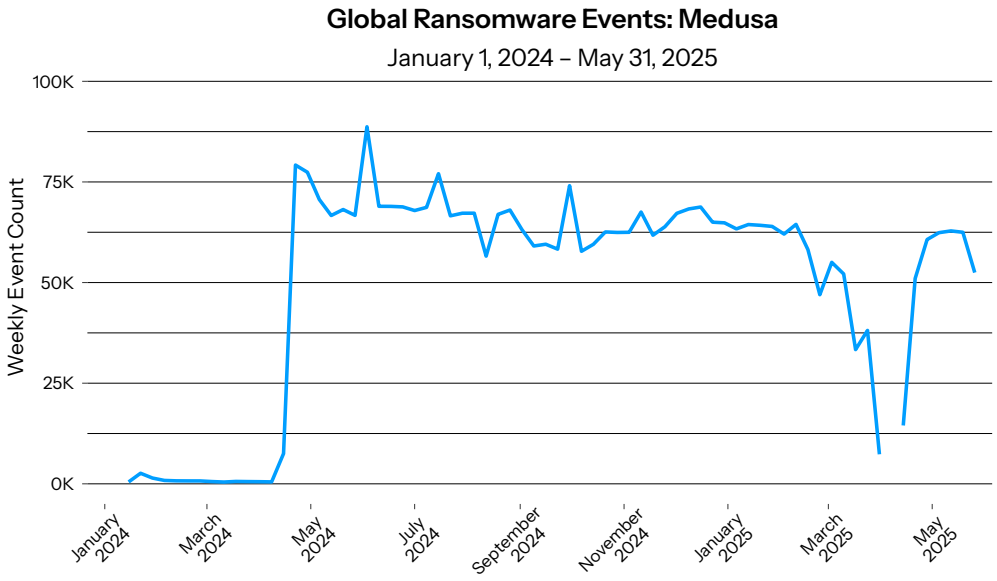

Fig. 11: Medusa continued attack attempts on our customers' networks during the reporting period

Medusa began as a closed operation wherein the developers handled all the attacks and negotiations, and then it shifted to a RaaS business model. To breach their intended targets, the group uses phishing campaigns and exploitation of unpatched vulnerabilities like CVE-2024-1709 and CVE-2023-48788. To exert extra pressure and a sense of urgency, their data leak site shows a countdown timer.

ALPHV/BlackCat

ALPHV, also known as BlackCat, is considered one of the most sophisticated RaaS groups that employs a triple extortion scheme. First identified in late 2021, this ransomware is notable for being written in the Rust programming language, which offers flexibility and evasion capabilities. The group employs living-off-the-land techniques to maintain persistence in target networks and it bypasses security controls like two-factor authentication using Evilginx 2, a tool that hijacks sessions and steals credentials.

In 2023, ALPHV targeted Reddit and deviated from traditional encryption tactics by primarily exfiltrating confidential information. The FBI disrupted the group's operations in December 2023 by seizing their data leak site. However, ALPHV quickly rebounded to execute a high-profile attack against Change Healthcare in February 2024. After that high-profile cyberattack, the group's activity decreased (Figure 12) and they "disappeared" (Figure 13), with some researchers speculating that its affiliates rebranded as and/or moved to RansomHub.

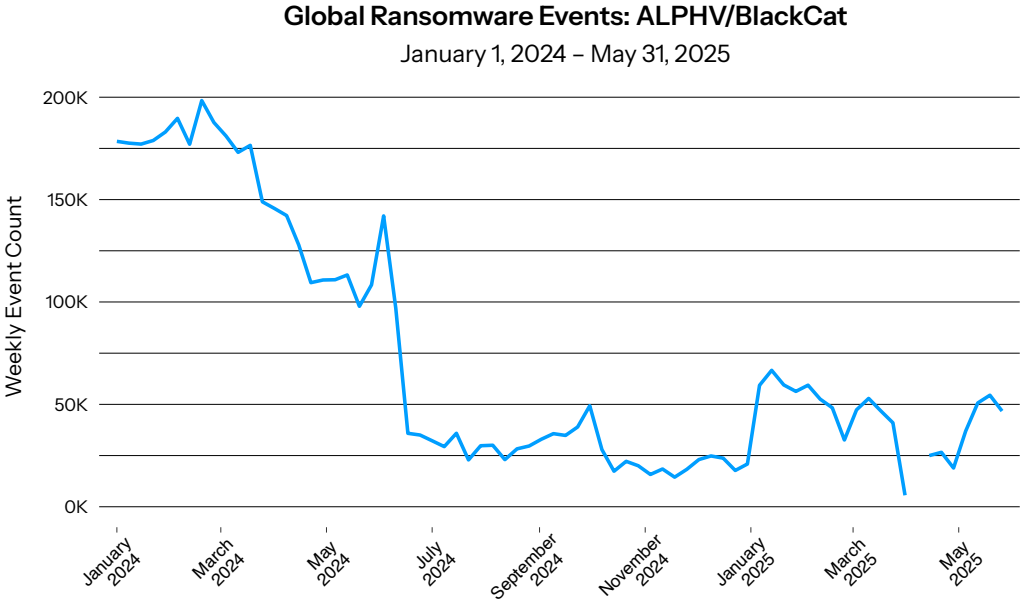

Fig. 12: ALPHV/BlackCat's activity steadily decreased following their high-profile cyberattack in February 2024

