ThreatLabz 2025
Ransomware Report

Table of Contents

Executive Summary_

Ransomware has long been a constant in the threat landscape—but how it operates is constantly changing. Today's campaigns are more targeted, automated, and efficient, driven in part by the growing use of generative AI enhancing and accelerating everything from phishing lures to malware development. This evolution has translated into a significant surge in ransomware activity and impact.

From April 2024 to April 2025, the Zscaler cloud blocked more ransomware attempts than in any previous year—more than 10.8 million hits—marking a 145.9% year-over-year increase and the highest volume recorded since tracking began. At the same time, the number of organizations listed on ransomware leak sites rose 70.1%, underscoring a broader shift to extortion-driven attacks. Today's campaigns are high-frequency and high-impact, designed to extract maximum leverage, often without the need for encryption. A growing number of ransomware operators are abandoning encryption altogether in favor of pure data extortion—an evolution mirrored by a 92.7% rise in data exfiltration volumes over the past year.

Even amid high-profile takedown initiatives like Operation Endgame, ransomware groups show no signs of slowing down. If anything, disruption may be driving reinvention. Thirty-four new ransomware families emerged during the analysis period for this report. Meanwhile, established groups such as DragonForce, Akira, and Clop climbed to the top of the activity charts, demonstrating the resilience of mature ransomware operations.

The Zscaler ThreatLabz 2025 Ransomware Report dives deeper into these developments and findings, covering top targeted sectors and regions, ransomware families to watch, evolving attack methodologies, and actionable guidance for defenders. Beyond threat tracking, learn how ThreatLabz plays an active role in protecting enterprises worldwide—from building custom tools for ransomware attack recovery to contributing to global efforts that expose and disrupt large-scale malware and ransomware ecosystems.

Key_ Findings

Ransomware attempts blocked by the Zscaler cloud increased by 145.9% year-over-year (April 2024—April 2025), marking the most significant spike we've seen in three years.

Data exfiltration volumes for 10 major ransomware families increased 92.7% year-over-year to 238.5 terabytes (TB) stolen, signaling the broader shift toward data theft as a primary extortion tactic.

Public extortion cases jumped by 70.1% based on data leak site analysis, proving the threat of reputational damage or regulatory consequences is often more compelling than encryption alone.

Manufacturing, Technology, and Healthcare were the top targeted industries, and the Oil & Gas sector experienced a 935.3% increase in attacks.

The United States remains the #1 global target, experiencing 50.8% of overall attacks, followed by Canada, the United Kingdom, Germany, and India.

Generative AI is becoming a force multiplier for ransomware threat actors, helping to rapidly create phishing lures, write malicious code, automate data extraction, and more.

RansomHub (833), Akira (520), and Clop (488) emerged as the most active ransomware families, collectively responsible for the largest share of attacks.

Vishing (voice-based phishing) is increasingly integrated into ransomware attacks as voice scams become more convincing and more effective at gaining initial access.

ThreatLabz identified 34 newly active ransomware families during the analysis period, bringing the total number tracked to 425 since our research began.

Despite rising ransomware activity, coordinated law enforcement efforts—supported by industry experts like Zscaler ThreatLabz—have made meaningful strides in disrupting major ransomware infrastructure, as demonstrated by Operation Endgame.

Ransomware_Landscape: Top Trends and Targets

While headline-making breaches illustrate the global scale of ransomware, the most valuable insights come from analyzing targeting patterns and operational behaviors threat actors use across campaigns.

This section goes beyond headlines to examine where ransomware is having the most significant impact (by industry and region), identify which ransomware families are leading the charge, and spotlight the emergence of new groups over the past year.

Ransomware attacks hit new highs

Steady growth in ransomware activity is no longer surprising, but the latest data shows a dramatic surge in attack volume: attempted ransomware attacks in the Zscaler cloud have jumped 145.9% year-over-year—and sixfold since 2021. This figure reflects the volume of ransomware-related indicators and events the platform blocked. The uptick reveals more than just higher volume; it signals a shift toward faster, more deliberate campaigns targeting high-impact environments.

For security teams, ransomware tactics may be largely familiar, but the rising pervasiveness, precision, and operational efficiency of recent campaigns point to an evolution—one fueled in part by GenAI accelerating ransomware's development into a more sophisticated and scalable cybercriminal business model.

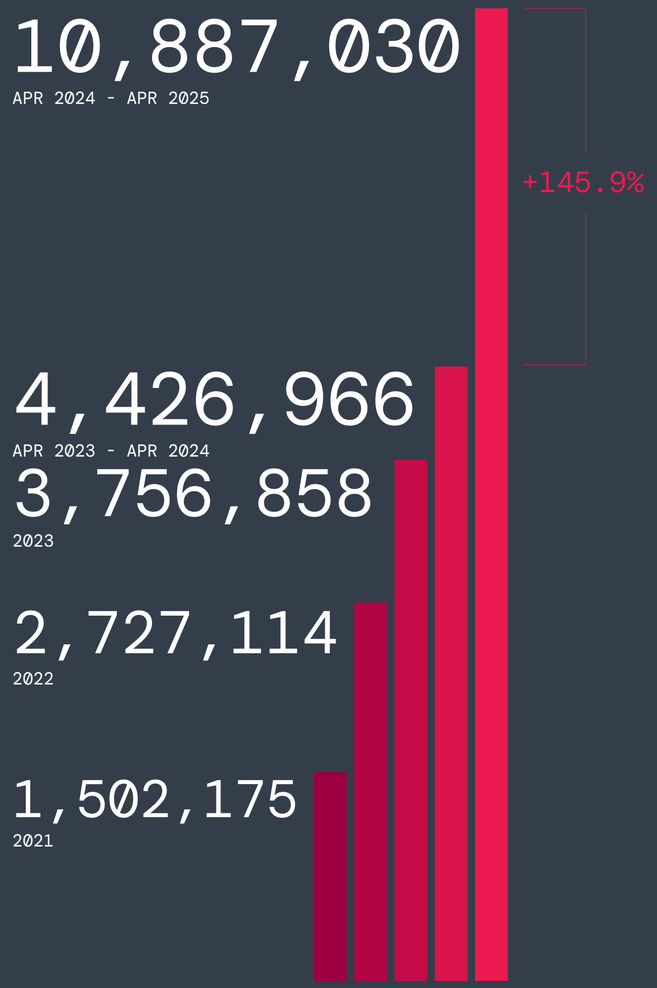


Figure 1: Ransomware attack indicators (events) blocked by Zscaler annually

Data exfiltration trends up 92.7%

Over the last year, ransomware groups have turned data theft from a supporting act into the main event. Increasingly, encryption alone—if at all—isn't the endgame. Threat actors are exfiltrating massive amounts of data to amplify pressure and raise the stakes for victims.

A recent uptick in data exfiltration reflects this trend. ThreatLabz analysis reveals that the total volume of data stolen increased year-over-year across 10 major ransomware groups. The total volume of exfiltrated data by these groups rose 92.7%, from 123.8 TB (April 2023—March 2024) to 238.5 TB (April 2024—March 2025). This excludes a single breach in the 2023—2024 period involving 100 TB of exfiltrated data—the largest exfiltration observed across the entire dataset—which heavily skews the annual total. Removing that outlier provided a more accurate view of broader trends in data theft activity.

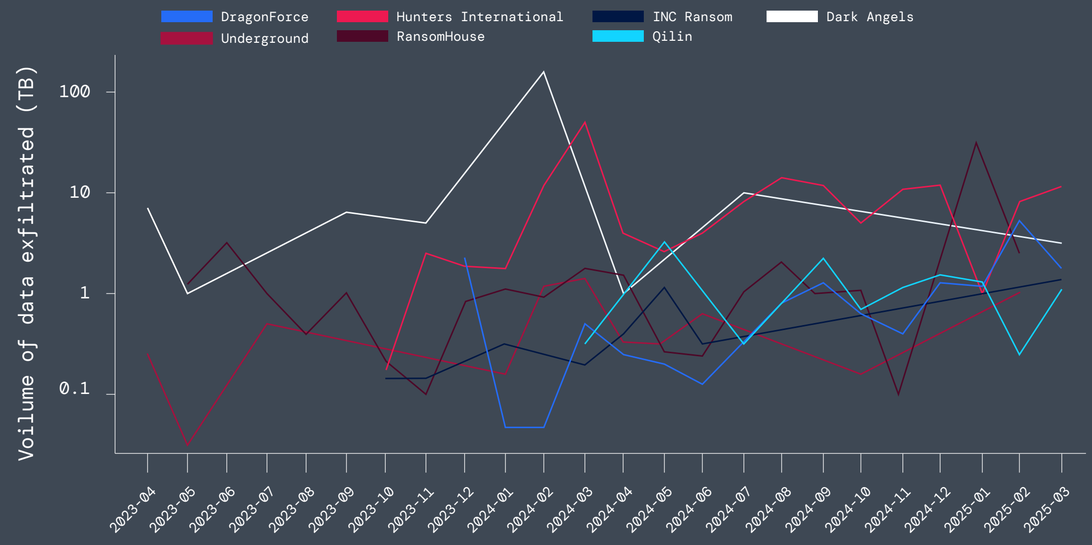


Figure 2: Data exfiltration by key ransomware groups

- **Hunters International** significantly increased its total data stolen year-over-year, up 224.3% from 37.7 TB to 122.1 TB. The median data loss per victim also rose from approximately 300 GB to 359 GB year-over-year, a 19.6% increase per victim. The next section ("Shifting to data extortion only") explores how the group decided to move entirely away from file encryption.
- **DragonForce** made the highest percentage jump in total exfiltration volume, up 382.6% from 4.2 TB to 20.3 TB. Although the median remained mostly stable with a slight decline, the increase in overall volume suggests the group has been compromising more victims.
- **Dark Angels** had the highest median impact per victim: a 132.6% increase from 2.15 TB to 5 TB. This tracks with the group's continued focus on large, high-value targets despite fewer overall incidents.
- **RansomHub** exfiltrated 86.2% more data year-over-year, with 22.4 TB total from April 2024 to March 2025. The group's median data loss per victim more than doubled from 50 GB to 118 GB.
- **RansomHouse** increased its total stolen volume by 83.1% year-over-year, from 17.2 TB to 31.6 TB. Its median data loss per victim also increased from 425 GB to 500 GB.

Shifting to data extortion only

The Zscaler ThreatLabz 2024 Ransomware Report examined how the Hive ransomware group rebranded as Hunters International in October 2023, following an FBI–led operation that seized the group's infrastructure earlier that year. Since the emergence of Hunters International, the group has been very active and heavily focused on data theft over encryption. In fact, from the group's inception, they have stolen nearly 160 TB of data. Each Hunters International victim lost an average of 698 GB, and the median data loss was 317 GB. Figure 3 shows the volumes of data stolen per month since the group's formation.

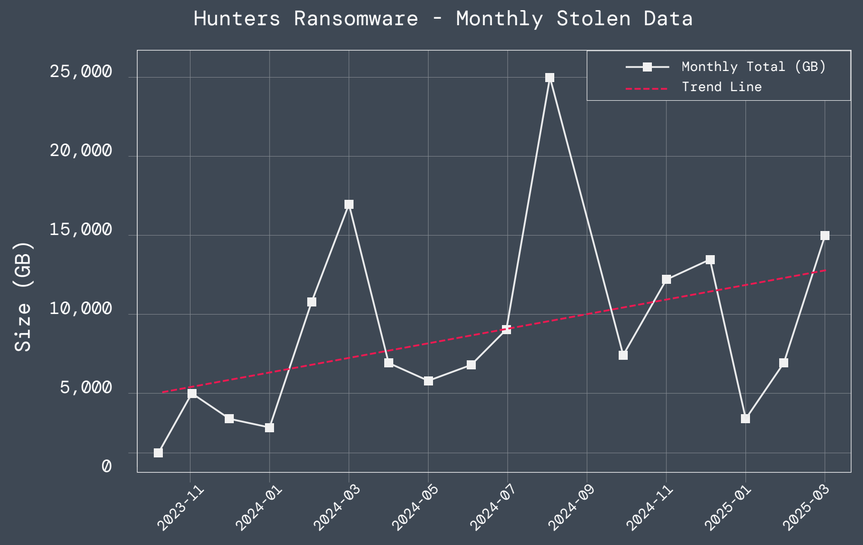


Figure 3: GB of data stolen per month by Hunters International

In May 2025, a new group surfaced under the brand World Leaks, launching attacks without deploying ransomware—choosing instead to focus exclusively on data extortion. The World Leaks site is visually and programmatically similar to Hunters International (see figure 4), indicating that the same group is likely behind both.

