zscaler™

ThreatLabz 2024_Ransomware Report

Table_of Contents

Executive Summary_

Ransomware attacks have reached new heights of ambition and audacity over the past year, marked by a notable surge in extortion attacks. Adding to the increase in ransomware attacks, ThreatLabz research uncovered an unprecedented ransom payout of US$75 million—the largest ever paid by one company. This amount is nearly double the highest publicly known ransom payment.[1] In 2023 alone, ransomware payments exceeded $1 billion, highlighting the escalating financial impact of these cybercrimes.

Ransomware threat actors' tactics have become increasingly sophisticated and bold. Notably, they have surpassed the traditional boundaries of the corporations they attack, even going so far as to target the children of executives to provoke faster and higher ransoms.[2] From critical infrastructure[3] and major corporations[4] to small and medium-sized enterprises, no organization is immune to finding themselves in the crosshairs of the next campaign or evolution of attacks.

Despite law enforcement takedowns of multiple initial access brokers under special ops "Operation Endgame" and "Operation Duck Hunt," many of the largest active ransomware families continue to rapidly regroup and launch new attacks while barely skipping a beat. Unfortunately, many ransomware actors are beyond the reach of law enforcement, making them virtually immune to criminal prosecution. As detailed in this report, law enforcement agencies have augmented their pressure tactics through reward money, sanctions, trolling, and exposing the individuals behind ransomware using various forms of psychological tactics.

As ransomware actors continuously evolve their tactics, it is crucial to stay up to date on how the threat landscape is changing.

The Zscaler ThreatLabz 2024 Ransomware Report offers an overview of the ransomware threat landscape from April 2023 through April 2024, detailing the latest trends, targets, ransomware families, and effective defense strategies.

ThreatLabz found that ransomware attacks increased by 17.8% year-over-year based on blocked attempts in the Zscaler cloud, while ransomware attacks identified through data leak site analysis surged by 57.8%. The most common targets were businesses in the manufacturing, healthcare, and technology sectors, putting critical operations and infrastructure squarely in the line of attack.

The findings presented in this report underscore the need for organizations to prioritize protection against the relentless tide of ransomware. The insights and strategies in the report serve as a crucial guide for improving your ransomware defenses. By understanding the latest trends and vulnerabilities, and implementing recommended best practices, you can significantly reduce the risk of becoming a ransomware victim and better protect your organization's critical assets and data.

[1] Bloomberg, **CNA Financial Paid $40 Million in Ransom After March Cyberattack**, May 20, 2021.
[2] Business Insider, **Hackers are now targeting the children of corporate executives in ransomware attacks**, May 12, 2024.
[3] Dark Reading, **Ascension Healthcare Suffers Major Cyberattack**, May 10, 2024.
[4] CyberScoop, **Boeing confirms attempted $200 million ransomware extortion attempt**, May 8, 2024.

Key_ Findings

Zscaler ThreatLabz research uncovered a record-breaking ransom payment of US$75 million —the largest ransomware payment by a company in history—nearly double the highest publicly known payout.

Ransomware attacks blocked by the Zscaler cloud increased by 17.8%, and the number of extorted companies on data leak sites grew by 57.8% in the same period year-over-year despite numerous law enforcement operations, including the seizure of infrastructure along with arrests, criminal indictments, and sanctions.

The manufacturing, healthcare, and technology sectors were the top targets of ransomware attacks, while the energy sector experienced a 500% year-over-year spike as critical infrastructure and susceptibility to operational disruptions make it particularly attractive to cybercriminals.

The United States remains the top target of ransomware, experiencing 49.95% of overall attacks, followed by the United Kingdom, Germany, Canada, and France.

ThreatLabz identified 19 new ransomware families during the analysis period, bringing the total number to 391 since our tracking started.

The most active ransomware families were **LockBit (22.1%)**, **BlackCat (a.k.a. ALPHV) (9.2%)**, and **8Base (7.9%)**.

Vulnerabilities remain an all-too-common ransomware attack vector, emphasizing the importance of timely patching and unified vulnerability management, underpinned by a zero trust architecture to provide protection even when patches are not available.

Voice-based social engineering attacks are increasingly being used to gain access to corporate networks—a technique used by Scattered Spider and the Qakbot threat group.

Ransomware_Landscape: Top Trends and Targets

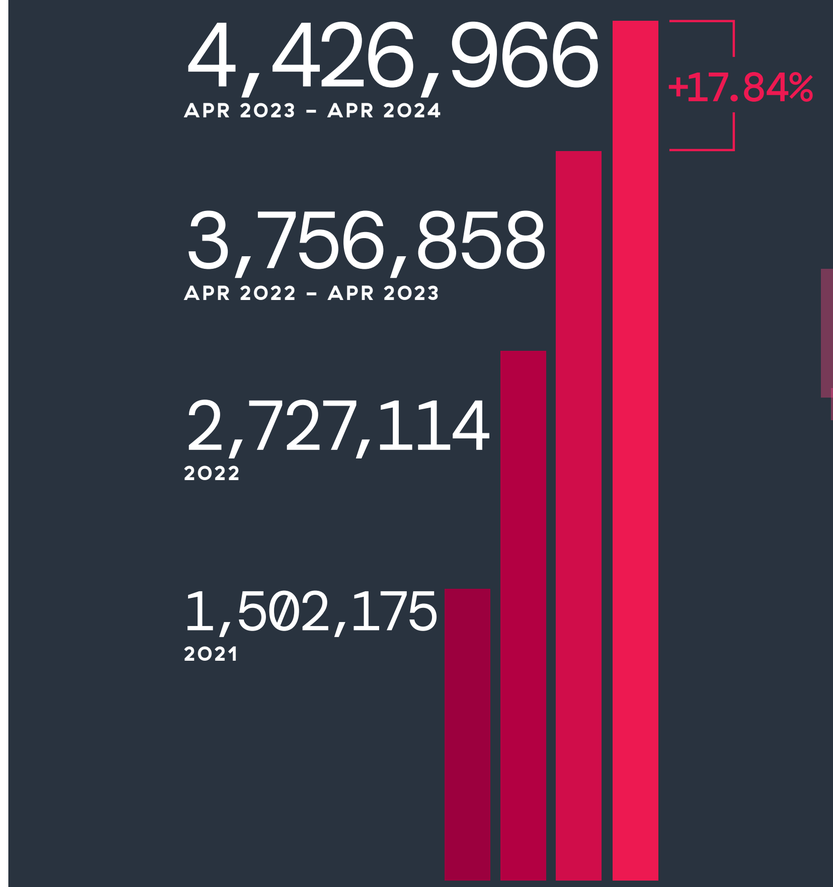
The dynamic nature of ransomware has placed it at the forefront of security concerns in recent years. Threat actors are constantly evolving their methods of attack and extortion, leveraging advances in artificial intelligence (AI) technology, leaked source code, and advanced encryption to maximize their impact and profitability.