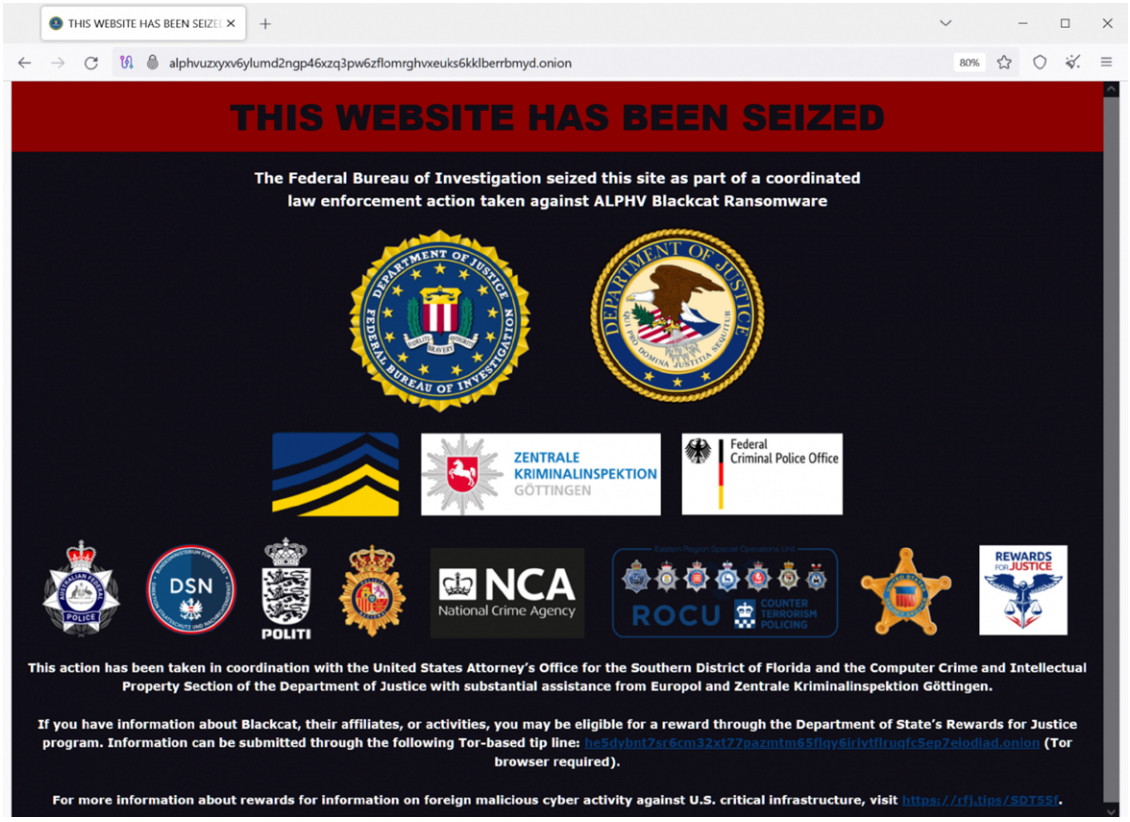

Fig. 13: To fake their own demise, ALPHV used a bogus banner indicating that the FBI had seized their data leak site (Source: Bleeping Computer)

Akira

Akira, which began in early 2023, rapidly expanded its victim list across industries, including manufacturing, education, and government. The group uses both double and triple extortion techniques — encrypting data; threatening leaks; and, in some cases, applying direct pressure via phone or by exploiting internal devices like unsecured webcams. Akira often gains access via VPN vulnerabilities and lives off the land with tools like PowerShell and SoftPerfect.

Interlock

Interlock is an emerging ransomware operation first observed in late 2024. It uses a double extortion model and maintains a leak site known as the Worldwide Secrets Blog. Victims are often compromised through phishing or via malicious installers that pose as browser updates. The group uses tools like AnyDesk and PowerShell for lateral movement and evasion, and is considered technically capable, despite its recent debut.

Combating RaaS

The continued success of RaaS in 2024 and 2025 underscores the evolving sophistication of cybercriminal operations. As threat actors increasingly leverage zero-day exploits, organizations need Zero Trust solutions to minimize potential damage.

There is also a critical need to secure VPNs, particularly those that use default or recycled credentials, to prevent unauthorized access. Our Defenders' Guide includes best practices such as using dedicated identities for VPN authentication and limiting service account permissions to help security practitioners enhance the security of their VPNs.

Companies must continuously innovate and update their cybersecurity defensive capabilities, ensuring that web application firewall (WAF) protections extend to newer infrastructure like APIs and GenAI. Additionally, implementing protections behind the edge, such as segmentation, that prevent active attacks from moving throughout the environment is crucial for minimizing ransomware impacts.

Putting the RaaS in hacktivism

In the criminal RaaS business model, alliances are formed for a variety of reasons. Alliances with hacktivists — hackers with malicious intent to promote a political or social cause — allow RaaS providers to borrow/lean on hacktivist motives or political justifications to attract attention, bolster legitimacy, or obscure their profit motives, particularly when under scrutiny from law enforcement or when facing potential government action. This approach also complicates efforts by authorities to treat RaaS groups solely as criminal enterprises.

In this section, we'll explore — in chronological order — some notable ransomware groups that are providing RaaS and are also considered hacktivists (we call them hacktivist/ransomware hybrids). We'll also take a deeper look into some hacktivist groups that are using ransomware as a tool.

Hacktivist/ransomware hybrids

Stormous

Stormous, a hacktivist/ransomware hybrid group that began operating in mid-2021, is both politically and financially motivated. It is known for forming alliances with other cybercriminal organizations (most prominently GhostSec) to launch joint ransomware campaigns using tools such as GhostLocker. It often leaves communications and ransom notes in Arabic, and its membership is believed to include individuals from Russia as well as from Middle Eastern countries. The group has taken responsibility for attacks on major companies, such as Coca-Cola and Mattel, and has also targeted government and private sector organizations across multiple countries. Stormous is known to target countries perceived as hostile to Russia or aligned with Western interests. This includes the United States, Ukraine, India, France, Spain, and Vietnam.

DragonForce

The hybrid threat actor known as DragonForce is a Malaysia-based geopolitical ransomware group that emerged in mid to late 2023. It quickly became known for high-profile, disruptive attacks across multiple industries and countries and is considered one of the most prolific currently active ransomware groups. DragonForce especially targets Israel and India. It also targets government agencies, public transportation, law firms, medical practices, and major retailers in the United Kingdom, and organizations in the United States, Saudi Arabia, Australia, and more.

KillSec

KillSec ransomware, which began October 2023, implements operations primarily driven by a pro-Russian and retaliatory political agenda, frequently aligning its cyberattacks with Russian geopolitical interests. Its main target is the healthcare industry, followed by finance and government entities. KillSec has shown a particular interest in targeting India and other Asian countries, such as Bangladesh, but also attacks other countries, including the United States.

CyberVolk

CyberVolk originally emerged in June 2024 as a politically motivated hacktivist group and started using ransomware for retaliation toward adversaries of Russia or India. The group mainly targets critical infrastructure, government entities, and scientific institutions, and it collaborates with other hacktivist and pro-Russia groups, such as NoName057(16), Moroccan Dragons, and LAPSUS$. Spain stands out as a primary target, especially following the arrest of NoName57(16) members. CyberVolk's operations have also been broadly aimed at NATO-aligned countries.

Dragon RaaS

Another hacktivist/ransomware hybrid group with "dragon" in their name, Dragon RaaS, emerged in July 2024 as an offshoot of the Stormous group. It is associated with pro-Russian hacktivist circles, and its core activity is ransomware deployment and extortion. Dragon RaaS focuses on smaller organizations with weak security, primarily in the United States, Israel, United Kingdom, France, and Germany.

Table 2 summarizes the details of these groups.

RaaS Hacktivists			
Group	Emergence	Origin	Targeted Regions
Stormous	Began operating in mid-2021	Russia and Middle East	U.S., Ukraine, India, France, Spain, Vietnam
DragonForce	Emerged in mid to late 2023	Malaysia	India, Israel, U.K., U.S., Saudi Arabia, Australia
KillSec	Began in October 2023	Eastern Europe and/or Russia	India, Bangladesh, Asia broadly, U.S.
CyberVolk	Started as hacktivists and began using ransomware in June 2024	Russia and India	Spain, NATO-aligned countries
Dragon RaaS	Emerged in July 2024	Russia	U.S., Israel, U.K., France, Germany

Table 2: Examples of hacktivist/ransomware hybrid groups that are using RaaS

Hacktivist groups that are using ransomware as a tool

The previous groups were characterized as hybrids: ransomware groups that are also considered to be hacktivists because they are leveraging RaaS platforms not only for driving financial profit but also for advancing ideological or political agendas. However, there are several prominent hacktivist groups that are not considered to be ransomware groups in the traditional sense, even though they are using ransomware as a tool.

For example, the hacktivist groups Head Mare, Twelve, and NullBulge have all incorporated ransomware into their hacktivist toolkit. Yet, they primarily use ransomware as a tool for political disruption, not financial gain. Also, each group uses LockBit ransomware built from leaked or publicly available builders instead of paying for RaaS arrangements, as typical RaaS affiliates do.