Since World Leaks started attacks in May 2025, the group has stolen more than 25 TB of data. The data theft statistics are very similar to Hunters International with each victim losing 769 GB on average with a median loss of 452 GB.

Incidentally, on July 3, 2025, Hunters International announced its shutdown via a message on its leak site, claiming the group was closing operations and providing free decryption tools (see figure 5).

This pivot from file encryption to data theft is not unprecedented. Other groups like BianLian and Clop have also shifted away from ransomware in favor of data extortion, a trend we explore in more detail later in this report.

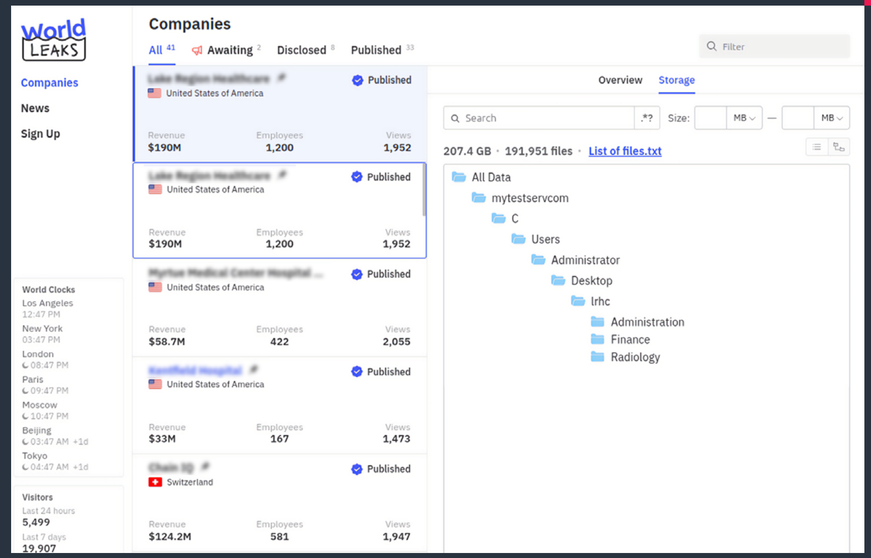


Figure 4: World Leaks ransomware group website

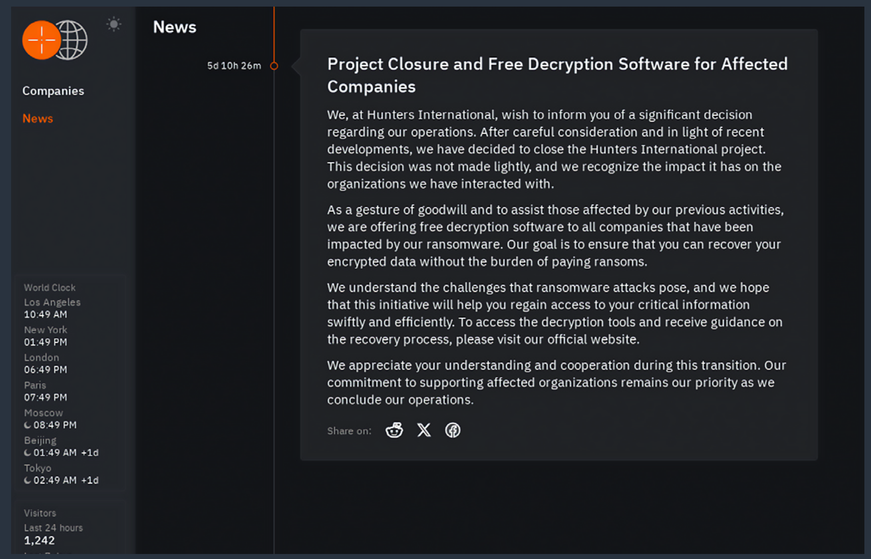


Figure 5: Hunters International shutdown notice

Industries facing the most attacks

Attackers continued to prioritize industries where the pressure to pay is highest—whether due to potential for operational disruption, the sensitivity of stolen data and the related potential for reputation damage, or regulatory exposure.

Figure 6 shows the number of ransomware incidents per industry based on leak site data, offering a snapshot of confirmed attacks where threat actors exfiltrated data and applied extortion pressure. Manufacturing, Technology, and Healthcare remained the most frequently targeted sectors, representing high-stakes environments ripe for extortion and leverage.

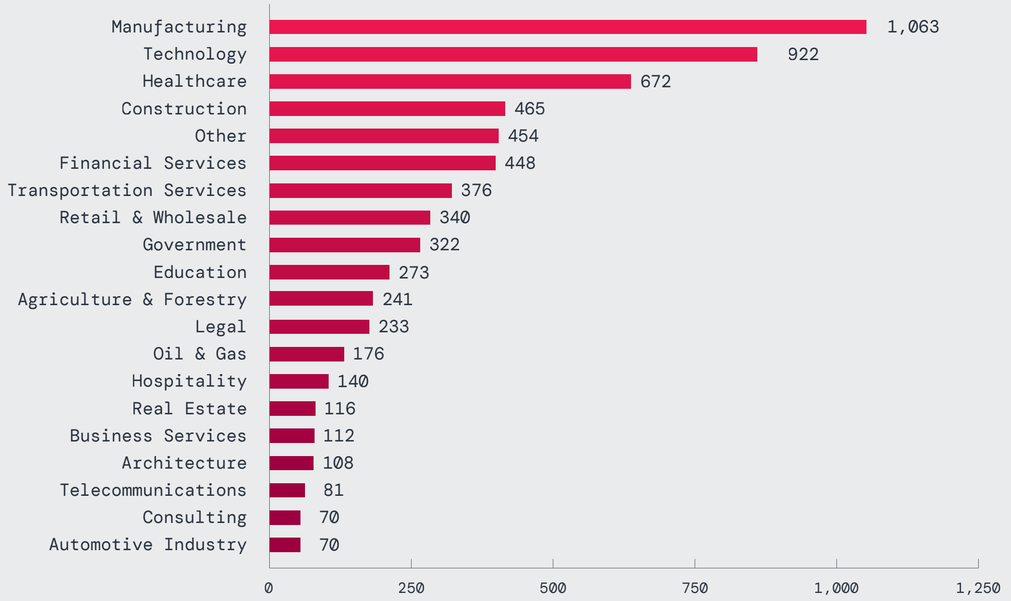


Figure 6: Ransomware attacks by industry based on data leak sites (top 20 industries)

Year-over-year trends

Figure 7 shows year-over-year percentage changes in ransomware attacks by industry.

Ransomware attacks on the Oil & Gas sector have spiked more than 900% year-over-year, likely driven by a combination of increased automation—from drilling rigs to pipelines—inflating the attack surface and outdated security practices. In 2025, the Cybersecurity and Infrastructure Security Agency (CISA) warned[1] that even "unsophisticated" threat actors are exploiting vulnerabilities in industrial control systems (ICS) and SCADA technology, which are essential for operations in oil and gas.

The Agriculture sector also saw ransomware attacks skyrocket by 677.4%. Farming operations are becoming more and more digitized (think smart tractors and IoT-enabled sensors), yet security defenses haven't kept pace. Still, there are signs of progress and recognition that farming systems are now prime ransomware targets: John Deere, a major manufacturer of agriculture machinery, hosted a 2025 hackathon where students worked to expose vulnerabilities in its smart tractors.[2]

Healthcare remains one of the most frequently and consistently targeted, with attacks rising steadily 115.4% year-over-year. According to The HIPAA Journal,[3] researchers at Michigan State University, Yale University, and Johns Hopkins University have found that ransomware is now one of the leading causes of healthcare data breaches. This risk became painfully real for several major healthcare organizations hit by ransomware attacks attributed to the Interlock ransomware gang (on our **ransomware family watch list**). Learn more in the section, **"Healthcare Under Siege: The Era of Massive Data Theft."**

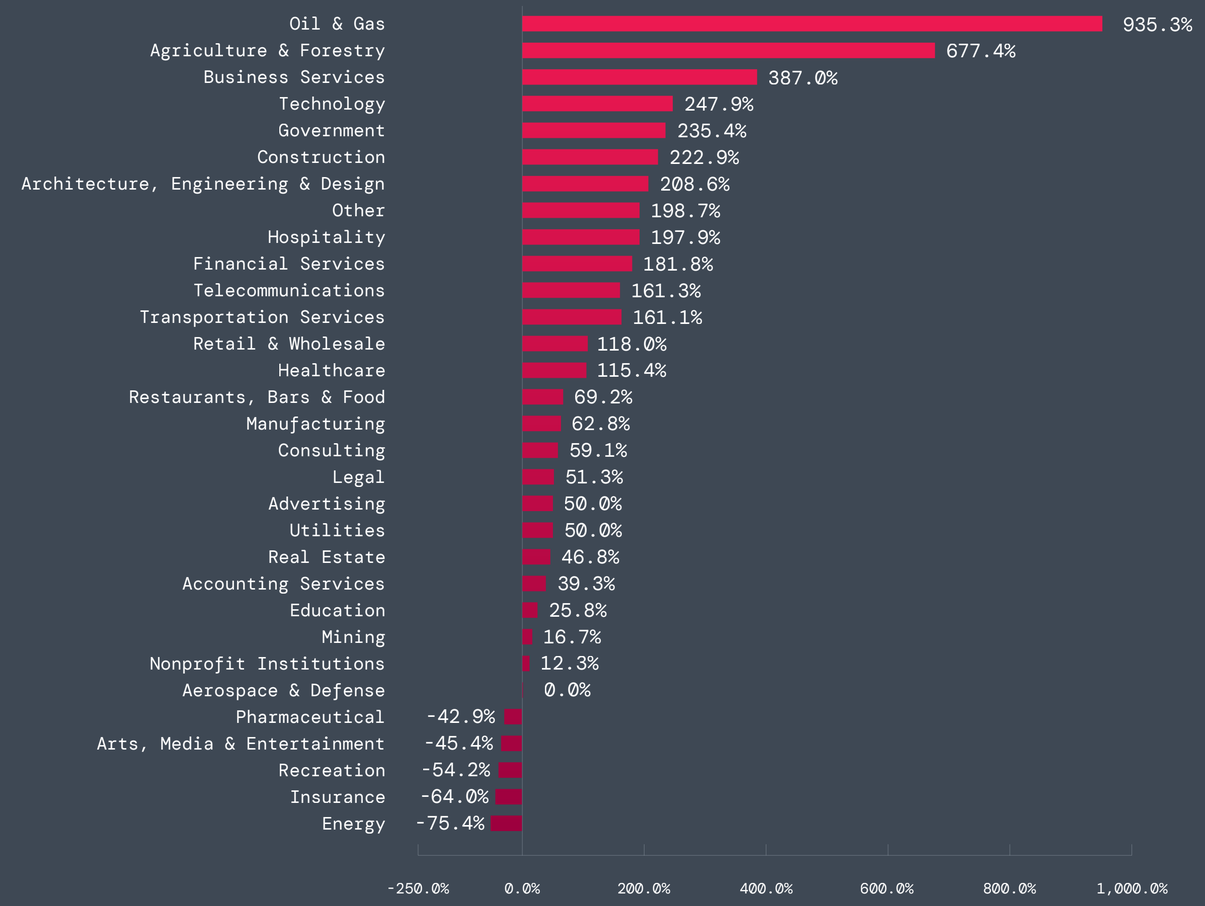


Figure 7: Year-over-year percentage change in ransomware extortion attacks by industry
(industries with <10 reported attacks in last year's dataset excluded to avoid overstating growth due to a low baseline)

[1] CISA, **Unsophisticated Cyber Actor(s) Targeting Operational Technology**, May 6, 2025.
[2] Axios, **John Deere invites students to hack tractors**, June 24, 2025.
[3] The HIPAA Journal, **Study Explores Extent of Hacking and Ransomware Attacks in Healthcare**, May 16, 2025.