This report examines the following ransomware attack trends from April 2023 through April 2024:

- Overall rise in ransomware attacks
- Industry verticals most impacted by ransomware
- Geographical distribution of victim organizations
- Increased law enforcement action against ransomware groups and initial access brokers
- Top ransomware threats and record-breaking ransom payments

Overall rise in ransomware attacks

The latest ThreatLabz analysis reveals a concerning trend, with a 17.84% year-over-year increase in ransomware attacks based on blocked attempts observed across the Zscaler cloud. The rise in ransomware activity translates to significant disruptions and financial impacts to victim organizations of all sizes. These attacks often disrupt business operations, causing extended downtime, substantial data loss, and high recovery costs. The financial burden is considerable; not only is there a ransom demand at play, but system restoration and damage control can come at a hefty price. In light of these escalating threats, the need for **robust ransomware defense measures** has never been greater.



Industry verticals most impacted by ransomware

Ransomware attacks pose significant risks to businesses of all sizes and industries. These attacks can compromise sensitive data, lead to heavy financial losses, disrupt business continuity, and damage reputations. Different industries face unique ransomware challenges based on how they operate, the data they handle, and their technological infrastructure.

Despite the variables, ransomware extortion attacks have consistently surged, with the number of victim companies listed on data leak sites increasing by 57.81% since last year's ThreatLabz report on ransomware trends. The manufacturing industry was by far the most targeted industry, accounting for 653 attacks—more than two times as many as any other industry.

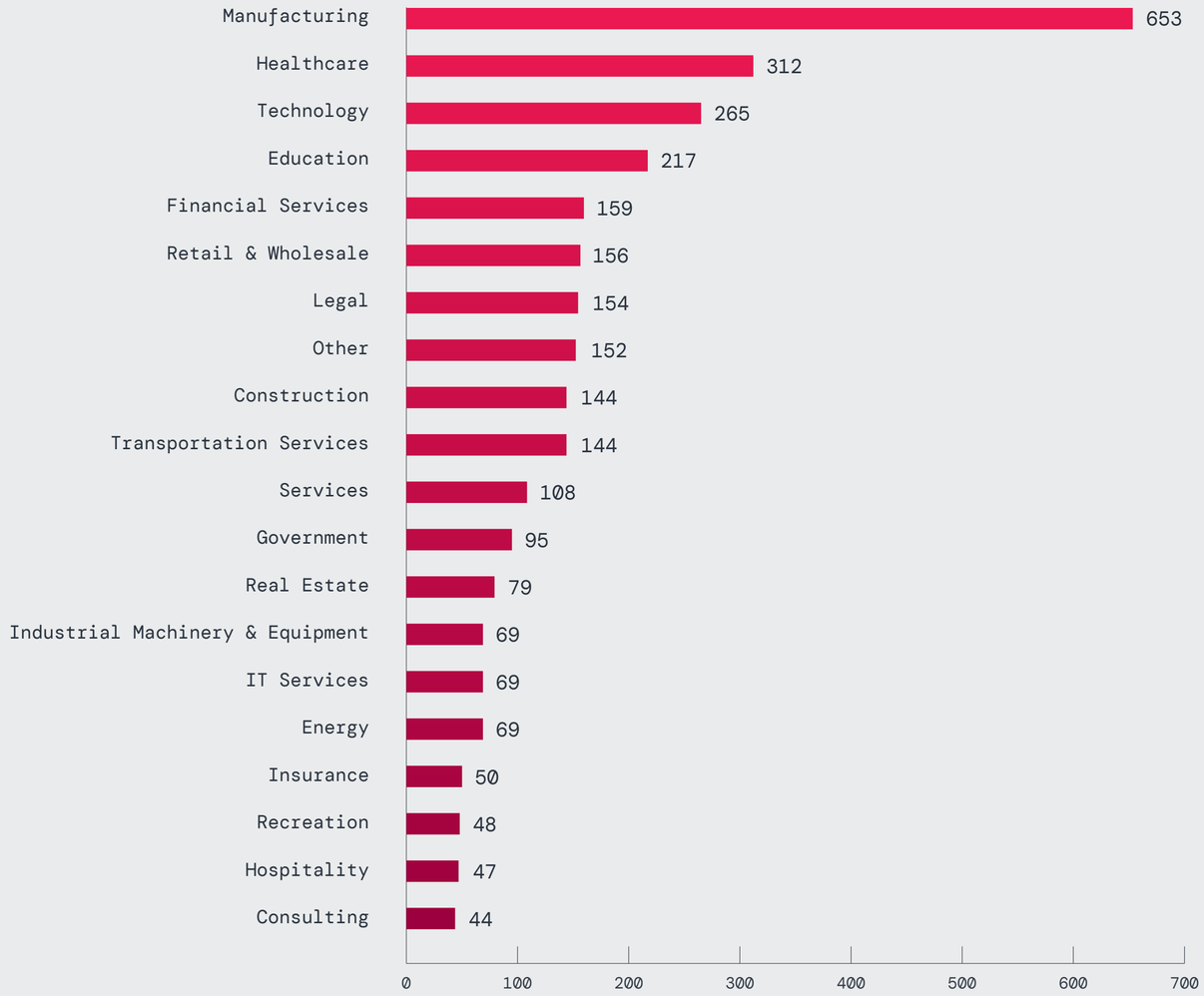


Figure 1: Ransomware attacks by industry based on data leak sites (top 20 industries only).

Year-over-year trends

The energy sector experienced a 527.27% year-over-year increase in ransomware attacks, likely due to its critical nature and the high ransom potential it offers to attackers.

Similarly, the restaurants, bars, and food services industry saw a 333.33% rise in such attacks. This may be attributed to the sector's rapid digitization, driven by the adoption of advanced point-of-sales systems and online ordering platforms. While these technologies may streamline operations and improve customer experiences, they can also introduce potential vulnerabilities.