While Head Mare primarily targets organizations in Russia and Belarus, Twelve mainly targets Russian entities, and NullBulge is not tied to a specific geographic region but to online communities and platforms where AI and gaming tools are developed, distributed, and used (Table 3).

Hacktivist Groups Using Ransomware			
Group	Emergence	Origin	Targeted Regions
Head Mare	2023	Aligns with anti-Russian hacktivism in the Russia-Ukraine war	Russia and Belarus
Twelve	Active since April 2023	Likely stems from Pro-Ukrainian orientation	Russia
NullBulge	Spring of 2024	Unknown	Not particularly geographically focused, but instead targets AI and gaming communities; impacted countries include U.S. and India

Table 3: Examples of hacktivist groups using ransomware as a tool

Security spotlight

A malicious treat with TrickBot by Or Zuckerman

Wizard Spider (aka TrickBot) is a financially motivated cybercrime group that targets critical infrastructure, including healthcare systems, and has ties to Russian intelligence services that provide a malicious tool known as TrickBot to its ransomware groups. Ransomware groups that are part of Wizard Spider and use TrickBot include Diavol and RaaS operators Ryuk and Conti. And these groups have been responsible for some of the most significant ransomware attacks worldwide.

TrickBot, which originated in 2016, began as a sophisticated, modular banking Trojan that has now developed into a highly versatile malware platform capable of supporting a wide range of cybercriminal activities (including ransomware). Strains linked to TrickBot have extorted more than US$724 million in cryptocurrency. TrickBot also provides initial access to victim networks, steals credentials, and enables lateral movement within compromised environments. In May 2025, TrickBot's infrastructure was disrupted by Europol and Eurojust as part of Operation Endgame 2.0, and its operators are facing heightened legal action. Yet, TrickBot has demonstrated the ability to recover from past disruptions, so continued vigilance is still warranted.

Wizard Spider's TTPs

The Akamai Hunt Team that supports customers recently uncovered four malicious scheduled tasks linked to the TrickBot malware family all disguised under the name "WindowsUpdate" across five customer assets. These tasks were set up to run payloads located in the C:\ProgramData directory. Within this folder, the discovered TrickBot malware family files included a malicious DLL file, a BAT script used to register the DLL as a COM object within the Windows Registry, and an executable that mimicked an interactive SQL shell, which may suggest the attacker engaged in direct, hands-on-keyboard activity. The impacted customers were notified and were able to take action before ransomware was able to launch.

The Akamai Hunt Team commonly works with customers to make sure they understand when common evasive techniques like API hammering are being implemented by both the DLL and BAT files. This involves repetitive benign API calls to delay execution and bypass detection mechanisms. These kinds of techniques (e.g., API hammering, TrickBot malware using scheduled tasks disguised as "WindowsUpdate," hands-on-keyboard activity) exemplify the broader TTPs used by Wizard Spider and its ransomware operators (Diavol, Ryuk, and Conti). These groups consistently leverage stealth, persistence, and TrickBot malware (often as an initial access vector) to maximize their reach and evade detection.

Industry trends

Financial services*

Ransomware remains one of the most serious and ubiquitous threats facing the financial services sector, according to the recent Navigating Cyber 2025: Annual Threat Review and Predictions report from the Financial Services Information Sharing and Analysis Center (FS-ISAC). However, while ransomware operators extorted record-high dollar amounts in 2024, FS-ISAC's intel-sharing platform recorded a significant decline in reports of ransomware incidents.

That trend is reflected in leak site data — except as it applies to Asia (Table 4). According to data collected by eCrime Threat and Risk Intelligence Services, Asia was a particular focus of ransomware attacks. Indeed, ransomware operators claimed more attacks on Indian financial institutions than either U.K. or Canadian firms, though still significantly fewer than U.S. firms.

Ransomware Leak Site Claims by Country	
United States	151
India	17
United Kingdom	16
Canada	11
Belgium	7

Table 4: Distribution of affected financial services organizations by country in 2024 (Source: eCrime Threat and Risk Intelligence Services)

Ransomware operators tend to be opportunists, but experts say they're also becoming more sophisticated.

FS-ISAC predicts that attackers will exploit GenAI to automate and customize attacks on financial services firms and sell initial access as an industrial-scale service offering. These types of approaches amplify the risks of the sector's already dangerous threat environment — and they make timely threat intelligence and investments in prevention increasingly critical to its cyber defense and resilience.

*The information in this section was provided by FS-ISAC.

Commerce

Ransomware groups consistently target the commerce industry, particularly retailers and ecommerce businesses. In early 2025, the CL0P ransomware group exploited two zero-day vulnerabilities (CVE-2024-50623 and CVE-2024-55956) in Cleo-managed file transfer solutions. Retailers rely on these platforms for essential functions, such as order management, which attackers leveraged as unexpected entry points. This tactic allowed CL0P to compromise 335 organizations across multiple industries in February 2025 alone.

Additionally, Scattered Spider (aka UNC3944) launched attacks against U.K. retailers using various ransomware variants and is now reportedly targeting U.S. retail organizations. The commerce industry's need for constant uptime and its valuable data make it particularly attractive to attackers. Rapid digitalization and increased reliance on third-party integrations further expand security gaps.

Healthcare

Healthcare organizations are targeted for their valuable data, and stolen patient records fuel secondary attacks like identity theft and fraud. Downtime from attacks jeopardizes patient care, with average ransom payouts of US$860,000 and daily downtime losses of US$1.9 million. In our SOTI report, Healthcare Under the Microscope: Attacks Focus on Applications and APIs, we analyzed how the industry's increasing reliance on web applications and APIs increases their vulnerability to ransomware.

Legacy systems, Internet of Medical Things devices, and limited cybersecurity resources, especially in rural hospitals, expand the attack surface. Strict regulations mean breaches have severe consequences, making healthcare a prime target.

Public sector

The public sector — comprising local, state, and federal governments and government-controlled institutions that provide public services — are lucrative targets for their valuable data, with successful attacks leading to service disruptions, data loss, and high recovery costs. The United States alone has experienced a significant uptick in government-targeted ransomware attacks, resulting in US$1.09 billion in downtime costs between 2018 and December 2024. Ransomware attacks affected 2.3 million records in 2024 — nearly triple the number from 2023. The latest Verizon 2025 Data Breach Investigations Report confirms this trend, noting targeted attacks against both U.S. federal and state governments and EMEA councils.

Despite legislative measures such as bans on ransom payments, attacks continue unabated, with Florida suffering one of the most severe government data breaches through ransomware in 2024. This trend extends globally: Fog ransomware targeted Brazilian ministries in 2024, while Indonesia's national data center fell victim to LockBit 3.0, disrupting essential services across more than 200 government agencies and triggering a ransom demand of US$8 million.

Manufacturing

In Q1 2025, more than 400 manufacturing companies were hit by ransomware, making manufacturing the top target overall during that quarter. This aligns with a surge in attacks on operational technology and industrial control systems. Manufacturers are vulnerable because of legacy systems, connected devices, and complex supply chains, as seen in the BlackSuit attack, which disrupted 15,000 car dealers. Ransomware in this industry leads to operational, financial, and reputational damages. The average recovery costs rose to US$1.7 million in 2024, which further incentivized cybercriminals to target this industry, which is perceived as more likely to pay ransoms.

Education

Educational institutions face unprecedented ransomware attacks, with average demands of US$608,000 and some as high as US$1.5 million. High-profile incidents include breaches at PowerSchool (a provider of cloud-based educational software in North America) and Chicago Public Schools, which exposed sensitive student data. As of writing, the hacker pleaded guilty for launching the attacks against Chicago Public Schools.