Global and regional hotspots

Leak site data reveals a clear geographic concentration, with a dominant share of attacks targeting organizations in the United States (50.8%), far ahead of countries like Canada (5.2%) and the United Kingdom (4.6%). This reflects how threat actors continue to prioritize digitally concentrated, high-value economies. Figure 8 breaks down the top 15 most targeted countries by share of ransomware attacks recorded on data leak sites.

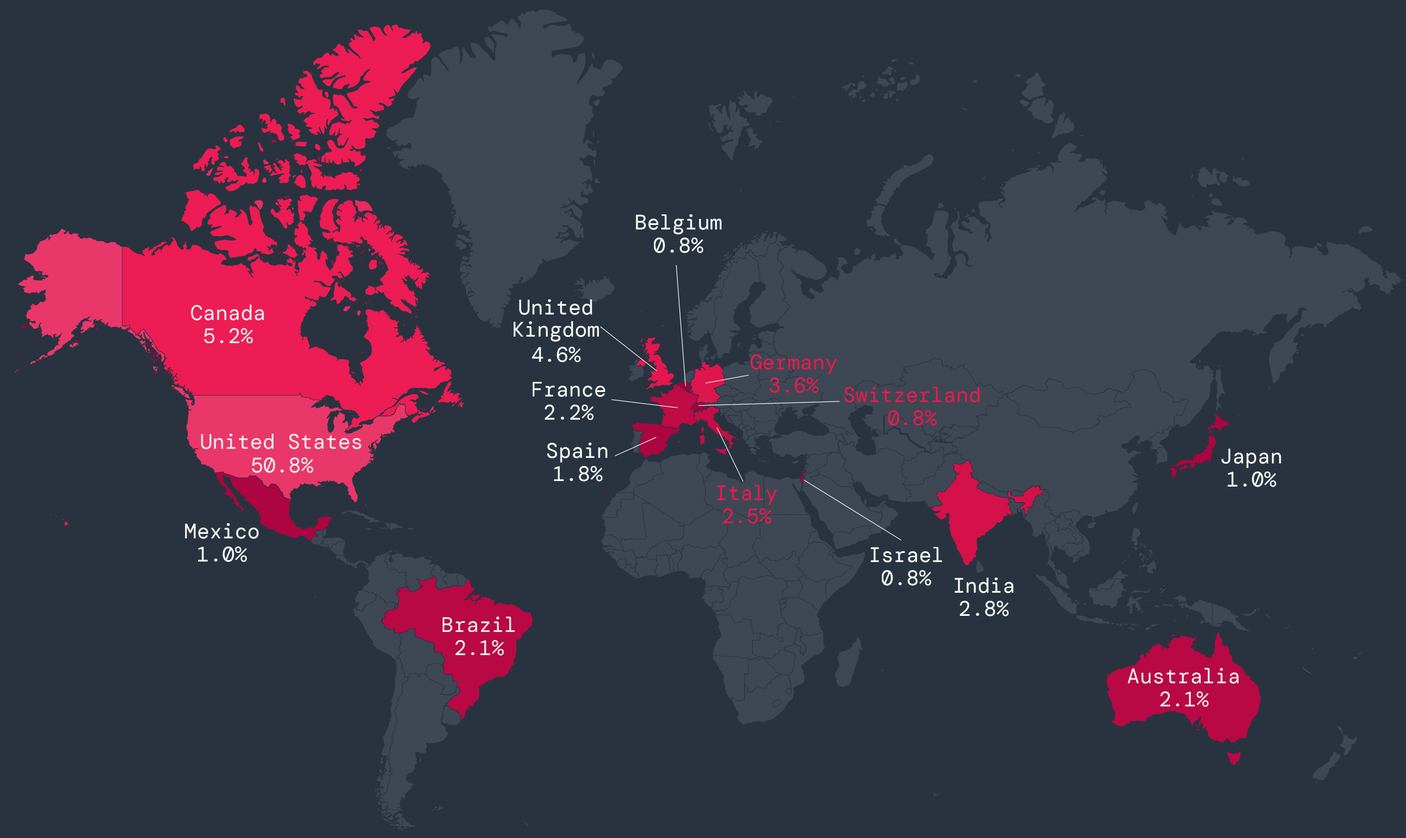


Figure 8: Top 15 countries based on share of ransomware attacks

Year-over-year trends

Ransomware's impact varies widely from region to region. Understanding where attacks are accelerating helps predict where threat actors are likely to strike next and supports more regionally informed defense strategies.

GLOBAL TOP 15: MASSIVE SPIKES IN THE US

Ransomware attacks surged worldwide, with the top 15 countries by number of ransomware attacks experiencing double- and triple-digit percentage increases (see figure 9). Attacks in the US more than doubled to 3,671 attacks—exceeding the combined total of the remaining top 15 most-targeted countries. Canada's 194.5% increase reinforces how threat actors are expanding across North America, with a growing focus on vulnerable sectors. The Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025-2026 names ransomware the top cybercrime threat to the nation's critical infrastructure, citing escalating attacks on healthcare, industrial, and public sector organizations.[4]

Country	Ransomware Attacks (2024 Report)	Ransomware Attacks (2025 Report)	Percentage Change
United States	1,821	3,671	101.6%
Canada	128	377	194.5%
United Kingdom	216	333	54.2%
Germany	149	260	74.5%
India	60	199	231.7%
Italy	118	181	53.4%
France	119	159	33.6%
Australia	73	152	108.2%
Brazil	57	149	161.4%
Spain	62	134	116.1%
Japan	42	75	78.6%
Mexico	57	74	29.8%
Switzerland	43	60	39.5%
Belgium	34	59	73.5%
Israel	11	59	436.4%

Figure 9: Year-over-year comparison of ransomware attacks by country

[4] Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025-2026, accessed July 14, 2025.

EMEA: INTENSIFYING ATTACKS IN EUROPE AND BEYOND

The Europe, Middle East, and Africa (EMEA) region experienced widespread increases in ransomware activity, as shown in figure 10. Notable year-over-year spikes included major economies like Spain (+116.1%) and Germany (+74.5%) as well as smaller markets such as Belgium (+73.5%). Israel saw a 436.4% spike, a sharp relative increase that, while from a smaller baseline of attacks, likely reflects growing geopolitical tensions and a rise in state-linked ransomware operations.

Country	Ransomware Attacks (2024 Report)	Ransomware Attacks (2025 Report)	Percentage Change
United Kingdom	216	333	54.2%
Germany	149	260	74.5%
Italy	118	181	53.4%
France	119	159	33.6%
Spain	62	134	116.1%
Switzerland	43	60	39.5%
Belgium	34	59	73.5%
Israel	11	59	436.4%
United Arab Emirates	21	52	147.6%
Netherlands	50	52	4%

Figure 10: Year-over-year comparison of ransomware attacks by country in the EMEA region

APAC: EXPLOSIVE GROWTH IN EMERGING AND ESTABLISHED MARKETS

The Asia-Pacific (APAC) region recorded some of the highest year-over-year increases globally. As figure 11 shows, ransomware actors broadened their footprint across a region characterized by fast-paced digital transformation and inconsistent levels of cyber maturity. The impact was felt throughout APAC, spanning regional tech and logistics hubs like Singapore (+237.5%) and Taiwan (+147.1%) to large-scale economies like China (+186.7%) and India (+231.7%).

Country	Ransomware Attacks (2024 Report)	Ransomware Attacks (2025 Report)	Percentage Change
India	60	199	231.7%
Australia	73	153	109.6%
Japan	42	75	78.6%
Singapore	16	54	237.5%
Indonesia	23	43	86.9%
China	15	43	186.7%
Taiwan	17	42	147.1%
Thailand	25	32	28%
Malaysia	20	27	35%
Hong Kong	7	23	228.6%

Figure 11: Year-over-year comparison of ransomware attacks by country in the APAC region

Most active ransomware groups in 2024–2025

Several highly active groups continued to dominate the ransomware ecosystem, with RansomHub leading the pack, claiming the highest number of publicly named victims at 833. This positioned the group as the most prolific ransomware operation based on reported activity over the last year. Interestingly, the group decided to cease operations and disappeared in April 2025.

Akira and Clop have both moved up in the ransomware attack rankings since last year. Akira, associated with 520 victims, has steadily expanded its reach through numerous affiliates and initial access brokers. Clop, known for its focus on supply chain attacks, is close behind with 488 victims, highlighting its strategy of targeting the third-party software applications that many companies use to maximize impact.

Figure 12 shows the ransomware groups with the most victims over the last year.

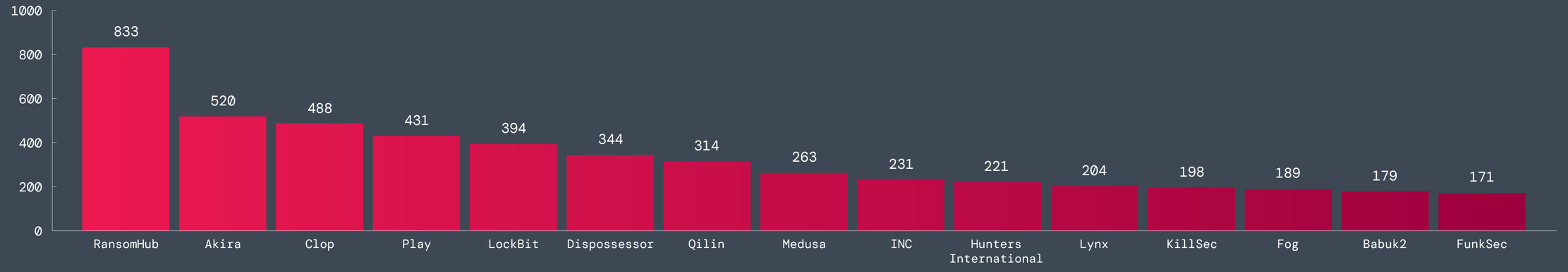


Figure 12: Ransomware attacks reported on data leak websites

New ransomware groups on the scene

The ransomware landscape is constantly shifting, with some legacy groups disappearing and new groups surfacing. This can be a strategic rebranding to sidestep sanctions or an effort by a new group to fill a void left by others. Regardless, affiliates from defunct ransomware groups regularly transition between operations, employing their established attack methodologies. The timeline in figure 13 showcases ransomware groups that became active and started publishing data on leak sites between April 2024 and April 2025.

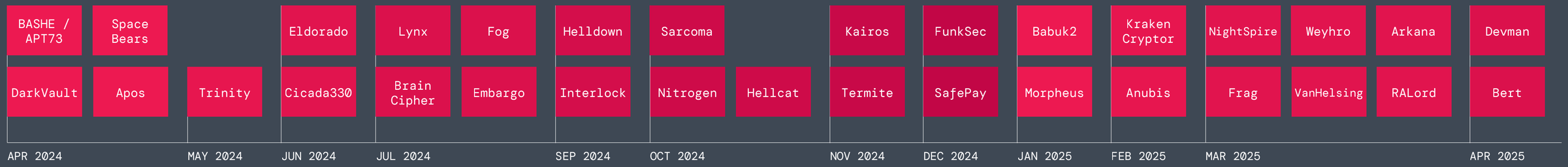


Figure 13: New ransomware groups with data leak sites

Major vulnerabilities exploited in ransomware campaigns

Ransomware groups are increasingly leveraging vulnerabilities in critical enterprise technologies to execute impactful attacks. Exploiting these vulnerabilities provides attackers direct pathways to move laterally, steal sensitive information, and spread ransomware across network environments. Nearly all of these vulnerabilities are easily exploited because they are internet-facing applications that can be discovered through basic scanning techniques. Key targets include VPNs, backup systems, hypervisors, remote access tools, and file transfer applications—technologies that are pervasive across organizations and essential to operations.