While this rise highlights the prevalence of ransomware attacks, it may not capture the full extent of ransomware incidents. Many attacks go unreported or are resolved privately through ransom payments without public disclosure. Thus, these figures should be seen as indicative of broader ransomware trends rather than a comprehensive representation of the entire threat landscape.

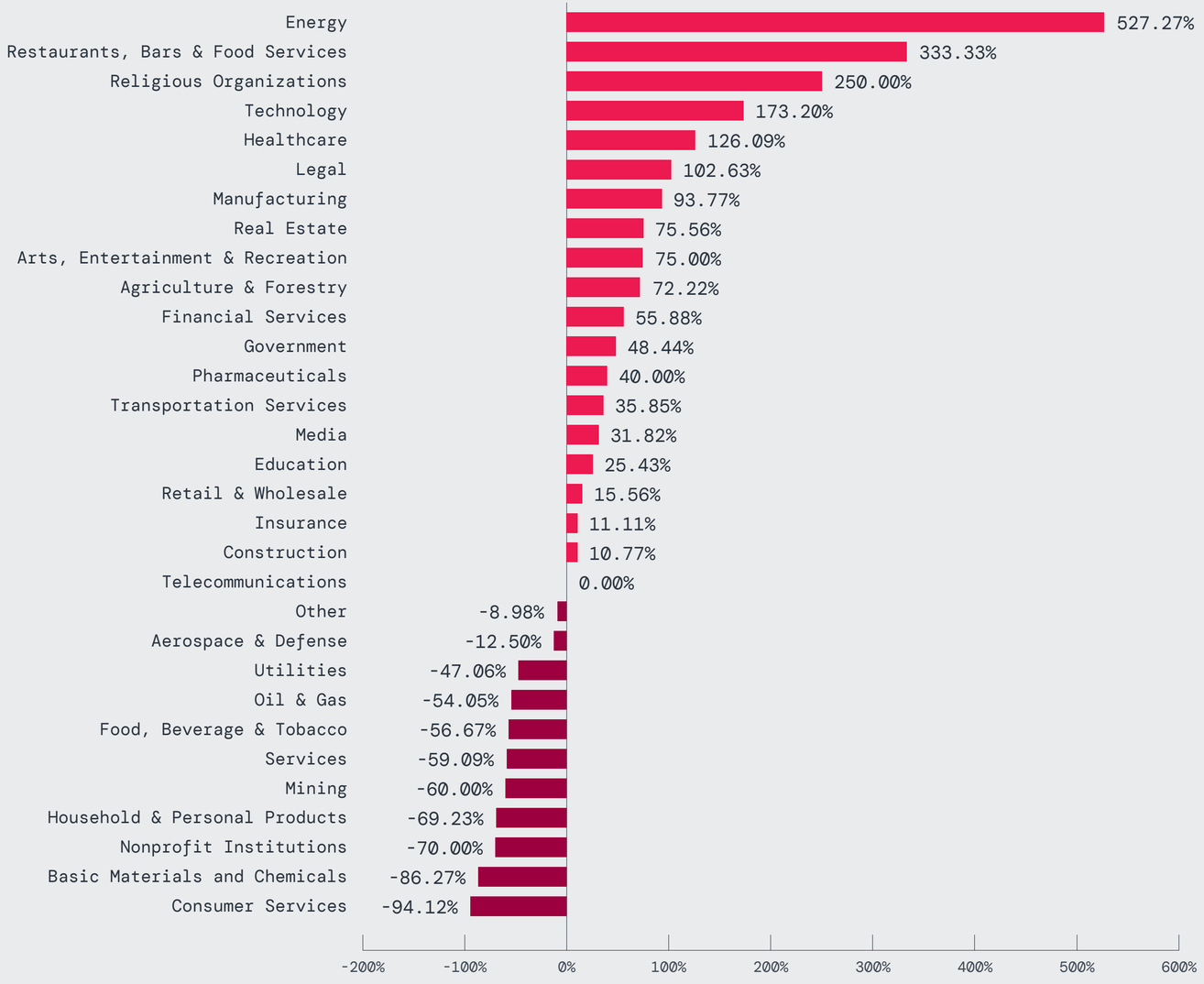


Figure 2: Year-over-year percentage change in ransomware extortion attacks by industry. Note that some sectors had a relatively low baseline of attacks in last year's report, making their growth appear more substantial.

Geographical distribution of victim organizations

The United States faced a markedly higher volume of ransomware attacks than any other country, accounting for about 50% of all incidents globally. In comparison, the United Kingdom was the second-most targeted nation, experiencing nearly 6% of ransomware attacks, followed by Germany (4.09%), Canada (3.51%), and France (3.26%). Figure 3 shows a heatmap illustrating countries impacted by ransom extortions between April 2023 and April 2024.

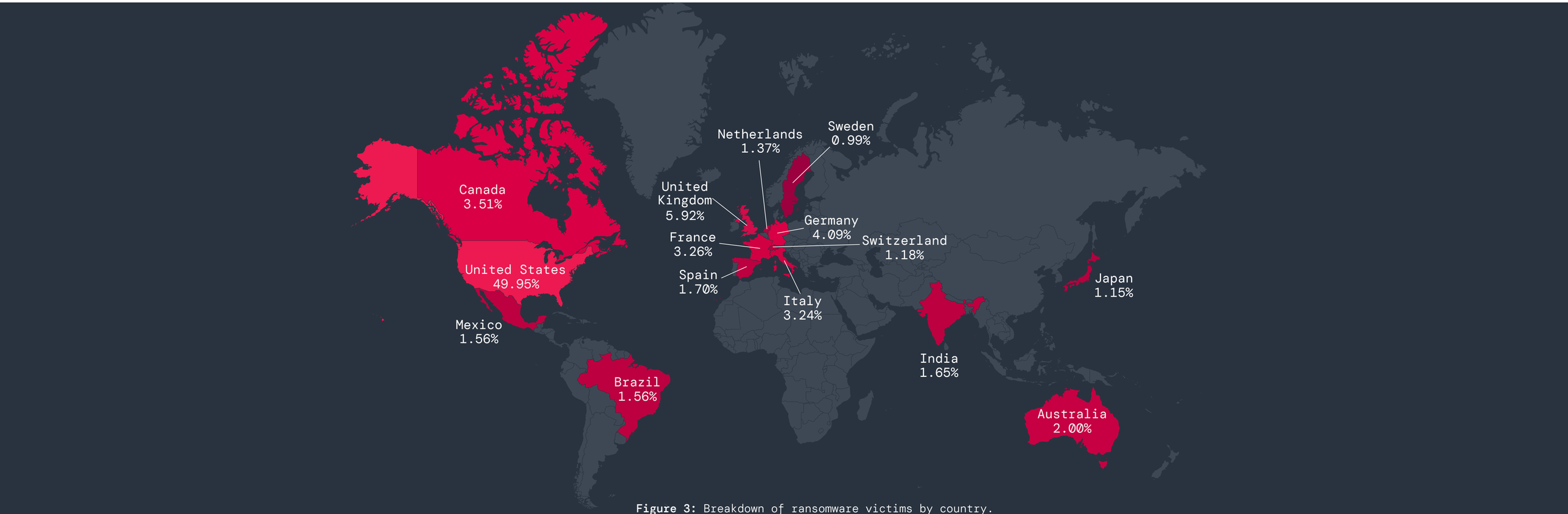


Figure 3: Breakdown of ransomware victims by country.