Schools are vulnerable because of limited resources, weak security, and lack of cyber awareness. Delayed incident reporting further increases risks, highlighting the need for prompt and transparent communication. Successful ransomware attacks on educational institutions often result in significant data loss, operational disruptions, educational delays — and, in some cases, permanent closure.

Industry trends summary

Although all industries are at risk of a ransomware attack, the severity of the attacks largely depends on an organization's level of preparedness and its ability to withstand and recover from such attacks. Organizations that lack robust cybersecurity measures or dedicated security personnel often experience significant data loss, prolonged operational disruptions, and, in extreme cases, may even be forced to cease operations entirely.

As industries embrace digital transformation, they inadvertently create additional security gaps and expand their attack surfaces. This means there are more entry points for cybercriminals to exploit, making comprehensive security strategies essential. A particularly concerning trend involves attackers targeting third-party vendors and supply chain partners to gain access to organizations that have better defenses. To address these growing risks, organizations must implement advanced strategies like microsegmentation to contain breaches and prevent lateral movement, which can ultimately reduce their exposure to ransomware.

Security spotlight

Cryptominers by Maor Dahan

Cryptominers, like ransomware, primarily seek financial gain through anonymous cryptocurrency transactions. Although ransomware operations typically involve complex network intrusions and direct extortion of victims for immediate payouts, cryptominers operate covertly, generating steady, low-risk income for cybercriminals.

Cryptominers and ransomware are distinct threats that stem from attackers' financial motives. Cryptominers primarily exploit organizations' computing resources to generate profit, whereas ransomware encrypts and/or exfiltrates sensitive data to extort ransom payments. Both types of malware capitalize on cryptocurrency's anonymity: Ransomware groups use it for facilitating ransom payments, and cryptominers use it to directly profit from mining operations.

Both types of attackers may use similar tactics, such as phishing campaigns and exploitation of vulnerabilities, to gain initial access before deploying their final payloads. However, detection strategies differ significantly between these threats. Malicious cryptomining remains stealthy over long periods to maximize returns, while ransomware, though initially covert, ultimately alerts the victims to demand payment after fulfilling its objectives. In this security spotlight, we'll take an in-depth look at cryptominers and the risks they pose to organizations.

What are cryptominers?

Cryptominers, or cryptojackers, are a type of malware that exploits the victim's resources for profit by mining cryptocurrency. In contrast to the usual use of cryptocurrency by attackers as a payment method, cryptominers use the fundamental base of the cryptocurrency, which is the blockchain mining operation, to generate financial gain.

Cryptocurrency was originally designed as a borderless, decentralized way to transfer money and detach from traditional banking systems. Since the first appearance of bitcoin, many other cryptocoins and crypto-based tokens have been created. Every token is based on a theme or set of features that distinguishes it from others.

As attackers seek to profit while ensuring their anonymity, cryptocurrencies are a lucrative option — they allow threat actors to use their crypto funds with minimal risk of identification by law enforcement. The most direct way to achieve financial gain without identification is by mining privacy-oriented cryptocurrencies, which give the attackers immediate profit without revealing themselves to the victim.

Adversary motivation

Threat actors choose to employ cryptominers for two main reasons: profit and privacy.

Motivated by profit

With the exception of state-sponsored threat actors and hacktivists, most cybercriminals are financially motivated. Cryptominers are a simple and direct way to monetize an intrusion without the extra step of translating the attacker's hold on the network into capital via ransomware extortion or by selling sensitive data. This makes cryptomining malware an attractive money generator for threat actors.

Other considerations that attackers take into account include cryptocurrency value and mining share rate. If the attacker generates 1 US cent per year (US$0.1), for instance, it is not worth the risk of being arrested. Therefore, one of the attacker's goals is to find a balance between effort and profit, which lets us narrow down the list of potential coins mined by attackers.

During our research, we identified an attacker who seems to be active since at least June 2018 and was able to generate an average revenue of 300 XMR every year. If we calculate their revenue according to the current Monero value (1 XMR = US$150), we see that they made approximately US$45,000. This is just slightly less than the average revenue of a small business with no employees in the United States in 2024.

Motivated by privacy

Privacy is intrinsic to most cryptocurrencies. They use cryptographic algorithms that preserve privacy and ownership through secret keys paired with corresponding public keys, which serve as wallet addresses. By leveraging this inherent feature of cryptocurrency, along with additional privacy algorithms designed to hide transaction amounts, sender addresses, and receiver addresses, an attacker can almost completely conceal their activities.

As we mentioned, attackers consider several trade-offs when shifting their botnets to mine specific cryptocurrencies. One of these trade-offs concerns the attacker's privacy vs. profit — there could be more profitable coins that offer less privacy. Coin privacy is measured through the anonymity it could provide in three aspects:

1. Communicating with the network; there are coins that rely on privacy network protocols such as Tor or I2P
2. Protecting transaction information, such as wallet addresses and amounts, to prevent tracing and hide account balances
3. Enlisting the cryptocurrency in exchange platforms that support privacy

For example, bitcoin lacks transaction privacy, making users vulnerable to monitoring and increasing the risk of deanonymization. This limitation restricts the range of cryptocurrencies that attackers can exploit. Consequently, adversaries remain motivated only as long as profitable privacy-focused coins are available.

This motivation will likely decline if privacy coins become unprofitable or if the mining process changes, such as shifting to proof of stake, thereby preventing attackers from easily generating profits through resource-intensive methods.

A motivated attacker has to consider how to execute such a cryptominer campaign — and understanding the fundamentals of the mining process is crucial for that consideration.

Cryptominers' impact on the world

Cryptominers have impacted the world since 2013, when a video games company allegedly exploited customers' machines to mine bitcoin. More than 10 years later, the threat has grown to an enormous scale and cryptominers are now a substantial piece of worldwide cybercrime.

Many case studies of cryptominers have been published over the years: from the WannaMine botnet in 2017 to the Migo campaign that targeted Redis to variants of cloud-specific and browser-mining scripts in early 2024. In recent years, Akamai has uncovered a few cryptomining botnets, such as Panchan and NoaBot.

Attack volume

More attackers have shifted their attention to cryptominers over time. Figure 14 shows that 2023 saw a huge spike in global malicious cryptomining activity — and this trend continued in 2024. Despite the explosive growth, there have not been significant changes to cryptominers' behavior. The typical cryptominer in 2024 acted very similarly to its predecessors from 10 years ago; that is, highly noisy, nontargeted attacks that infect cloud resources and domestic computers to mine privacy-oriented coins.