VPNs

Virtual private network (VPN) vulnerabilities typically provide attackers direct access to an organization's internal network, effectively enabling threat actors to perform reconnaissance, move laterally, and compromise critical systems to steal data and deploy ransomware.

Examples of these vulnerabilities include **CVE-2024-55591** (affecting FortiProxy SSL VPN devices) and **CVE-2024-40766** (affecting SonicWall SSL VPN devices).

Backup Solutions

Backup and replication technologies have become pivotal attack vectors for ransomware operators. Vulnerabilities in these systems allow direct access to steal information and disable backup solutions prior to file encryption.

An example vulnerability that has been exploited by ransomware threat actors is **CVE-2023-27532** (Veeam Backup & Replication).

Virtualization Software

Hypervisors such as VMware ESXi concentrate workloads, making them high-value ransomware targets. Exploits against ESXi can compromise entire virtualized environments.

For example, the vulnerability **CVE-2024-37085** allows attackers to manipulate the ESX Admins group to gain control of a server. Over the last several years, ransomware groups have also increasingly developed custom ransomware builds exclusively to encrypt files in ESXi environments.

Remote Access Tools

Remote monitoring and management (RMM) tools are critical in corporate IT environments for managing endpoints and infrastructure. However, they are also common targets by ransomware groups, especially when the underlying software is vulnerable.

Examples of these vulnerabilities are **CVE-2024-57726**, **CVE-2024-57727**, and **CVE-2024-57728** (SimpleHelp RMM), which have enabled ransomware threat actors to gain access to corporate environments.

File Transfer Applications

Companies use file transfer applications to efficiently share files across internal systems and between external partners, vendors, or customers. However, when exposed to the internet, any vulnerability present in the underlying application can be exploited to access the organization's data. This group of applications has been the primary target by the Clop ransomware group, which we discuss later in the report.

Over the last year alone, the group leveraged multiple zero-day vulnerabilities in file transfer applications (**CVE-2024-50623** and **CVE-2024-55956**) to steal data from hundreds of organizations.

Shoring up vulnerable systems

To combat the ransomware campaigns driven by these vulnerabilities, defenders must adopt a layered approach to security:

1. **Patching as priority:** Expedite fixes for edge-facing services—firewalls, VPNs, and backup systems.
2. **Segmentation and zero trust:** Block lateral movement by enforcing user-app segmentation, device posture management, strict access controls, and monitoring privileged accounts.
3. **Advanced threat protection with zero day coverage:** Leverage inline sandboxing and isolation technologies to prevent zero day exploitation. Perform TLS inspection to block malicious payloads and apply data loss prevention (DLP) controls to stop data exfiltration.

By proactively closing these security gaps, defenders can reduce ransomware actors' ability to exploit vulnerabilities and significantly strengthen their organizational resilience.

Ransomware_Roundup: What's Making Headlines

Black Basta Leverages ChatGPT for Criminal Activities

In February 2025, a treasure trove of messages from the Black Basta ransomware group's internal Matrix chat server were leaked online, giving researchers a firsthand look into the group's operations. Spanning September 2023 to September 2024, these chats shed light on the group's inner structure, attack strategies, and processes. Most notably, they reveal how Black Basta utilizes ChatGPT, which comes as no surprise given its widespread popularity. According to the ThreatLabz 2025 AI Security Report, ChatGPT dominates the AI landscape, accounting for roughly 45% of all AI-related transactions.

Due to ChatGPT's widespread popularity and saturation in the AI landscape, ThreatLabz concentrated its analysis on how Black Basta integrates ChatGPT into its routine operations.

Our findings reveal that the ransomware group employs ChatGPT in several ways:

- **Code rewriting:** The chat logs explicitly mention using ChatGPT to rewrite scripts in Python.
- **AI reliance:** The group refers to relying partly on ChatGPT alongside internet resources, suggesting its integration into their broader workflow. In addition, the chat logs show members encouraging one another to problem-solve using ChatGPT.
- **Interest in unrestricted AI models:** Discussion about WormGPT reflects an interest in exploring uncensored AI tools, which may offer capabilities not limited by the legal and ethical rules built into ChatGPT.

Russian	English	What Does This Mean?
щас попизжу с chat gpt	*Now I'll have a chat with ChatGPT*	Demonstrates that Black Basta members use ChatGPT to assist with technical tasks.
чату gpt задайте вопрос *он поможет вам*	*Ask ChatGPT the question* *He will help you.*	Shows how Black Basta is using ChatGPT as a problem-solving tool and encouraging others in the group to use it.
что они подразумевают под тем что все что ты писал надо переписать на питон ? *надо тз и какие функции, а я скажу возможно это или нет* *попробуй переписать чатом gpt*	*What do they mean by "everything you've written needs to be rewritten in Python"?* *The requirements and what functions are needed—let me know, and I'll say if it's possible or not.* *Try rewriting it with ChatGPT.*	Highlights how Black Basta is using ChatGPT's capabilities to assist in rewriting scripts in Python, potentially saving time and/or compensating for weak Python coding skills.
на половину инет, на половину chatgpt	*Half of it is internet-based, and half is ChatGPT.*	Suggests Black Basta members are taking a hybrid approach to attacks where ChatGPT plays a significant role alongside internet sources.
бля найти бы доступ в WormGPT *без цензуры chatGPT который*	*I don't know where to find access to WormGPT.* *uncensored chatGPT which*	Demonstrates Black Basta's interest in moving beyond ChatGPT to more unethical tools like WormGPT. Suggests they have used ChatGPT extensively and are familiar with its limitations.

Hello? It’s Ransomware Calling: Inside the Multi-Stage Attack Playbook

There has been a shift away from initial access brokers using large-scale spam campaigns as the initial infection vector. Instead, more targeted attacks have been used effectively over the last two years using the methodology illustrated in figure 14.

Threat actors behind these attacks first perform reconnaissance using sites like ZoomInfo to purchase contact information about employees at a targeted company. Additional employee information can be obtained through sites like LinkedIn, enabling threat actors to pinpoint personnel to impersonate, especially those in the company's IT department. Specific employees with privileged access (typically in HR, payroll, and finance) are common targets for attacks.

After the victim's contact information is obtained, the attack kicks off with “spam bombing” to flood a victim's inbox. The threat actor then makes a phone call to that employee (with the information previously obtained) and impersonates another employee in the company's IT department—a classic example of vishing (voice phishing). The callers are chosen to match the impersonated IT employee (male, female, native speaker). The threat actor informs the victim that they are with the company's IT department and reaching out to help the victim "update their spam filter" and requests remote access through an RMM tool such as Microsoft Teams, Quick Assist, Team Viewer, AnyDesk, etc. If the victim falls for the ruse, the threat actor performs a series of actions to install a backdoor on the victim's system while providing enough credibility that the victim's spam filters were “updated.” Figure 15 shows a real website operated by a ransomware initial access broker that uses this ploy.

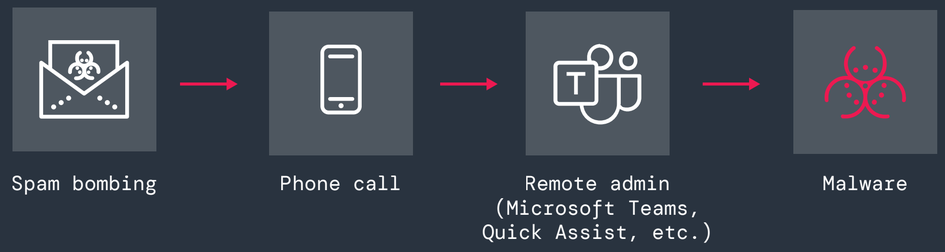


Figure 14: Multi-stage ransomware attack methodology

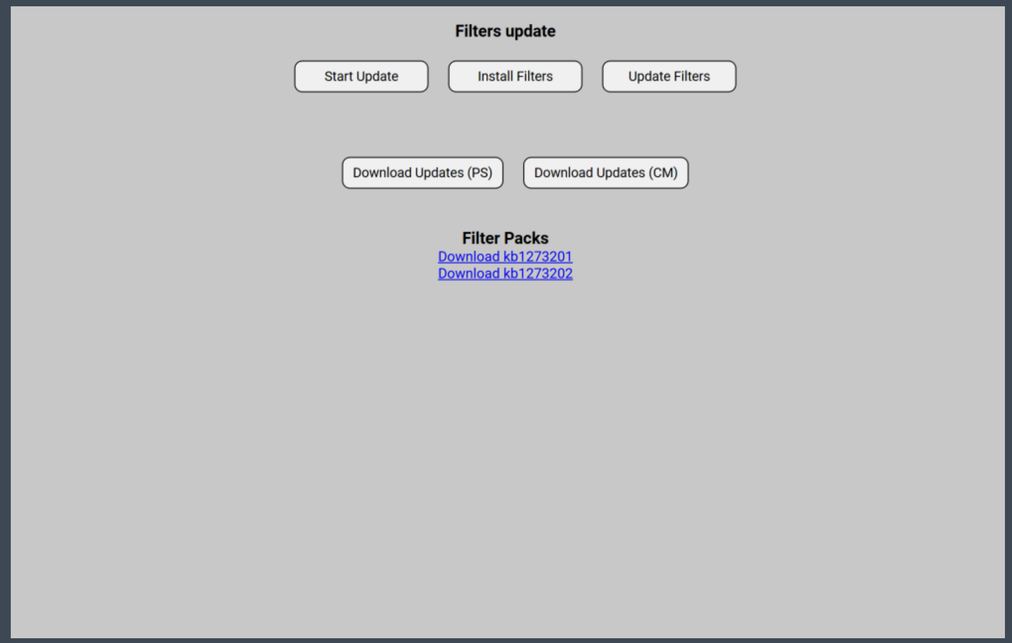


Figure 15: A ransomware initial access broker’s fake “Filters update” website

These websites, often hosted on Azure or Amazon Web Services, are deceptively simple but can employ numerous techniques especially designed to evade antivirus and malware sandboxes. For instance:

- The Filter Packs links are actually a multi-part ZIP archive (split into two parts, e.g., kbxxxxxxx) encrypted with a passphrase.
- The Download Updates button(s) copies PowerShell or Windows shell commands to the victim's clipboard, which are then executed. These commands prompt the threat actor for the ZIP archive's passphrase. In addition, the commands set registry values with the malware payload's command and control information. Thus, the malware executable by itself will not operate properly in a sandbox environment with this prior initialization step.
- After the ZIP archive is decrypted and decompressed, a legitimate executable (e.g., Microsoft OneDrive) is leveraged to decrypt and deploy a malicious payload via DLL sideloading.

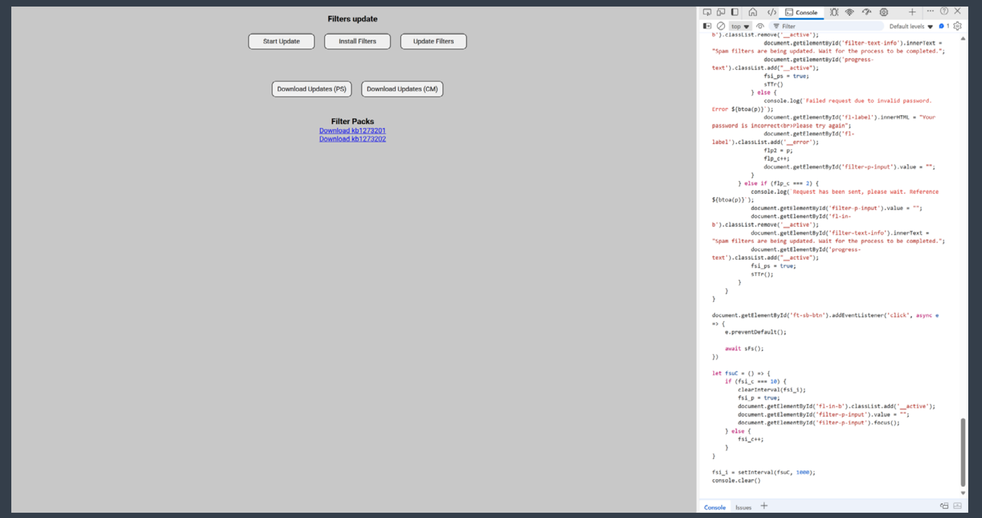


Figure 16: Accessing the console on a victim's endpoint

The top three buttons are designed to steal the victim's Microsoft 365 password. When clicked, each button copies JavaScript content to the victim's clipboard. The threat actor then opens the web browser's developer tools to access the console as shown in figure 16.