Understanding the distribution of ransomware attacks is essential for risk assessment, resource allocation, policy development, international cooperation, and public awareness efforts in combating ransomware threats.

Risk assessment

Analyzing heavily targeted regions helps organizations in those areas to assess their own risk levels and implement stronger cybersecurity. In ThreatLabz research, the US accounts for 50% of global ransomware attacks, calling for organizations within its borders to prioritize stringent security protocols.

Resource allocation

Targeted data enables governments and organizations to strategically allocate resources, enhancing their security posture by prioritizing support, funding, and expertise in areas with the highest threat levels.

Policy development

Governments can use insights from regional ransomware attacks to inform legislation, improve security standards, promote international cooperation, and facilitate public–private sector information sharing. As a recent notable example, the SEC's new cybersecurity rules mark a major step in enhancing transparency and accountability amid growing threats.

International cooperation

Identifying the most targeted countries allows coordinated efforts between law enforcement, organizations, and governments to combat ransomware at the national and international levels. Operation Duck Hunt and Operation Endgame exemplify how international cooperation can disrupt cybercriminal activities.

Public awareness

Highlighting frequently targeted countries may urge individuals, organizations, and governments to take more proactive measures when it comes to cybersecurity training, incident response planning, and investment in defensive technologies.

Year-over-year trends

ThreatLabz compared ransomware attacks from this year's report with the ThreatLabz 2023 Ransomware Report to assess rates of change. Among the top 15 most targeted countries, the US experienced a notable year-over-year increase of 101.88%, and Sweden saw a staggering 350% rise, although it accounted for a significantly smaller share of the total attacks.

While analyzing ransomware trends at a global level is invaluable, it is also important to examine the specific developments in different regions of the world. Studying regional breakdowns helps organizations create tailored security plans and aid governments in developing more effective cybersecurity policies.

CHANGES IN RANSOMWARE ATTACKS ACROSS TOP 15 TARGETED COUNTRIES

Country	Ransomware attacks by country (2023)	Ransomware attacks by country (2024)	Percentage change
United States of America	902	1,821	101.88%
United Kingdom	144	216	50.00%
Germany	110	149	35.45%
Canada	151	128	-15.23%
France	87	119	36.78%
Italy	63	118	87.30%
Australia	69	73	5.80%
Brazil	38	57	50.00%
Spain	36	62	72.22%
Mexico	31	57	83.87%
Netherlands	17	50	194.12%
India	62	60	-3.23%
Switzerland	32	43	34.38%
Japan	44	42	-4.55%
Sweden	8	36	350.00%

Figure 5: Year-over-year comparison of ransomware attacks by country.

CHANGES IN RANSOMWARE ATTACK RATES ACROSS EMEA

Country	Companies impacted by ransomware attacks (2023)	Companies impacted by ransomware attacks (2024)	Percentage change
United Kingdom	144	216	50.00%
Germany	110	149	35.45%
France	87	119	36.78%
Italy	63	118	87.30%
Spain	36	62	72.22%
Netherlands	17	50	194.12%
Switzerland	32	43	34.38%
Sweden	8	36	350.00%
Belgium	16	34	112.50%
South Africa	13	24	84.62%
Austria	15	24	60.00%
United Arab Emirates	12	21	75.00%

Figure 6: Year-over-year comparison of ransomware attacks by country in the EMEA region.

CHANGES IN RANSOMWARE ATTACK RATES ACROSS APAC

Country	Companies impacted by ransomware attacks (2023)	Companies impacted by ransomware attacks (2024)	Percentage change
Australia	69	73	5.80%
India	62	60	-3.23%
Japan	44	42	-4.55%
Thailand	13	25	92.31%
Indonesia	15	23	53.33%
Malaysia	14	20	42.86%
Taiwan	23	17	-26.09%
Philippines	7	16	128.57%
Singapore	8	16	100.00%
China	21	15	-28.57%
South Korea	12	10	-16.67%
Vietnam	10	10	0.00%

Figure 7: Year-over-year comparison of ransomware attacks by country in the APAC region.

Most active ransomware groups in 2023-2024

LockBit (22.1%), BlackCat (9.2%), and 8Base (7.9%) were the most active ransomware extortion groups over the past year, each responsible for a significant number of attacks. Figure 8 shows the number of data leak victims per ransomware family during this period.

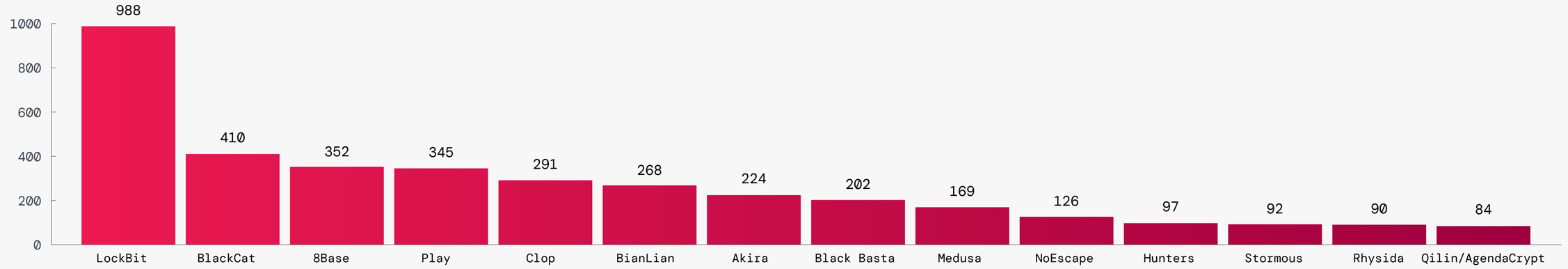


Figure 8: Ransomware attacks revealed on maliciously operated data leak websites.