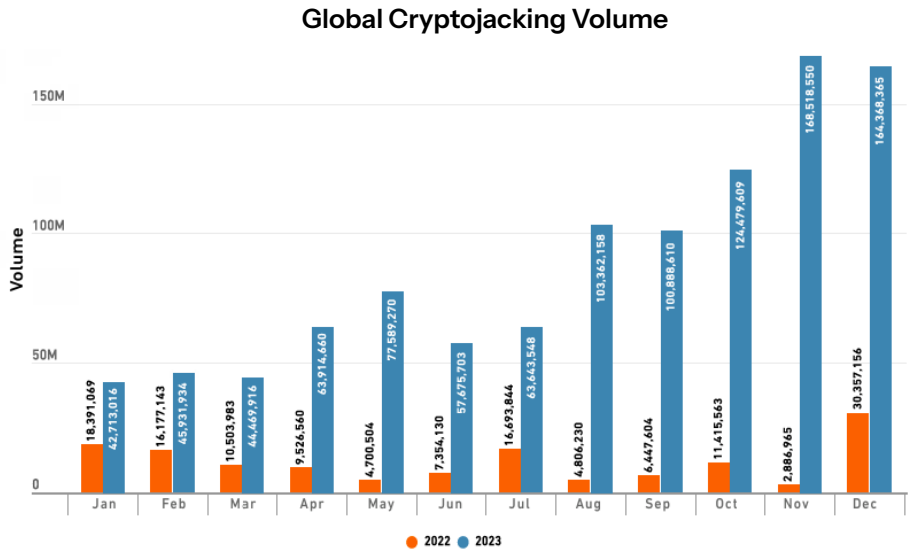

Fig. 14: Volume of cryptominers attacks detected (Source: SonicWall)

Cryptominers' industries and sectors distribution

Cryptominers affect a wide variety of industries and sectors (Figure 15).

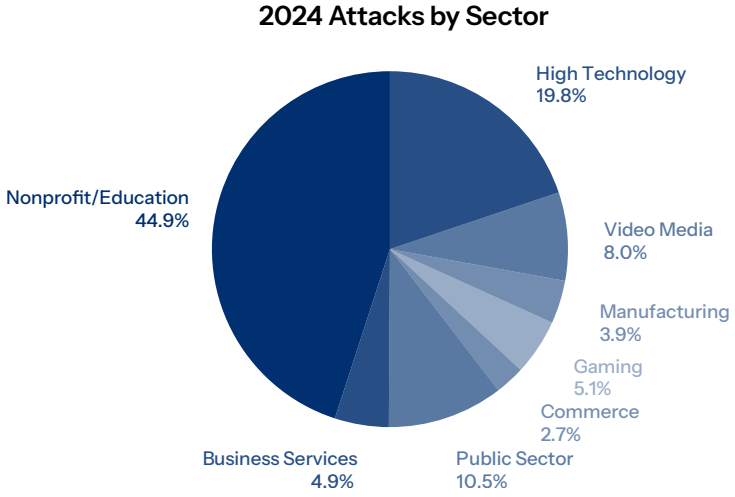

Fig. 15: The distribution of observed attacks across various sectors in 2024

Higher education institutions were among the most targeted sectors, presumably because of their significant computational resources, which are often unattended.

Among large tech companies, cryptominers preferentially target industries like cloud and hosting services. These targets provide a great opportunity to attackers, as they allow them to access extensive computational resources while eliminating by-products in the victim's environment, such as substantial noise, heat, and electricity consumption that could potentially lead to their detection.

This type of attack can be financially devastating for victims — in 2022, Sysdig suggested that for every US$1 of cryptominer profit, the victim loses approximately US$53 (Figure 16).

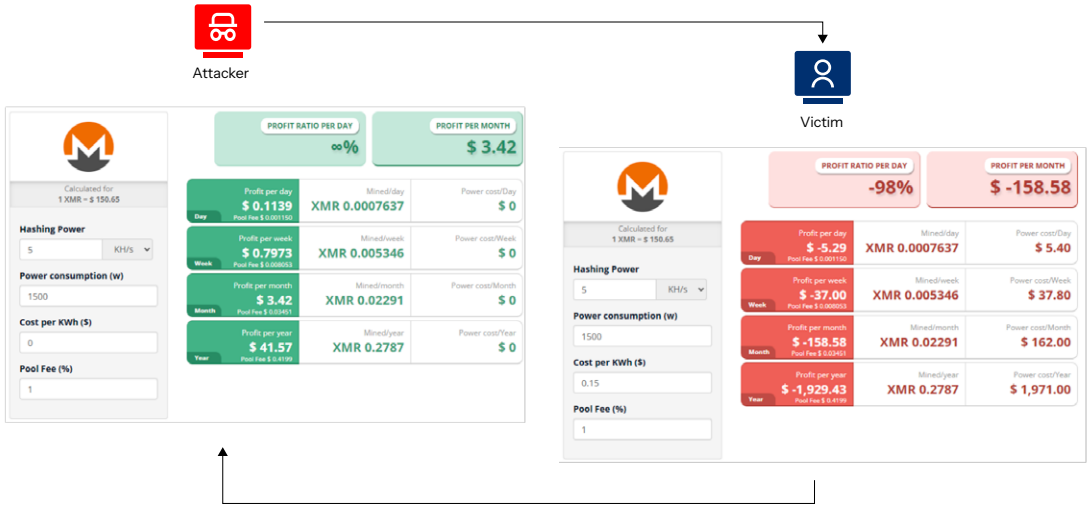

Fig. 16: Attacker profit compared with victim expenses

GenAI offers new attack surfaces for cryptominers

We predict the recent rise of GenAI will significantly affect the cryptominer landscape. As AI computation is highly reliant on graphics processing units (GPUs), those components are becoming more common in organizational networks and servers. Because many mining algorithms are also designed for GPUs, the underlying computing infrastructure of the AI industry is very attractive for cryptominer operators.

It's probably just a matter of time before we witness a campaign that targets AI infrastructures either directly through the model interaction or through the training process — or both.

Cryptocurrency choice for cryptomining attacks

Attackers now have many cryptocurrency options beyond bitcoin, each with unique features. When selecting a coin, cybercriminals consider several key factors:

- Cross-platform compatibility: The coin must be mineable across various architectures (x86, AMD64, ARM, etc.).
- Hardware flexibility: Mining should be possible on standard devices; it should not require specialized hardware like GPUs.
- Privacy features: The cryptocurrency should support untraceable transactions to help hide illegal activities.
- Profitability: The coin should offer high, sustainable returns.

These criteria help attackers maximize their gains while minimizing detection risks.

Mitigating the risk of cryptominers

By leveraging Akamai's security stack, organizations can mitigate the risk of cryptominer infections across multiple layers of the attack surface.

Use Akamai Guardicore Segmentation to prevent lateral movement

Many cryptominers exhibit worm-like behavior — once they compromise a host, they attempt to move laterally across the network to infect as many additional systems as possible. This lateral movement is typically carried out by spraying weak credentials or exploiting known (n-day) vulnerabilities across internal subnets.

By using Akamai Guardicore Segmentation to implement a strict microsegmentation policy, defenders can significantly reduce this risk. By restricting unnecessary internal communications, defenders can effectively block the majority of lateral movement attempts and contain infections before they spread.

Use Akamai Secure Internet Access Enterprise to block mining-related connections

Many cryptomining configurations rely on direct communication with known mining pools (that is, DNS addresses used by all nodes in the mining network during the different mining operations).

Since cryptomining typically has no legitimate use case in most corporate environments, identifying and blocking connections to these domains can be a highly effective way to disrupt mining malware. Akamai Secure Internet Access Enterprise helps protect against this threat by blocking access to known mining pool addresses by default.

Use Akamai Hunt to proactively identify malicious cryptominers

Not all cryptomining malware can be reliably detected using static indicators of compromise, such as file hashes or known DNS addresses. To identify previously unknown or evasive samples, Akamai Hunt employs a proactive set of behavior-based detection techniques.