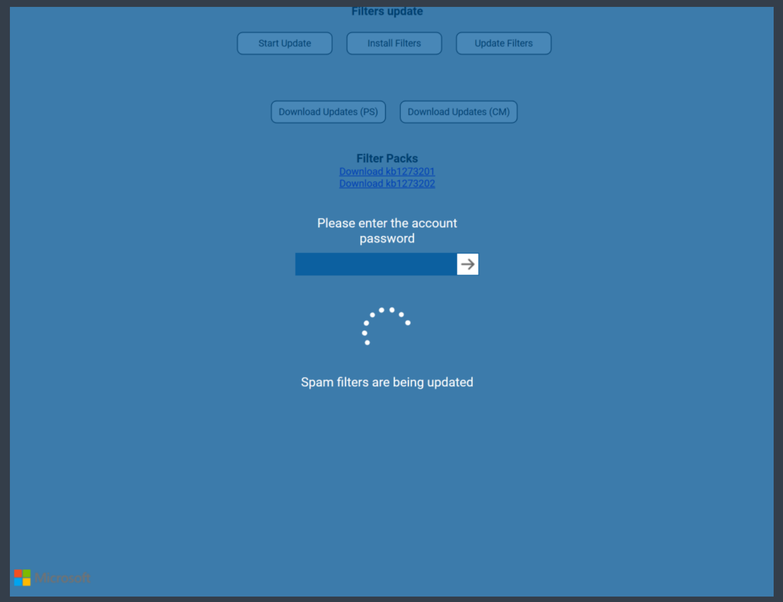


Figure 17: A malicious password entry field

The JavaScript content from the clipboard is then pasted into the console and executed, displaying an overlay that prompts the victim to enter their password, as in figure 17.

After the victim's account password is stolen and the malware backdoor installed, the threat actor attempts to move laterally within the organization to steal information and deploy ransomware. This new style of targeted ransomware attacks often succeeds, with a high rate of victims falling for these lures.

Leaky LockBit: RaaS Mechanisms Exposed in Dark Web Breach

In May 2025, LockBit's affiliate and admin panels were defaced with a link to download the group's database (see figure 18).

The leaked MySQL database provides researchers, including ThreatLabz, a detailed view of LockBit's internal operations following a major **international law enforcement operation** known as Operation Cronos in February 2024, which led to the group's leader being publicly indicted. Even after the takedown, LockBit **bounced back in a matter of days**, launching new attacks with a fresh leak site. The leaked database includes the group's activities around the time of the **LockBit 4.0 release** from December 18, 2024, to April 29, 2025. The information exposes 75 affiliate monikers, 4,423 ransom chat messages, and around 60,000 bitcoin wallet addresses. Out of the 75 affiliates, 54 affiliates created LockBit ransomware builds for 246 victims across 156 organizations. Each affiliate was tagged with a specific trust level, as shown in figure 19.

Figure 18: Defaced LockBit admin panel

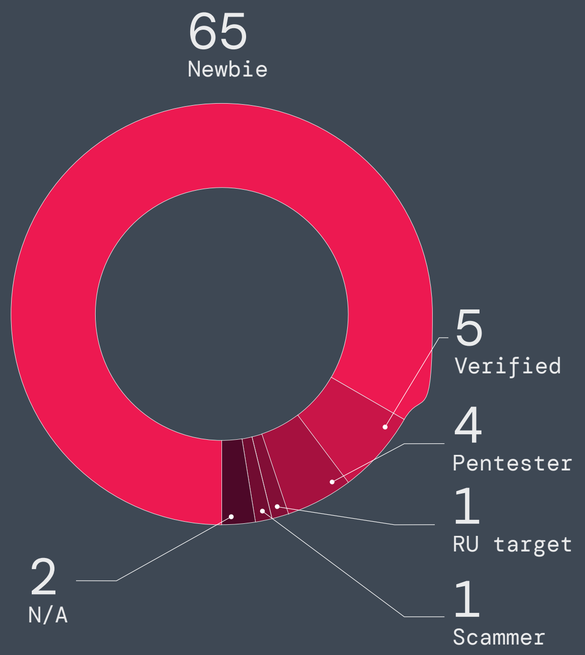


Figure 19: Number of LockBit affiliates by "trust level"

There were 35 affiliates with a paused status, presumably those who were inactive or suspended. Interestingly, one affiliate using the moniker BaleyBeach switched over to using LockBit following the closure of rival RansomHub (which we will discuss later). Below is a chat message sent by this affiliate to a victim.

> "We were affiliates of RansomHub, now RansomHub closed, we movede [sic] here. So existing companies (including yours) which we had to deal with still have chance [sic] to prevent their data leak."

Figure 20 shows the number of LockBit builds generated by affiliates with the most builds.

Neither the admin and matrix777 users had trust levels assigned and were registered with the same TOX ID, indicating that they are likely the same person.

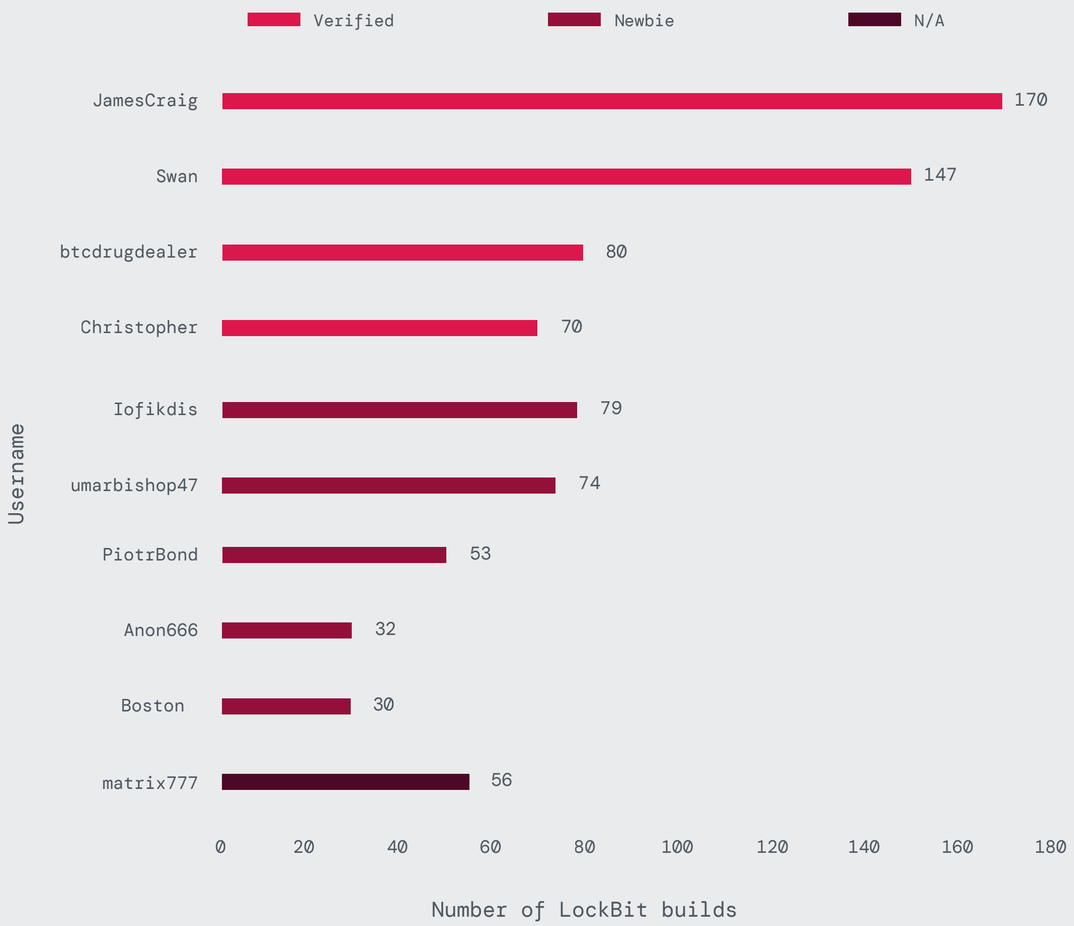


Figure 20: Number of LockBit builds per affiliate

Overall, 208 victims engaged in ransom chats, and 20 paid a ransom. Only 10 LockBit affiliates received ransom payments over this nearly six-month period, as shown in figure 21.

In one instance,* a victim agreed to pay the LockBit affiliate Swan $2 million, but the chat logs ended just before payment information was provided. However, we can infer that the payment was in fact made through another bitcoin wallet in the database, controlled by the LockBit group, who received a 20% commission for that victim. Thus, only two affiliates, Swan and Christopher, earned over US$100,000. In total, all LockBit affiliates earned a combined $2,334,615 ($1,867,692 after commissions) in ransom payments. The LockBit group received 20% of that amount or about $466,923. While not insignificant, these ransom payments are far lower than many of the top ransomware groups, which frequently receive many multimillion-dollar payments. Thus, this leaked LockBit database indicates the February 2024 disruption significantly weakened the group.

Username	Approximate payments received (US$)	Number of paid victims	Total victim chats
Swan	$2,021,000*	2*	17
Christopher	$231,015	8	44
umarbishop47	$40,000	1	10
PiotrBond	$13,000	2	16
ArrynBaird	$10,000	1	5
Iofikdis	$6,000	1	12
RiccardoBond	$4,400	1	4
Brown	$3,600	1	5
JamesCraig	$3,600	2	17
btcdrugdealer	$2,000	1	6