Newest ransomware groups on the scene

Figure 9 showcases a timeline of new ransomware groups that began publishing data on leak sites as part of their extortion strategy.

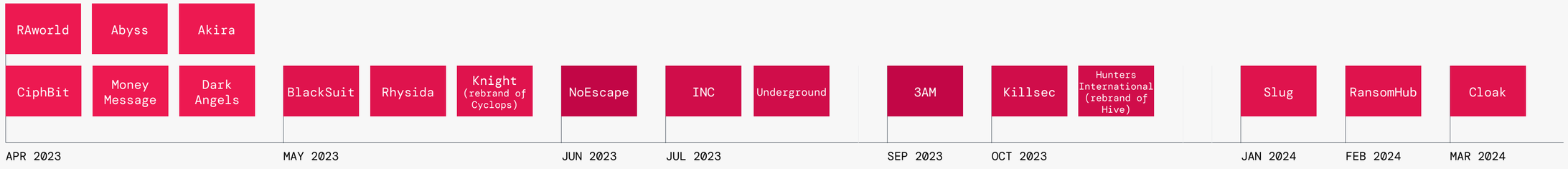


Figure 9: New ransomware groups with data leak sites.

Major vulnerabilities used in ransomware attacks

Vulnerabilities in software, systems, and the overall digital infrastructure can serve as critical entry points for ransomware attacks. Organizations must be aware of these vulnerabilities and take proactive measures to address them.

The Cybersecurity & Infrastructure Security Agency (CISA) maintains a comprehensive list of vulnerabilities,[5] including those actively exploited by ransomware groups. It is highly recommended that organizations closely monitor this list and prioritize the mitigation of vulnerabilities mentioned therein. Proactive vulnerability management is essential for strengthening the overall cybersecurity posture of an organization.

In many cases, the vulnerabilities exploited by ransomware groups impact internet–connected assets in organizations' external attack surface, such as gateways, VPNs, and other remote connectivity technologies. Because they are internet–facing, these vulnerabilities are significantly easier for threat actors to scan for and exploit. CISA's latest guidance[6] further emphasizes vulnerabilities in VPNs and remote connectivity solutions as critical points of concern, advising the adoption of the most current approaches, such as zero trust architecture, SSE, and SASE, which are based on granular access control policies.

Over the past year, prominent ransomware families have targeted and exploited the vulnerabilities shown in figure 10, significantly impacting a wide range of systems.

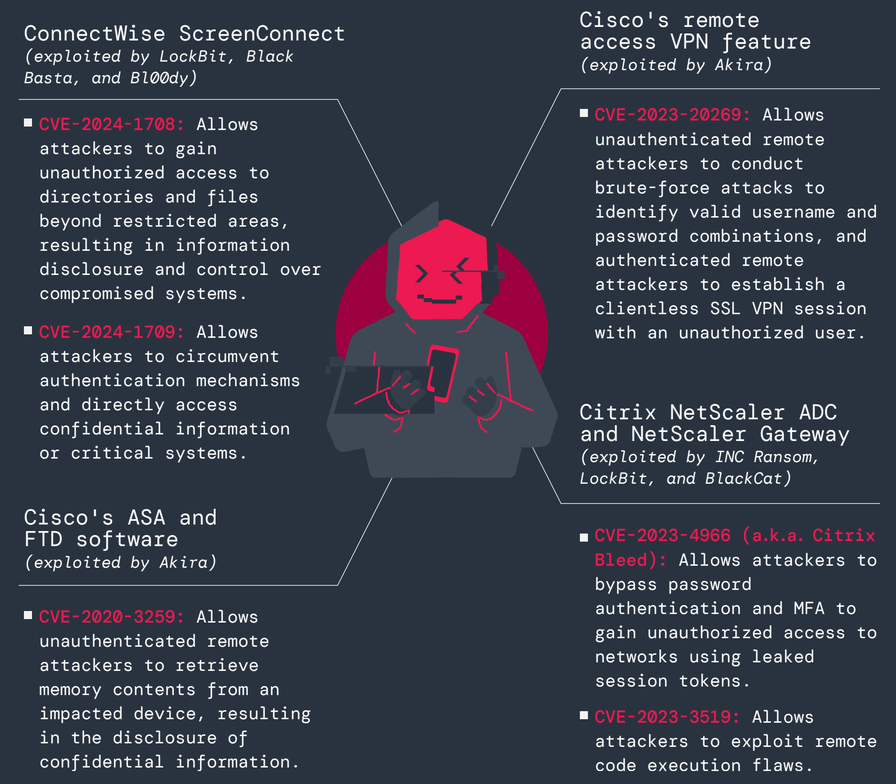


Figure 10: Prevalent vulnerabilities from April 2023-April 2024.

Available patches for these vulnerabilities should be applied as soon as possible, along with the following mitigation measures:

- Disable remote access to servers
- Use strong passwords and multifactor authentication
- Monitor servers for suspicious activity

[5] Cybersecurity & Infrastructure Security Agency, **Known Exploited Vulnerabilities Catalog**, accessed June 25, 2024.
[6] Cybersecurity & Infrastructure Security Agency, **Modern Approaches to Network Access Security**, June 18, 2024.

Ransomware_Roundup: What's Making Headlines

Ransomware is pervasive and transcends industries—and when one group is shut down, another is reborn or emerges anew. Here are some recent stories highlighting the ever-evolving ransomware landscape.

The ransomware plague in healthcare

The healthcare industry faced significant challenges throughout 2023 and into 2024 as it was heavily targeted by ransomware groups. The repercussions of disrupting healthcare operations are serious: ambulances get rerouted, prescriptions are delayed, and essential medical procedures have to be postponed. Moreover, the theft of sensitive health data can have far-reaching consequences, including identity theft and healthcare fraud, further exacerbating vulnerabilities in the healthcare ecosystem.

UNFORESEEN CONSEQUENCES OF RANSOM PAYMENTS

A healthcare technology provider for payment solutions fell victim to a ransomware attack orchestrated by the BlackCat group. Despite complying with the attackers' demands and paying a staggering $22 million ransom, the ordeal took an unexpected turn. BlackCat reneged on their promise to share a portion of the ransom with the affiliate behind the attack (a so-called "exit scam"), prompting the affiliate to threaten the healthcare provider with the release of sensitive data.