These techniques focus on identifying anomalous behaviors that are commonly associated with cryptominers, such as suspicious communication patterns, unusual process execution, and persistence mechanisms. When such anomalies are detected, the associated processes are further analyzed to confirm malicious activity.

Spotlight summary

The use of cryptocurrency in cybercrime operations is not limited to collecting ransomware payments. Cryptominer malware exploits the fundamental aspect of cryptocurrency — its mining process — as a primary means of generating profit. Cryptomining is effective, simple, and very stealthy, and it provides a great opportunity for less sophisticated threat actors to monetize their intrusions.

The impact of ransomware attacks on operational continuity

Ransomware poses a significant threat to operations, extending far beyond immediate ransom payments. The true financial and operational impacts include prolonged downtime, productivity and revenue losses, and extensive postincident recovery and mitigation efforts. These ramifications can persist for weeks or even months, depending on the organization's cybersecurity posture, incident response capabilities, and security controls.

The average reported downtime following a ransomware incident is 21 days, which can lead to severe consequences such as reputational harm, diminished customer trust, permanent closure — and, particularly in critical industries like healthcare and manufacturing, patient safety risks and supply chain disruptions.

It's also not just the attack on the initial target that can cause impacts; there can be a ripple effect. Ransomware actors may target supply chains, including commercial software deployed internally and external service providers, which are often considered to be "softer targets" because of their lower cybersecurity maturity. For example, in April 2025, attackers gained access to customer data at two large banks by actively targeting external partners.

Potential costs beyond ransom demands

Ransom payments represent only a fraction of the total cost of a ransomware attack. Cybersecurity Ventures predicts that by 2031, ransomware damages will reach US$276 billion annually (or US$525,000 per minute), up from US$57 billion per year (or US$109,000 per minute) in 2025. Additionally, long-term impacts include loss of customer loyalty and damage to brand reputation. Organizations may also face regulatory sanctions and penalties for breaches of data protection laws such as GDPR or HIPAA, further compounding financial and reputational harm.

Ransomware often causes partial or complete shutdowns of business-critical functions, effectively crippling operations. As attackers increasingly employ multi-extortion tactics to encrypt and exfiltrate sensitive data, such as intellectual property and customer information, the risk of permanent data loss remains high. Even if a ransom is paid, there is no guarantee that companies will recover all their data.

Additionally, recovery costs from ransomware attacks in 2024 had a sharp increase — with the average expense reaching US$2.73 million, up from the US$1.82 million reported in 2023. This figure excludes any ransoms that attackers collected.

Addressing the increasing frequency and severity of ransomware attacks

A report from Cybersecurity Ventures projects that by 2031, consumers and businesses will face a combined 43,200 ransomware attacks per day, or one every two seconds. To minimize the impact of this threat, organizations must:

- Develop a comprehensive business continuity plan to maintain mission-critical functions during and after an attack, reducing downtime and financial loss
- Perform regular data backups
- Implement network segmentation to limit the spread of ransomware within the environment if an attack is successful
- Ensure rapid response to significantly reduce the scope and duration of an attack

For more details on how to protect the network and critical assets, refer to our Mitigation section.

Security spotlight

Ransomware and the law by James A. Casey

We often hear answers like “Because I can, Mr. Bond” when villains in the James Bond films are asked why they commit crimes. This bit of dialog exemplifies the classic Bond villain’s blend of menace and sophistication. This description applies equally to ransomware criminals — they engage in ransomware attacks because they can, and because they are effective. As ransomware has emerged as one of the most significant cybersecurity threats facing organizations worldwide, governments have scrambled to address this growing menace through various laws, regulations, programs, and awareness campaigns.

Current state of the law

Many of the legal efforts, however, are not specifically aimed at ransomware, but rather are just an application of broader spectrum cybersecurity laws. Ransomware, despite its prevalence and effectiveness, is just another cyberattack in the bad guys’ arsenals. The same legal principles apply to ransomware incidents as to other cyberattacks, and much of the same cyber hygiene and security best practices will help to mitigate the risk.

In the United States, for example, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) offer cyber prevention and response frameworks; the Computer Fraud and Abuse Act (CFAA) continues to serve as the foundation for prosecuting cyberattacks, including ransomware; and various federal and state cyber incident reporting rules apply to all cyber events.

The European Union has various cyber laws, including the robust legal framework created by the NIS2 Directive which establishes strict reporting guidelines, significant penalties, and executive accountability, and is broadly applied across industry sectors. To the extent that a ransomware attack involves personal information, privacy laws in many jurisdictions will apply to create additional requirements and reporting obligations.

In addition to legislative and regulatory activity, nations have participated in cooperative arrangements to try and address the threat. All 50 members of the International Counter Ransomware Initiative (ICRI), for example, endorsed a joint policy statement asserting “relevant institutions under our national government authority should not pay ransomware extortion demands.” And the Oxford Statement on Ransomware Operations establishes principles for applying international law to ransomware. Although these efforts do not create any binding obligations and are not applicable to the private sector, they demonstrate the significant attention being paid to the ransomware threat at all levels.

Ransom payment restrictions

Ransomware does raise one unique issue that specific legal efforts attempt to address — extortion. A successful ransomware attack necessarily raises the question, "Should we pay the ransom?" The answer to that question will depend on many different factors, including the impact to the business; the size of the ransom and the nature of the extortion (i.e., single, double, triple, or even quadruple extortion); the identity, if known, of the attacker; and the likelihood that paying will actually result in release of the data or a standing down on other threats.

While these factors may motivate the business to pay, the position of most governments is that victims should not pay. Outright legal bans are rare and mostly limited to government/public sector entities and critical industry sectors in a few countries. Virtually all countries' governments, however, recommend against payment. Reasons for this position are obvious — if ransoms are not paid, then the effectiveness of the attack vector is reduced and potentially becomes less attractive to hacker groups. In addition, payment of ransoms potentially funds other criminal activities, both financial and ideological, increasing the risk to everyone. Finally, there is no guarantee that paying a given ransom or related extortion demand will result in the release of data or termination of the related threats (data disclosure/sale, DDoS attacks, customer notifications).

In fact, the number of organizations that refused to respond to ransom demands increased from 50% in 2022 to 64% in 2024. Consequently, ransom demands have become significantly lower, which may also be due in part to government intervention; that is, the success of takedowns and seizures of infrastructure by law enforcement.

The 3 categories of legal efforts to discourage ransom payments

The legal means employed by governments to discourage payments fall into three basic categories. The first, and most common category, is legal restriction on payments to sanctioned or restricted entities and nations, as well as more general restriction on payments to criminal enterprises. The United States and other allied regimes make it illegal to pay any ransomware actors in comprehensively sanctioned countries (e.g., North Korea, Iran, Syria, and Cuba) or who are on applicable entity lists such as the U.S. Office of Foreign Assets Control list of Specially Designated Nationals. Indeed, nearly every country with sanctions laws or anti–money laundering statutes makes it illegal to pay ransoms to sanctioned entities or criminal organizations. This is not unique, of course, to ransomware — these laws apply to any transaction with sanctioned parties, including terrorist groups, organized criminals, and state-sanctioned cyber actors.