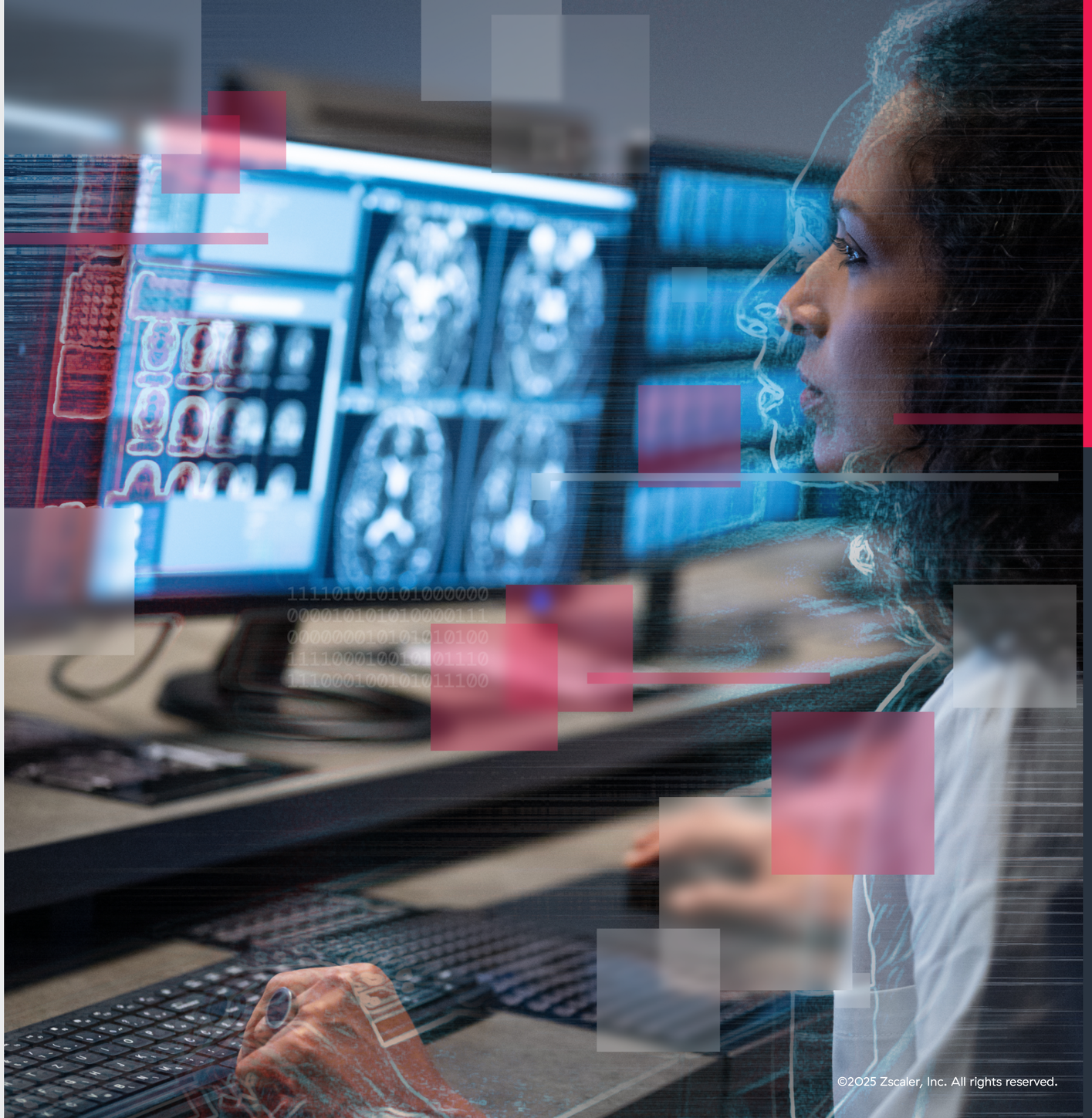
Figure 21: Ransom payments received by LockBit affiliates

Healthcare Under Siege: The Era of Massive Data Theft

Ransomware's playbook in the healthcare sector has evolved with a new prescription: exfiltrate first, disrupt second. Threat actors today prioritize data theft as a primary source of leverage, and with healthcare institutions holding vast repositories of protected health information (PHI), they have become lucrative targets for ransomware operators looking to maximize pressure. Because patient trust is critical in healthcare, a public breach can be as damaging as downtime.

Globally, the healthcare sector saw a substantial year-over-year increase in ransomware attacks. These attacks often combined high-volume data exfiltration with encryption, leaving institutions grappling with operational chaos, financial loss, and reputational damage. In 2024, the US Department of Health and Human Services Office for Civil Rights (OCR) reported 725 breaches involving 500 or individuals, with around 275 million healthcare records exposed.[5]

Ransomware in healthcare is no longer just about disruption. It's about leverage—and that starts with data. By stealing and exposing millions of records, ransomware operators can double down pressure on healthcare victims. Recent data from multiple ransomware families underlines a critical trend: the scale of data theft is rapidly accelerating. Among the groups driving this evolution is Interlock, featured in the section, **"Top 5 Ransomware Families to Watch in 2025–2026."**



[5] The HIPAA Journal, 2024 **Healthcare Data Breach Report**, January 30, 2025.

Turning the Ransomware Tide: From the Front Lines

Despite the significant increase in ransomware attacks over the last year, there are success stories to report in the fight against ransomware. Collaboration between global law enforcement and private industry researchers has proven effective in dismantling some key elements of ransomware operations and supporting victim recovery.

For example, in early 2025, ThreatLabz discovered a vulnerability in RansomHub that made file decryption possible without having to pay a ransom. Building on this discovery, the ThreatLabz team developed *DecryptHub* (see figure 22), a specialized portal designed to help organizations impacted by RansomHub's ransomware attacks.

The ThreatLabz DecryptHub portal helped dozens of victim organizations recover files, saving them potentially millions of dollars in ransom payments.

RansomHub was one of the largest and most active ransomware groups prior to shuttering in April 2025. Many of the group's affiliates were previously associated with the defunct BlackCat ransomware operation. Similar to BlackCat, RansomHub used the Rust programming language to develop and cross-compile ransomware for numerous architectures, including:

- Windows (x86, x64, ARM, ARM64)
- FreeBSD (x64)
- Linux (x86, x64, ARM, ARM64, ARMv5, ARMv5-64, ARMv6, ARMv6-64, ARMv7, ARMv7-64)
- ESXi (x64)

Another notable achievement over the past year is the large-scale law enforcement operation, codenamed **Operation Endgame**, executed in coordination with industry partners, including Zscaler (see figure 23).

Operation Endgame is a global initiative aimed at dismantling cybercriminal organizations and the malware ecosystem that facilitates ransomware attacks. The most recent success was the takedown of **DanaBot**, a powerful modular malware family that operated a malware-as-a-service (MaaS) platform with links to various ransomware groups. This builds on a string of victories in 2024, when Operation Endgame targeted well-known malware families like **SmokeLoader**, IcedID, SystemBC, Pikabot, and Bumblebee.

Zscaler ThreatLabz has been supporting Operation Endgame over the past two years, providing vital resources and intelligence to identify malware campaigns, dismantle criminal infrastructure, and expose cybercriminals. ThreatLabz has also released free tools via **GitHub** that can be used to detect and remediate infections—underscoring the importance of collaboration in the fight against ransomware.

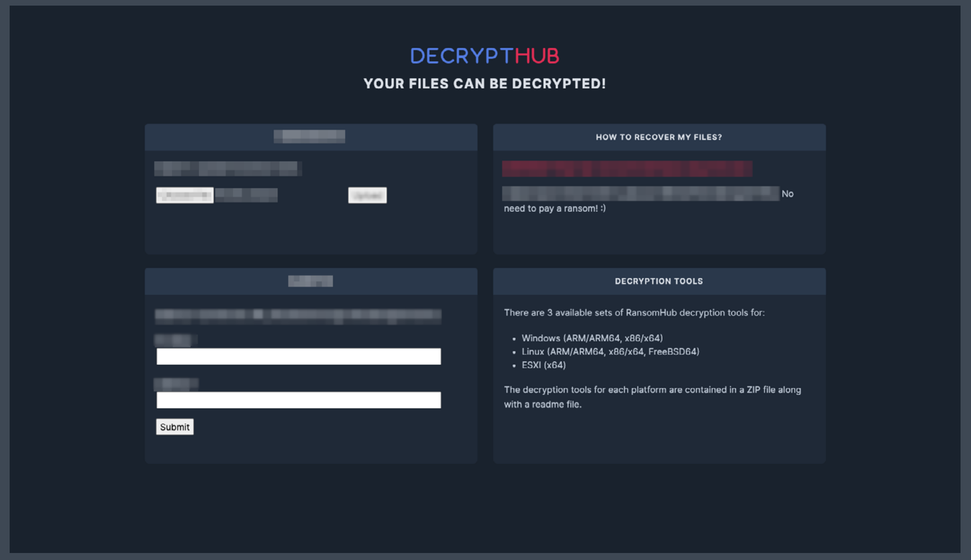


Figure 22: The DecryptHub victim portal

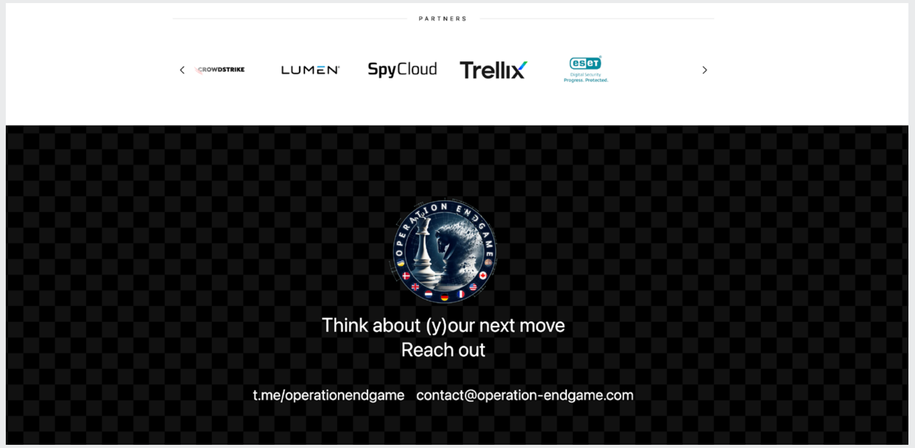


Figure 23: Operation Endgame contact details

Top 5 Ransomware_ Families to Watch in 2025-2026

#1 Dark Angels

The Dark Angels ransomware group, active since April 2022, is one of the most successful ransomware families to date. The group has gained notoriety for their highly lucrative attacks, with a record-breaking $75 million ransom payment that ThreatLabz disclosed in 2024. The group stands out from the pack for a variety of reasons. Unlike other threat groups, Dark Angels does not outsource attacks to third-party affiliates (i.e., initial access brokers). The number of attacks launched by Dark Angels is limited and focused on large organizations. Dark Angels exfiltrates vast amounts of data from victims, with an average of 9.6 TB and a median of 2.35 TB. The group then chooses whether to deploy ransomware and encrypt an organization's data. Dark Angels attempts to avoid debilitating organizations with ransomware to avoid news headlines and fly under the radar.

The group posts stolen victim data on a website named Dunghill Leak and a Telegram channel, neither of which mentions Dark Angels, likely in part to distance themselves (from an attribution standpoint) from the attacks.

Dark Angels infiltrates corporate networks using a variety of techniques, including phishing emails, and through publicly exposed applications that contain vulnerabilities such as CVE-2023-22069. The group scans compromised networks and takes advantage of Microsoft Active Directory environments. The primary targets are users with domain administrator privileges to facilitate lateral movement and access to the organization's domain controllers.

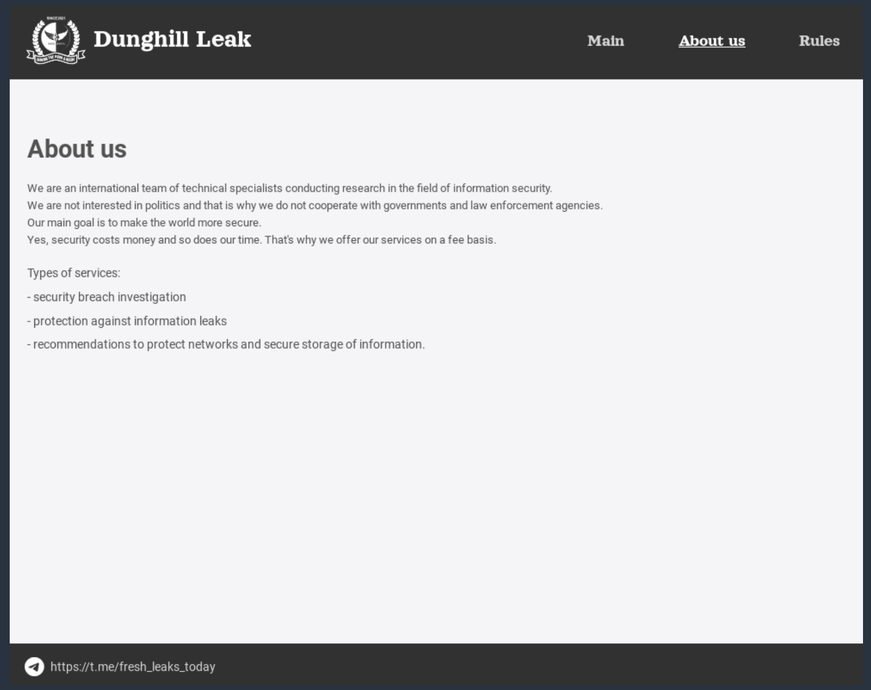


Figure 24: Dark Angels group's Dunghill Leak site

Interestingly, Dark Angels has not developed its own ransomware. Instead, the group relies on custom builds of third-party ransomware families including Babuk, Read the Manual (RTM) Locker, and a variant of RagnarLocker. Dark Angels targets files on Windows, Linux, ARM, and ESXi for file encryption.