This is a stark reminder that the old adage "there is no honor among thieves" holds true for ransomware attacks. Even if ransoms are paid, there is no guarantee that the threat group will not still post or delete stolen data. In addition, some ransomware decryption tools contain bugs that prevent successful data recovery, and may take longer to recover data than from a backup.

DOUBLE EXTORTION, DOUBLE VICTIMIZATION

In February 2023, a prominent US pharmaceutical distributor confirmed that their IT systems had been compromised. The breach affected one of the distributor's subsidiaries, with the stolen files later leaked by the Lorenz ransomware group.[7] Then, in February 2024, the same distributor faced another ransomware attack.[8] This appears to be part of a growing trend ThreatLabz has observed, where a company has been subject to multiple ransomware incidents within one year.

[7] BleepingComputer, **Drug distributor AmerisourceBergen confirms security breach**, February 8, 2023.
[8] BleepingComputer, **Pharmaceutical giant Cencora says data was stolen in a cyberattack**, February 27, 2024.

The impact of the SEC's cybersecurity ruling

In 2023, the SEC introduced new cybersecurity disclosure rules to enhance transparency and accountability among publicly traded companies. Effective December 15, 2023, these rules mandate the timely reporting of material cybersecurity incidents and require detailed information about a company's cybersecurity risk management, strategy, and governance. Key components of the SEC rulings include the addition of Item 1.05 to for 8-K, which necessitates reporting of material cybersecurity incidents within four business days of the company's determination of materiality. Additionally, Form 10-K now requires annual reporting on cybersecurity risk management and strategy, starting with fiscal years ending on or after December 15, 2023. Foreign private issuers must also comply with comparable disclosures on Form 6-K and Form 20-K.

The rulings present a new challenge for ransomware actors offering publicly traded companies private payment resolution services, as the companies are now still required to fully disclose the attack. On the positive side, the new mandate undercuts encryptionless extortion attacks, an emerging trend by which ransomware actors rely solely on the threat of leaking stolen data to demand ransoms.

HOW THE NEW RULES IMPACT COMPANIES

The SEC's cybersecurity rulings can pose serious challenges for companies in terms of compliance and risk management. While intended to enhance transparency and investor protection, these rules require companies to navigate complex reporting requirements and provide prompt disclosure of material incidents.

One major impact is the increased pressure on companies to quantify and assess cyber incidents accurately. Determining materiality and the potential impact of cyber incidents requires careful analysis, which can be costly and may require companies (big and small) to rethink their incident response protocols and update their disclosures to meet the SEC's requirements.

Moreover, compliance timelines vary based on the size and reporting status of companies, adding another layer of complexity. Smaller reporting companies often have different, and typically longer, compliance deadlines compared to larger corporations. And while larger corporations must adhere to tighter deadlines, their scale also affords them more resources to analyze the materiality of a cybersecurity incident.

The new disclosure requirements also eliminate the possibility for public companies to pay ransoms quietly without incurring reputational damage and the backlash that follows after openly sharing information about a breach.

SOME COMPANIES ARE ALREADY IN VIOLATION OF THE SEC'S RULES

Despite the SEC's clear guidelines, some companies have already fallen short of compliance with the new cybersecurity rules. Recent disclosures from well-known companies have raised concerns about noncompliance and the adequacy of their incident reporting.[9] Many of these disclosures lack quantitative data and detailed assessments of the financial and operational implications of the cyber incidents, which is precisely what the SEC now mandates. This trend, where companies provide deficient cyber incident disclosures despite the SEC ruling, may call for enhanced guidance and regulatory oversight to ensure consistent and effective compliance.

The SEC's cybersecurity rulings represent a significant regulatory shift aimed at improving transparency and accountability in incident reporting. Adhering to these new rules consistently and in good faith will require ongoing collaboration between regulators, companies, and industry stakeholders.

[9] Forbes, **Companies Are Already Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**, March 4, 2024.

Impact of law enforcement actions

Qakbot disrupted by “Operation Duck Hunt”

On August 29, 2023, in a coordinated multinational effort, the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) announced Operation Duck Hunt. Zscaler ThreatLabz provided significant technical assistance to law enforcement for this operation.[10] Qakbot’s infrastructure was designed to be resilient against takedown attempts through a multi-tiered infrastructure, as shown in figure 11.

This infrastructure provided several layers of resiliency, with each tier requiring a coordinated effort to dismantle. The first tier of Qakbot’s infrastructure included infected systems running a supernode plugin that relayed traffic upstream to several proxies designed to hide the master Qakbot backend server.

Operation Duck Hunt redirected the supernode’s upstream proxy servers to a set of sinkhole servers to immediately take over Qakbot’s infrastructure as shown in figure 12.

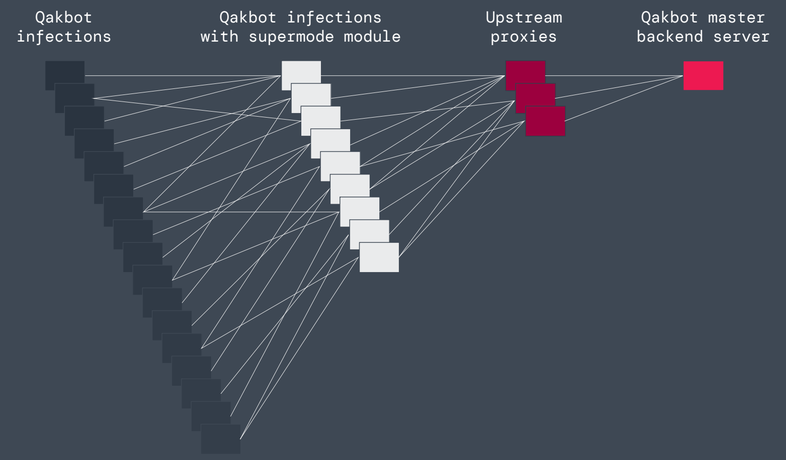


Figure 11: Qakbot’s multi-tiered infrastructure.