The second category of legal efforts focuses on reporting obligations. Cyber incident reporting is ubiquitous across jurisdictions globally and would generally apply to ransomware attacks. More specific obligations related to ransomware payments, however, are starting to be enacted. Effective May 30, 2025, the Australian Cyber Security Act, for example, introduced mandatory reporting for ransomware payments. The United Kingdom is considering mandatory reporting for payments by public sector entities and critical infrastructure. And in the United States, the CIRCIA will require covered entities to report ransomware payments within 24 hours (rules pending finalization). We can expect to see more of these kinds of ransomware specific requirements in the future.

The third category is specific ban legislation. The proposed U.K. cyber security act would potentially ban payments by public sector and critical infrastructure entities. We can expect to see other more comprehensive bans or, at least, sectoral bans for important industries, including financial, healthcare, and critical infrastructure sectors.

Looking ahead

Despite regional differences, there are a number of common elements that emerge in ransomware regulations and cyber best practices.

- Incident reporting: Most jurisdictions require prompt reporting of significant cyber incidents, including ransomware.
- Risk management: Governments continue to focus on requirements to ensure that organizations implement appropriate cybersecurity measures.
- Supply chain security: There is an increasing focus on securing third-party relationships and the supply chain overall.
- Executive accountability: We are seeing a growing trend of holding management responsible for cybersecurity.

Ransomware-specific regulations, guidelines, and requirements likely will continue to evolve as threats become more sophisticated.

- Emerging ransomware tactics using artificial intelligence will drive regulatory updates.
- New legislation and legal enforcement efforts will focus on RaaS models.
- Increased penalties and victim support mechanisms are being considered globally.
- International cooperation will continue to combat cross-border threats.

As ransomware continues to pose a significant threat to organizations worldwide, staying informed about these evolving international regulations and enforcement efforts will be essential for maintaining compliance and enhancing cybersecurity posture.

Building ransomware resilience around the world

Cyber insurance and multilayered security are interlocking building blocks for cyber resilience. This is particularly true in the case of a ransomware attack in which the goal is encryption of as much of the network as possible. Once this happens, the financial implications of an attack — downtime, remediation, and potential legal fees and regulatory fines — may include paying a ransom.

Since 2022, the FBI's IC3 has offered up thousands of decryption keys to victims of ransomware, helping them to avoid more than US$800 million in payments. However, decryption keys aren't always available, so organizations need their own strategies to build resilience.

Navigating payment and cyber insurance decisions

Before an incident, organizations should have ransomware payment policies in place. Paying a ransom is no guarantee that you will recover everything, but you may be able to recover the majority of the systems that were impacted.

Organizations also need to support cryptocurrency payments. Engaging with organized criminals who have the will and the means to put an organization out of business is a high-pressure situation, so organizations should establish a relationship with a third party who specializes in negotiating with cybercriminals. Seasoned negotiators aim to minimize the financial damage and help the company resume operations, but victims should still expect to pay 50% to 80% of the original demand.

S&P Global Ratings has projected that annual cyber insurance premiums will reach approximately US$23 billion by the end of 2026, up from an estimated US$14 billion at the close of 2023, with an increase of 15% to 20% per year. Currently, North America accounts for approximately 51% of gross premiums written on cyber insurance, EMEA about 38%, APAC 9%, and LATAM 3%. The fastest growth rates are anticipated in APAC and LATAM, where cyber insurance markets are smaller and less mature than in the United States and Europe.

In 2024, insurance claims were higher for ransomware attacks than for other types of incidents, and made up about 21% of claims — although the average claim size and frequency have been declining over the last two years. Approximately 44% of policyholders who fell victim to ransomware decided to pay ransom "when deemed reasonable and necessary," with the insurer negotiating ransomware payments down by an average of 60% in these cases.

The most common ransomware group identified in ransomware insurance cases was Akira, accounting for 13.4% of events, followed by Play (6.2%), Medusa (5.7%), and RansomHub (4.6%). Black Basta had the highest average ransom demand at US$4 million but accounted for only 3% of claims.

Trustworthiness is not a two-way street

An interesting dynamic is that, in some cases, cyber insurance incentivizes criminals because criminal groups can demand the amount that insurance will cover for the key to decrypt the data. On the other hand, the involvement of insurance company negotiators, or negotiators they sanction, likely increases the probability that the encryption keys work, and complete recovery is more assured.

Although this is a business transaction and cybercriminals don't want to bite the hand that feeds them, they also don't play by the rules. Trustworthiness is not a two-way street. Despite having their demands met, cybercriminals may not delete stolen data, as in the case of LockBit. And when data is encrypted, 35% of companies either don't receive the decryption keys they paid for or the keys don't work. Even with working keys, the recovery process is painstaking and requires expertise. Plus, there's still the risk of being targeted again by the same or affiliated threat actors.

Organizations that have decided not to pay often fall back on their business continuity/disaster recovery crisis management plan. This approach can take days to weeks, depending on what kinds of investments have been made to facilitate a recovery and how often the plans are tested and updated.

Driving stronger regional security programs

The increase in the number of ransomware attacks, the emerging sophistication of AI-driven attacks, and growing legislation have all combined to force cyber insurance companies to raise rates and increase auditing of the company's cybersecurity capabilities. This has driven a compliance mindset to ensure that companies can get the best rates, which can result in loss of coverage if the insurance plan was based on security control that was not implemented and allowed the ransomware to execute.

Exclusions and limitations can also result in loss of coverage. If the company is attacked by hacktivists that are supporting a geoconflict, the attack could be considered a nation-state attack and not covered under an act-of-war exception. Finally, companies need to ensure that they understand the insurance agreement; in some cases, any actions taken before the insurance company is notified will not be covered.

While many companies depend on insurance to mitigate the risk of major cyber events, including covering the cost of decryption keys, no companies rely on it to the exclusion of security programs. In fact, many insurance companies only cover the company if they have deployed a baseline set of controls, with the cost of insurance decreasing as the company can demonstrate more security controls. This effectively incentivizes companies to strengthen security programs.

To this end, organizations around the world are building resilience to ransomware attacks by implementing Zero Trust solutions to control access and by using microsegmentation for detailed visibility and controls to detect, prevent, and contain lateral movement. Regional use cases include:

- Zero Trust enforcement is simplified in APAC
- Rapid time to policy thwarts an attack in LATAM
- Microsegmentation provides resiliency in EMEA
- Smart policies outsmart ransomware in North America

Zero Trust enforcement is simplified in APAC

A think tank and consulting services provider needed an easier way to deploy and manage Zero Trust access control mechanisms to enhance security for its own network and its critical infrastructure clients. As threat actors increasingly adopt GenAI to lower the barriers to entry, greater visibility into and control over devices lent to employees or outsourced companies would help to protect against data leakage and the spread of malware across the network.

Software-based microsegmentation provided network visualization and granular access control to enforce Zero Trust principles for employees of the consulting services provider and for its third-party associates. A proof of concept validated that the firm can stop unwanted behavior, such as lateral movement that ransomware relies on, and reduce the internal attack surface.

Microsegmentation provides resiliency in EMEA

An international brand needed to enhance its cybersecurity posture to guard against internal threats. The few network firewalls in place were not able to prevent lateral movement across the network and provide visibility into communication paths and potential security risks.

Deploying privileged access and granular segmentation helped them achieve Zero Trust by restricting unsanctioned remote access and more effectively defining user-based segmentation. To test resiliency, they deployed a ransomware breach test and were able to identify and isolate the rogue machine in record time to prevent the breach from spreading.