#2 Clop/Cl0p

Clop, also known as ClOp, is a ransomware group that has been active since 2019. Clop has largely shifted away from file encryption, instead focusing on data extortion via supply chain attacks that exploit zero-day vulnerabilities, especially in popular web-based secure file transfer application platforms that enable them to access and steal sensitive data from hundreds or even thousands of organizations at a time. One of the first file transfer applications that was exploited was Acellion's legacy File Transfer Application (FTA) in December 2020. The legacy Acellion FTA had numerous vulnerabilities (CVE-2021-2710, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104) that Clop exploited to deploy a custom webshell to steal data from dozens of organizations. In July 2021, Clop exploited CVE-2021-35211 in the **Serv-U Managed File Transfer and Serv-U Secure FTP applications**. In these instances, Clop used the vulnerability to gain access to organizations' internal networks, leading to data exfiltration and file encryption.

In early 2023, Clop conducted another supply chain attack targeting GoAnywhere's Managed File Transfer (MFT) application. This attack exploited CVE-2023-0669, allowing unauthenticated remote code execution and data theft. Clop leveraged the zero-day vulnerability to steal data **from more than 100 companies**. In May 2023, only a few months after the GoAnywhere MFT incident, Clop exploited a zero-day SQL injection vulnerability (**CVE-2023-34362**) in the MOVEit Transfer application to steal data from companies that had internet-facing instances. This was one of the largest ransomware supply chain attacks to date, impacting more than 2,500 organizations and leading to the loss of personal information for **millions of people**. Clop announced this attack on their data leak site, as shown in figure 25.

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@GOTO-PAY.COM OR SUPPORT@IN2PAY.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Figure 25: Clop's announcement of the CVE-2023-34362 MOVEit vulnerability exploit

Clop's most recent large-scale supply chain attacks were in October 2024, which exploited two vulnerabilities CVE-2024-50623 and CVE-2024-55956 in Cleo's Harmony, VLTrader, and LexiCom file transfer applications. These vulnerabilities allowed an unauthenticated user to import and **execute arbitrary Bash or PowerShell commands**. Once again, Clop used these vulnerabilities to steal data from organizations that used Cleo's file transfer applications that were exposed to the internet. An example Clop ransom note provided to a victim of these Cleo attacks was captured by ThreatLabz and is available here.

The breadth of Clop's attacks is significant, with some victims subjected to multiple breaches by the group. In fact, ThreatLabz identified a victim from Clop's MOVEit attack, who previously paid $1 million in ransom, later falling victim to the group's Cleo attack.

#3 DragonForce

DragonForce emerged as a RaaS group in December 2023. Early versions of DragonForce's ransomware used the leaked LockBit builder, and the group later created its own ransomware based on the leaked Conti source code. In early 2025, DragonForce announced a new "cartel" business model on a cybercrime forum and its news website, as shown in figure 26.

This new model enables ransomware affiliates to use the group's infrastructure, tools, and services for their own attacks with an 80/20 percent profit-share scheme. The group's affiliates have stolen more than 30 TB of data, with each victim losing approximately 156 GB on average, with a median of 72 GB.

DragonForce received relatively modest attention until April 2025, when the group announced that they were "merging" with RansomHub, one of the largest and most active ransomware groups at the time. RansomHub denied the claim and accused members of DragonForce of disrupting their infrastructure and defacing their website. Whether the claim was accurate or by coincidence, RansomHub shut down operations and many of the group's affiliates migrated to DragonForce. These affiliates include Scattered Spider (aka "The Com"), which has conducted significant attacks on large organizations using various social engineering techniques targeting IT departments to bypass multifactor authentication (MFA). Scattered Spider is believed to be behind the DragonForce attacks targeting multiple UK retailers in April and May 2025.

#4 Akira

Since emerging in April 2023, Akira has established itself as one of the most active ransomware groups. The initial versions of Akira were based on the leaked Conti source code. The group later developed a Rust-based ransomware named Megazord. However, the group abandoned Megazord in favor of the C/C++ based variant, which is now compiled for ESXi versions 6 and 7 as well as Windows x86 and x64. The latest variant uses the GNU Multiple Precision Arithmetic Library (GMP) for RSA encryption instead of the native Windows APIs found in earlier versions. It's interesting to point out that Black Basta previously used the same GMP library for asymmetric encryption in their ransomware (before migrating to the Crypto++ library).

Akira affiliates continue to focus primarily on file encryption rather than stealing large amounts of data. The volumes of data exfiltration by Akira affiliates are typically lower on average than many other ransomware groups that steal terabytes of data or more from individual victims. In fact, on Akira's data leak site (see figure 27), the average and median data theft volumes were 44.87 GB and 14.33 GB, respectively. The largest data theft was about 370 GB, far smaller than many top ransomware families. However, despite not emphasizing data theft, Akira has significant numbers of victims and is responsible for more than 13 TB of data loss in total.

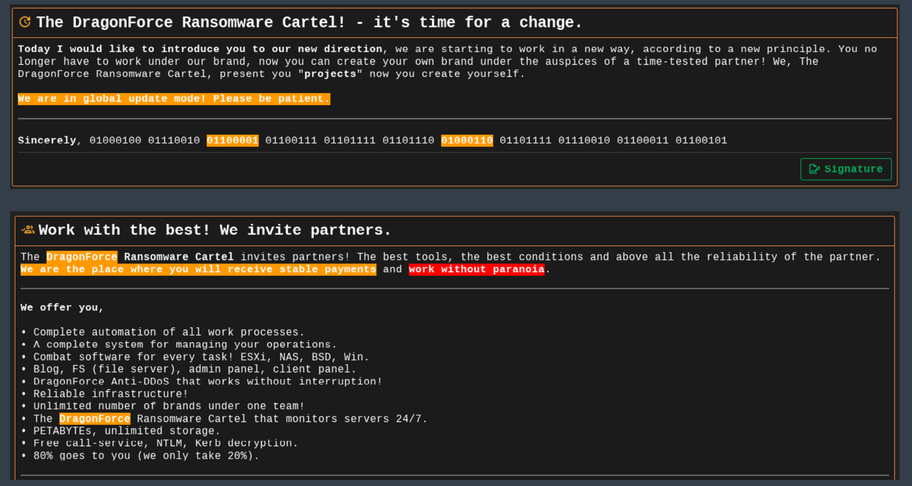


Figure 26: DragonForce "cartel" announcement

Figure 27: Akira group's data leak site

#5 Interlock

Interlock is a newer ransomware group that has been conducting attacks since at least September 2024, compromising around 50 victim organizations. Interlock's attacks span various sectors, including healthcare, education, finance, government, and manufacturing. The former two sectors have been particularly hard-hit by Interlock. This targeting is likely due to the group's keen awareness of compliance frameworks such as GDPR, HIPAA, CCPA, NYDFS, and GLBA. Interlock attempts to leverage these regulations to pressure these victims into paying a ransom. In fact, Interlock's ransom notes specifically call out the financial penalties for such violations.

The group has developed ransomware variants for Windows, Linux, and FreeBSD. The ransomware isn't noteworthy other than it is relatively uncommon to create specific builds for the latter. However, since many large organizations use FreeBSD to run critical server infrastructure, it is not surprising and will remain a target.

Similar to Dark Angels, Interlock steals significant volumes of data from organizations. In one instance, Interlock stole more than 11 TB of data from a single victim. Another victim in the healthcare industry lost more than 5 TB of data and paid over $2.5 million in ransom. Overall, the group has stolen more than 73.5 TB of data in the last nine months alone. On average, each victim lost 1.6 TB of data, with the median loss around 700 GB.

The About section on Interlock's data leak site, shown in figure 28, highlights the group's stance toward victims. Interlock blames victims for "recklessness" and "negligence" as the root causes that lead to the group's ransomware attacks.

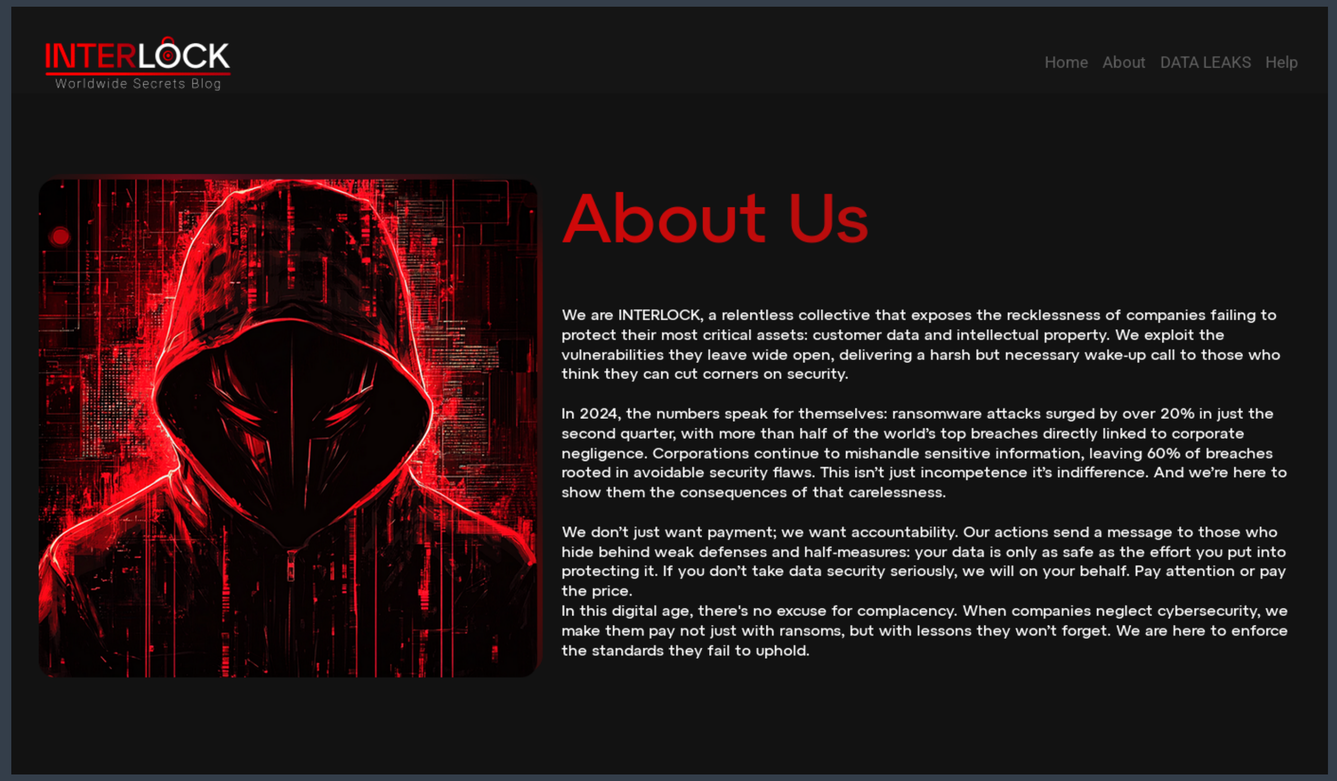


Figure 28: Interlock group's "About Us" page

ThreatLabz Ransomware_Notes Archive

Zscaler ThreatLabz maintains a **public GitHub repository** that, as of this writing, added another 73 new ransomware notes over the past year, bringing the total to 1,018. This archive can be valuable for tracking ransomware groups over time, including their data leak websites and negotiation tactics, as well as for using stylometric analysis to link ransomware groups that rebrand.

2026_ Predictions

1. Ransomware groups will weaponize GenAI for scalable, multi-phase extortion campaigns.

Generative AI will increasingly become core infrastructure for ransomware operations. Leaked communications from the Black Basta group reveal how ransomware threat actors are already using tools like ChatGPT to generate phishing lures and fake documents, debug and rewrite malware, and craft deepfake content. Looking ahead, expect ransomware operations to expand this model—with vast possibilities, including using LLMs to analyze and summarize sensitive data that is stolen. In addition, as companies increase the amount of data they collect for AI training purposes, this data will make lucrative targets for ransomware gangs.