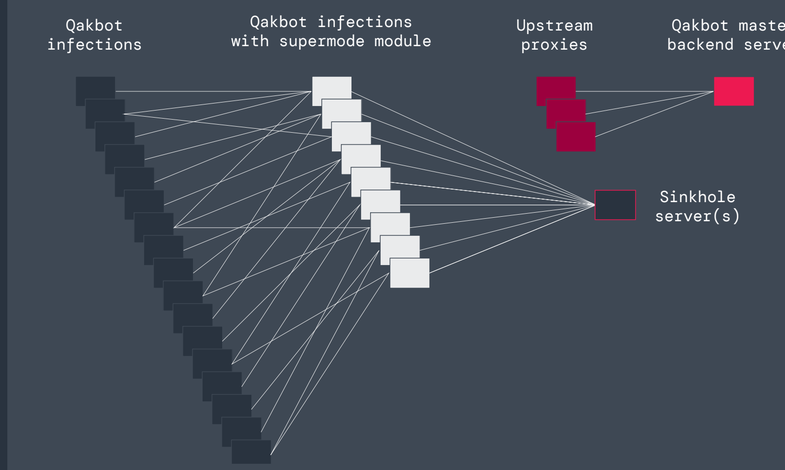


Figure 12: Qakbot architecture after redirecting each supernode’s upstream proxies.

Once the FBI hijacked the supernodes, the sinkhole servers instructed victim computers to download shellcode that reflectively loaded a DLL that neutralized the malware. This successfully disinfected the victim computers and prevented further attacks.

At the time of the takedown, Qakbot had infected more than 700,000 computers worldwide, including more than 200,000 in the United States alone.[11] Prior to this operation, Qakbot was active for nearly 15 years, originally designed to facilitate credit card and wire fraud. In 2019, the group pivoted to serving as an initial access broker for ransomware groups including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta.

Qakbot malware was typically distributed through spam emails containing malicious attachments or links. Once infected, Cobalt Strike was frequently deployed for lateral movement and the eventual deployment of ransomware.

Unfortunately, there were no arrests or unsealed indictments against any of the threat actors, and Qakbot resurfaced in December 2023. The group updated the malware to support 64-bit versions of Windows, changed the internal configuration format, and modified the network communication to use AES encryption. As we will discuss later in the report, the Qakbot threat actor has significantly changed their TTPs since Operation Duck Hunt.

[10] US Department of Justice, Qakbot Malware Disrupted in International Cyber Takedown, August 29, 2023.
[11] TechCrunch, How the FBI took down the notorious Qakbot botnet, September 1, 2023.

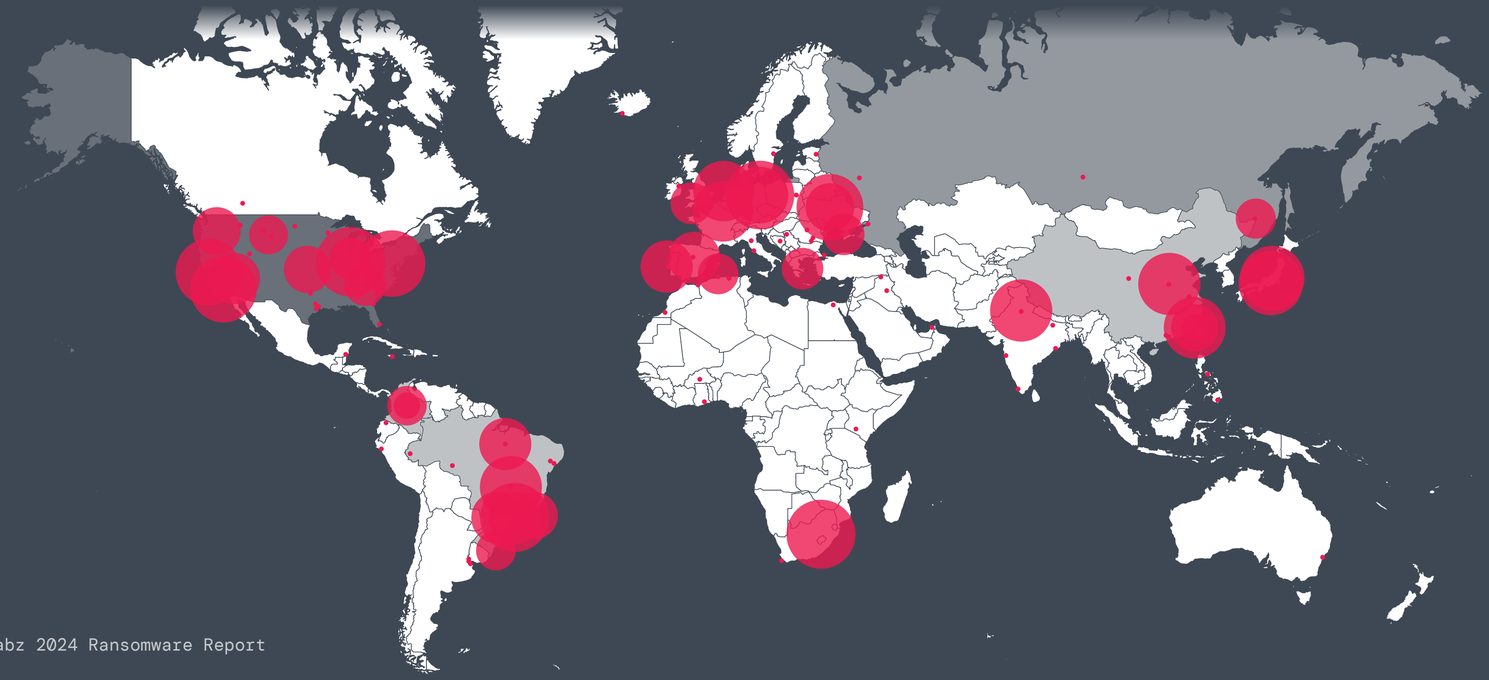
“Operation Endgame” simultaneously targeted multiple initial access brokers

On May 28, 2024, in collaboration with numerous international law enforcement agencies, Europol announced Operation Endgame, which simultaneously targeted multiple initial access brokers. This led to more than a dozen global searches, several arrests, and the shutdown of more than 100 servers used for criminal activity. These servers were integral to the operations of various malware downloaders (a.k.a. “loaders”) that had been used to infiltrate victims’ computers, deploying malicious software including ransomware.

The malware families targeted in this operation were responsible for infecting millions of computers around the globe, including in healthcare facilities and critical infrastructure services. As part of the operation, action was taken against SmokeLoader, Pikabot, Bumblebee, and IcedID.

Zscaler ThreatLabz provided critical technical assistance for Operation Endgame’s SmokeLoader sinkhole and remediation efforts.