Rapid time to policy thwarts an attack in LATAM

Shortly after transitioning to a work-from-home model, a successful ransomware attack hit a critical database at a large bank. The security and IT teams needed to act fast to limit the loss of sensitive financial data. They had to determine and secure the initial attack vector and prevent ransomware from spreading laterally to backup servers and the production environment.

Software-based segmentation had already been deployed in other parts of the bank. So, the teams were able to move quickly. In only three days, they were able to gain the process-level visibility necessary to identify the attack vector and put enforceable policies in place. The teams blocked ransomware from propagating further and improved remote access security moving forward.

Smart policies outsmart ransomware in North America

A healthcare company faced growing ransomware threats and needed visibility far beyond traditional firewalls to isolate and eliminate threats faster and maintain application availability even during security incidents.

Microsegmentation made it possible to better ringfence apps and implement ransomware prevention policies quickly while providing cost savings over other approaches. The company's IT team neutralized 4,000 cyberattacks on day one and gained unexpected benefits, including faster network troubleshooting, incident investigation, and policy creation and enforcement.

Mitigation

A robust defense against ransomware involves a multilayered approach, a strong commitment to safeguarding data at the edge, and the use of segmentation to stop attacks from spreading laterally so that threat actors do not reach internal resources. Also, extensive visibility is essential for identifying threats. Advanced, up-to-date technologies may assist with these needs and are also vital for defending against the increasingly sophisticated AI-powered tools employed by cybercriminals. Recommended mitigation strategies to help protect organizations against ransomware attacks, include:

- **Implement a Zero Trust architecture** that includes segmentation of critical assets and a secure application gateway with cloud-based Zero Trust Network Access to secure north-south and east-west communications. Strict access controls limit threats that bypass edge defenses (which aligns with NIST Zero Trust Architecture), reduce the lateral movement of ransomware within the enterprise, help detect and prevent data exfiltration, and can greatly decrease ransomware response time for organizations following best practices.
- **Counter AI-enhanced attacks**, and match the speed and adaptability of AI-driven attackers, by deploying AI-powered threat detection that enables real-time automated responses and accelerated incident responses to new and evolving ransomware tactics.
- **Provide comprehensive edge protection** that includes a defense against JavaScript, web application, and API attacks, addresses the increasing threat of zero-day and day-one vulnerabilities, and ensures tight security for all public-facing systems.
- **Achieve awareness** across multiple environments with accelerated threat detection that minimizes dwell time; adopt capabilities that provide rapid visibility and mitigation; shift from pure prevention to strategies that detect insider threats and threats that have bypassed defenses; and consider partnering with security enhancement providers or threat hunting teams to strengthen internal capabilities.
- **Use the MITRE ATT&CK framework** to map security controls to attacker tactics and to identify where known threat actors (e.g., DragonForce, CL0P) can be defeated. The framework can also assist in visualizing how to deploy resources for protection.
- **Combat social engineering and deepfake threats** by establishing strong verification protocols — such as phish-proof multi-factor authentication and other multistep approval processes for sensitive transactions or access requests — to prevent single points of failure. Educate staff on deepfake risks.

- **Safeguard outbound traffic** from connecting to infected websites by using solutions with URL inspection to detect and block phishing attempts and by employing endpoint detection that provides alerts on malicious activity from phishing emails or payloads.
- **Incorporate compliance by design** by ensuring that security controls and data protection measures are integrated throughout the lifecycle of products and services, including for north-south and east-west traffic.
- **Boost resilience** and proper risk management by having comprehensive business continuity and disaster recovery plans and cyber insurance to provide financial support for managing losses, recovery costs, and operational stability during and after a ransomware attack.
- **Strengthen and test backup defenses continuously** and keep them physically or logically separated from the main network to prevent alteration or deletion.
- **Manage vulnerabilities** and catch them before attackers do by scanning and using tools and processes that prioritize systems exposed to the internet or that contain sensitive data. Focus on fixing the most critical issues quickly instead of everything at once.

Conclusion

The ransomware criminal economy remains dynamic and rapidly changing, with a confluence of factors accelerating this pace, including hacktivism, widespread cryptocurrency adoption, the RaaS business model, GenAI and LLMs, expanding compliance requirements and legislation, and law enforcement actions. As these threats proliferate, organizations must redefine cyber resilience and implement practical frameworks to achieve comprehensive protection.

In the past, resilience simply meant maintaining data backups. Today, many organizations may feel compelled to pay a ransom to avoid facing the ramifications of successful attacks, even though the governments of most countries encourage them not to do so.

Ultimately, adopting an “assume compromise” mindset can aid defenders to be on the lookout for indicators of compromise, and to respond before an attack attempt turns into a successful intrusion. By deploying purple teams that blend offensive and defensive tactics, defenders can more effectively counter sophisticated ransomware threats. This approach not only improves incident detection and response, but also strengthens overall resilience against persistent, adaptive adversaries.

Methodology

The Akamai ransomware data in this report was collected from our Secure Internet Access Enterprise customers, who provide us with data from billions of events monthly. We actively monitor a range of activities, including indicators of compromise, TTPs, and weaponization efforts from more than 100 ransomware groups.

This report focused on the events reported by customers and the detections made within their environments. In this context, we classify an "event" as any communication attempt to an IP or domain associated with a threat, regardless of its outcome. Our detection mechanisms categorize each event based on confidence and severity levels, which aids in assessing the certainty of an activity's malicious intent and its potential impact.

The data in this report includes the 17-month period from January 1, 2024, through May 31, 2025. (Note: We experienced a data outage in April 2025 resulting in missing data during this month.)

Guest contributors

Or Zuckerman
Senior Security Researcher Lead, Akamai

Or Zuckerman is Senior Security Researcher Lead at Akamai, working in various security fields, including incident response, forensic research, and detection method development.

Maor Dahan
Senior Security Researcher, Akamai

Maor Dahan is a Senior Security Researcher at Akamai with more than a decade of experience in the cybersecurity industry. Maor specializes in operating system internals, vulnerability research, and malware analysis, and designed and developed advanced detection and prevention mechanisms for innovative security products like EDR, EPP, and virtualized-based security.

James A. Casey
Vice President, Chief Privacy Officer, Akamai

James A. Casey is Vice President and Chief Privacy Officer at Akamai and heads the Akamai Global Data Protection team. Jim has served as in-house counsel for technology companies for the past 20+ years and has significant experience supporting new technology and product initiatives in the internet, cybersecurity, information services and analytics, and telecommunications industries. Jim provides legal counsel in a variety of areas, including technology law and regulation, public policy, privacy and artificial intelligence governance, import/export and trade compliance, and cybersecurity. Prior to moving in-house, Jim's law firm experience focused on supporting of technology regulation and initiatives in the data, telecommunications, and internet industries, both domestically and internationally, as well as supporting technology and telecommunications projects with native peoples in the United States and around the world.

Credits

Research director

Kimberly Gomez

Editorial and writing

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Review and subject matter contribution

Tanya Belousov
James Casey
Maor Dahan
Ori David
Reuben Koh
Richard Meeus
Steve Winterfeld
Or Zuckerman

Data analysis

Moshe Cohen
Chelsea Tuttle

Promotional materials

Barney Beal
Ashley Linares

Marketing and publishing

Georgina Morales Hampe
Emily Spinks

State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. akamai.com/soti

Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-research

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

Akamai security research

Read the Akamai security research blog for a rapid response perspective on today's most important research. akamai.com/blog/security-research