2. Ransomware groups will continue to employ multi-stage social engineering attacks.

Ransomware operators will double down on targeted attacks and ditch mass spam campaigns for highly precise social engineering. Using platforms like LinkedIn and ZoomInfo, they'll pinpoint employees with privileged access, overwhelm inboxes with spam, then impersonate IT staff via phone calls to gain entry.

3. Voice-based attacks will rise as ransomware operators refine social engineering tactics.

Ransomware groups will continue to leverage voice-based attack vectors through voice phishing or "vishing" and AI-generated audio to gain access to victim organizations. These tactics exploit human trust and urgency, often impersonating executives or IT staff to manipulate employees into disclosing credentials or granting access to internal systems. As generative AI tools become more accessible, ransomware threat actors will essentially put vishing on autopilot—leveraging tactics like multilingual voice cloning and adaptive call scripts to deceive enterprise employees and open the door to encryption and extortion.

4. Data extortion will remain a key driver for ransom payments, with increased volumes of theft.

Data theft is becoming the primary lever in ransomware campaigns, and this trend will accelerate. Groups like Clop, BianLian, and Hunters International have led the shift toward pure extortion operations, abandoning encryption entirely. ThreatLabz observed that several of these groups now steal hundreds of gigabytes per victim on average. As organizations improve their backup and recovery capabilities, threat actors will increasingly weaponize stolen data to pressure victim organizations into paying.

5. Ransomware source code and builder leaks will power the next generation of attacks.

As ransomware builder tools and source code continue to leak (intentionally or otherwise), a new wave of low-effort, high-impact attacks will emerge. Leaks from major ransomware groups have already fueled spin-off operations, rebranded variants, and copycat campaigns. Emerging groups will build on leaked codebases, modifying payloads and delivery techniques while evading existing detection signatures.

6. Law enforcement will expand focus to target ransomware enablers.

International law enforcement operations are growing bolder and more targeted, taking down not just ransomware groups, but also the infrastructure and services that enable their attacks. Operation Endgame demonstrated that malware distribution platforms can be dismantled at scale.

7. Ransomware affiliates will continue to move between groups.

The ransomware-as-a-service (RaaS) model gives affiliates flexibility—and creates volatility in the threat landscape. Affiliates frequently shift between groups based on takedown pressures, payout terms, tooling, or reputation. This constant movement leads to recycled infrastructure, overlapping tactics, and rapid rebrands when operations are disrupted. As long as affiliate models remain profitable with low risk, this pattern will continue.

How Zscaler Stops Ransomware with Zero Trust + AI

Ransomware thrives in environments where security is fragmented, visibility is limited, and trust is implicit. Yet many organizations still rely on traditional security tools—next-generation firewalls, VPNs, and point products like anti-malware—that weren't designed to handle modern threats.

These legacy architectures create more risk than they mitigate. They leave critical gaps in ransomware protection, from blind spots in encrypted traffic to siloed threat visibility and complex, inconsistent policy management. Worse, these architectures rely on broad, overly permissive access models that expose internal resources. Once attackers gain a foothold, they can move laterally across systems—making it easier for ransomware threat actors to spread, escalate privileges, and reach sensitive data without detection.

The **Zscaler Zero Trust Exchange™** eliminates these risks by replacing outdated, network-centric models with a cloud native, AI-powered zero trust architecture. It delivers a unified, scalable platform that minimizes risk and simplifies ransomware protection across users, devices, and applications—no matter where they reside.

ZSCALER STOPS RANSOMWARE AT EVERY STAGE OF THE ATTACK LIFE CYCLE:

- **Minimize the attack surface:** Effectively eliminate exposed infrastructure that ransomware can target by hiding users, applications, and devices behind a cloud proxy, where they are not visible or discoverable from the internet, creating a far smaller attack surface. There are no public IPs and no direct network access—ransomware threat actors cannot find or reach internal resources. Breach prediction technology leverages AI to simulate attack scenarios and pinpoint likely paths threat actors could exploit, allowing security teams to remediate before an attack occurs.
- **Prevent initial compromise:** Protect users from accessing malicious content and detect unknown threats before they reach your network through full TLS/SSL inspection and inline sandboxing and isolation. These capabilities stop ransomware before it can execute, minimizing the risk of a compromise occurring in the first place.
- **Eliminate lateral movement:** Connect users directly to applications (and apps to other apps), not the network itself, eliminating the risk of lateral movement. AI-powered segmentation adapts access based on user behavior, device posture, and app context. Ransomware threat actors can't spread from one system to another, even if an endpoint is compromised. AI and identity threat detection and response (ITDR) help surface anomalous access patterns while deception technology and decoys lure ransomware threat actors into monitored traps.
- **Block data exfiltration:** Extortion-first ransomware campaigns rely on stealing sensitive data. Inline data loss protection (DLP), CASB, and traffic inspection capabilities block unauthorized transfers to sanctioned cloud apps, shadow IT, and command-and-control (C2) infrastructure.

KEY AI-POWERED RANSOMWARE PROTECTIONS FROM ZSCALER INCLUDE:

- **Breach prediction** preempts potential breach scenarios using generative AI and multidimensional predictive models.
- **Phishing and C2 detection** uses inline AI-based detection from the Zscaler Secure Web Gateway to identify and block never-before-seen phishing sites and C2 infrastructure.
- **Inline sandboxing** offers comprehensive malware and zero-day threat prevention by using advanced AI models to analyze suspicious files in a controlled environment.
- **Zero Trust Browser** leverages AI to identify and isolate malicious web content, preventing data leaks and malware delivery.
- **Segmentation** uses machine learning to auto-generate recommendations for app segments and policies, ultimately minimizing the attack surface and preventing lateral movement.
- **Dynamic, risk-based policy** continuously evaluates the risk posture of users, devices, and applications using AI-driven behavioral analysis to enforce dynamic security and access policies.
- **Data discovery and classification** instantly scans and classifies sensitive data across endpoint, inline traffic, and cloud apps, making it more difficult for ransomware to target and encrypt sensitive data.
- **Data loss prevention (DLP) controls** block unauthorized data transfers, backed by AI-based content inspection and policy enforcement, preventing ransomware operators from stealing sensitive data for extortion.

AS RANSOMWARE TACTICS EVOLVE, SO MUST DEFENSES. THE ZSCALER ZERO TRUST EXCHANGE IS INTEGRAL TO HELPING ORGANIZATIONS SHRINK THEIR ATTACK SURFACE, STOP NOVEL AND EVASIVE RANSOMWARE THREATS, PREVENT LATERAL MOVEMENT (EVEN POST-COMPROMISE), AND DISRUPT EXTORTION ATTEMPTS BEFORE DATA IS EXFILTRATED.

Ransomware Prevention_ Checklist

Zero trust is a must-have when it comes to stopping ransomware, but effective ransomware defense doesn't stop there. It also depends on broader operational layers, including employee training, secure backups, and a well-prepared response plan.

Based on insights from ThreatLabz experts, this checklist brings together the most effective steps you can take right now to reduce your ransomware risk and build lasting resilience.

Back up data regularly

- [ ] Maintain routine, encrypted backups, both online and offline.
- [ ] Test recovery procedures frequently and adapt backup strategies as ransomware tactics evolve.

Enforce multifactor authentication (MFA)

- [ ] Require MFA across all user accounts, especially for privileged access.
- [ ] Integrate with identity protection to detect and block account takeovers effectively.

Harden application security

- [ ] Remove applications from public exposure to prevent ransomware actors from exploiting vulnerabilities.
- [ ] Implement a zero trust architecture for internal apps to safeguard them against ransomware.

Keep software and systems up to date

- [ ] Apply the latest security patches promptly to close known vulnerabilities.
- [ ] Use AI-driven threat intelligence to prioritize patching based on real-world risk.

Standardize corporate security policies

- [ ] Ensure all users follow consistent security procedures, including MFA, software updates, and access controls.
- [ ] Adopt a security service edge (SSE) architecture to protect users, whether on-premises or remote.

Apply least-privileged access controls

- [ ] Implement least-privileged policies to limit users' access strictly to the data and systems required for their roles.
- [ ] Employ AI-powered solutions to dynamically analyze behavior and adjust privileges accordingly.

Strengthen identity protection

- [ ] Use ITDR tools to monitor for identity misconfigurations, remediate vulnerabilities in Active Directory that adversaries exploit to escalate privileges and move laterally, and detect stealthy identity threats.

Use AI-driven browser isolation

- [ ] Safely isolate user sessions from the web to prevent drive-by downloads, phishing, and credential theft.
- [ ] Let users access suspicious sites in a contained, read-only environment.

Leverage deception technology

- [ ] Set traps (e.g., honeypots, fake credentials) to detect, misdirect, and delay attackers early in the kill chain.
- [ ] Use alerts from deception systems to speed up incident response.

Provide ongoing employee training

- [ ] Regularly educate users on ransomware techniques, including phishing, social engineering, and fake software updates.
- [ ] Simulate real-world attack scenarios to enhance employee preparedness.

Inspect all traffic—especially encrypted

- [ ] 87% of threats hide in encrypted channels—inspect all traffic, encrypted or not, to uncover hidden threats and prevent compromise.

Deploy AI-powered sandboxing

- [ ] Detect and block evasive, never-before-seen malware using AI/ML-behavior-based analysis.
- [ ] Quarantine suspicious files before they reach endpoints.

Control SaaS access with a CASB

- [ ] Monitor and manage cloud app usage to block malicious activities like file downloads and data exfiltration.
- [ ] Enforce policies around data sharing and downloads.

Create a tested ransomware response plan

- [ ] Include procedures for data recovery, incident response, and communication protocols.
- [ ] Run regular tabletop exercises to evaluate readiness and close gaps.

Implement zero trust network access (ZTNA)

- [ ] Replace broad network access with precise, identity-based segmentation (user-to-app and app-to-app).
- [ ] Broker access via least-privileged access controls to prevent lateral movement and reduce attack surface.

Implement inline data loss prevention (DLP)

- [ ] Prevent data exfiltration and sensitive file transfers by deploying inline DLP measures.
- [ ] Apply policies across web, cloud, and email channels.

Research_ Methodology

The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The ThreatLabz team collected data between April 2024 and April 2025 from sources including:

- **The Zscaler global security cloud.** Zscaler's cloud processes more than 500 trillion daily signals, blocks more than 9 billion total threats and policy violations per day, and delivers 250,000+ daily security updates to Zscaler customers. We analyzed this data, which includes information about source IP addresses, destination IP addresses, and file types associated with ransomware attacks, to identify ransomware activity.
- **The ThreatLabz team's own analysis of ransomware samples and attack data.** ThreatLabz tracks ransomware families and threat actors along with corresponding attack telemetry. The team performs deep-dive reverse engineering to understand the tools used by initial access brokers as well as the ransomware itself, including the file encryption algorithms. In a number of cases, the team has discovered cryptographic flaws that can be exploited to decrypt files without paying a ransom, and created decryption tools. The team provides these tools to international law enforcement agencies to offer to victims free of charge. ThreatLabz also has built a proprietary malware automation platform that can automatically detect and stop threats in Zscaler's cloud.
- **External intelligence sources.** We also compiled and compared our own data with open source research where applicable.

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, **research.zscaler.com**.

***Follow Zscaler ThreatLabz* for regular insights on the latest ransomware threats and developments, including published indicators of compromise (IOCs) and MITRE ATT&CK mappings. This information can be used to train your team, improve your security posture, and help prevent ransomware attacks.**

ThreatLabz also maintains GitHub repositories with IOCs, tools (including proof-of-concept ransomware decryption tools), and an archive of ransomware notes from all major ransomware groups.

X @ThreatLabz

ThreatLabz security research blog

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.

zscaler™ | Zero Trust Everywhere

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**