SmokeLoader, active since 2011, was used by several initial access brokers for ransomware, including Raspberry Robin and the Stop (a.k.a. DJVU) ransomware gang. Operation Endgame seized more than 1,000 SmokeLoader domains used by these threat groups. The domains were then redirected to a sinkhole server controlled by law enforcement. The map in figure 13 depicts infected systems that communicated with the SmokeLoader sinkhole.



This map demonstrates the far-reaching impact that SmokeLoader had around the world, with significant infections in Latin America, Asia, North America, and Europe.

Figure 13: Map of SmokeLoader infections communicating with the Operation Endgame sinkhole. (Source: Zscaler ThreatLabz)

When systems infected with SmokeLoader connected to the sinkhole server, they received the malware's own built-in uninstall command. To date, more than 40,000 systems infected with SmokeLoader have been cleaned, as shown in figure 14.

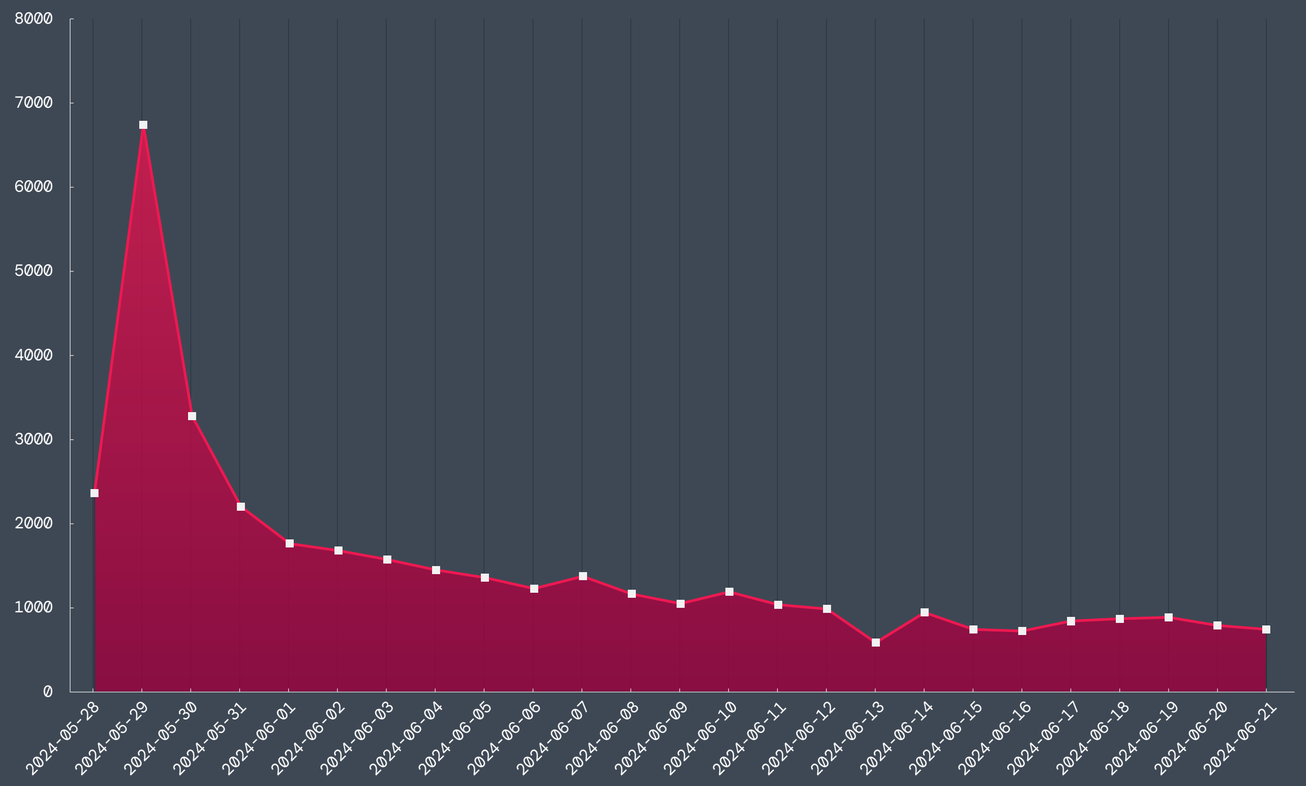


Figure 14: SmokeLoader systems cleaned by Operation Endgame.

Pikabot originally emerged in early 2023 and exhibited significant activity in the latter half of the year. This increase was due to the malware becoming the initial access broker of choice for Black Basta ransomware after Operation Duck Hunt disrupted Qakbot. In February 2024, **Pikabot reemerged with significant changes** in its code base and structure. Pikabot was observed by ThreatLabz regularly deploying **Cobalt Strike** and Metasploit's **Meterpreter**.

Bumblebee was introduced in March 2022 and had ties to the former Conti ransomware group. The malware was the successor to the group's BazarLoader malware tool, which they used for initial access for Conti and Diavol ransomware attacks. ThreatLabz frequently observed both BazarLoader and Bumblebee deploying Cobalt Strike payloads for lateral movement. Bumblebee has also been associated with Akira and Black Basta ransomware attacks.

Similar to Qakbot, IcedID was originally designed as a banking trojan when it appeared in 2017. However, the group later shifted their focus to serving as an initial access broker for ransomware. Over the years, the malware code for IcedID has been forked and modified for various purposes. In addition, the same developers created a new malware loader known as Latrodectus, released in November 2023, which was also likely used to deploy ransomware.

Following Operation Endgame, there has been minimal activity for most of these initial access brokers **with the exception of Latrodectus**, which resurfaced in less than a month. However, the lull is likely to be short-lived as the threat actors regroup.

Hive ransomware reborn as Hunters International

In January 2023, the Hive ransomware group's infrastructure was shut down. After a seven-month covert operation, the FBI successfully infiltrated Hive's servers, recovering more than 300 decryption keys that prevented approximately $130 million in ransom payments. Operating since June 2021, the Hive collective targeted and victimized more than 1,500 organizations worldwide, amassing over $100 million in ransom payments.[12] Victims included hospitals, school districts, financial institutions, and various other entities. However, no arrests associated with Hive were made, and the group rebranded as Hunters International in October 2023. Cybercriminals often use this rebranding strategy after a major disruption.

The group made one noticeable change to their operation: they will no longer offer discounts or negotiate with victims from the initial ransom demand, as shown in figure 15.

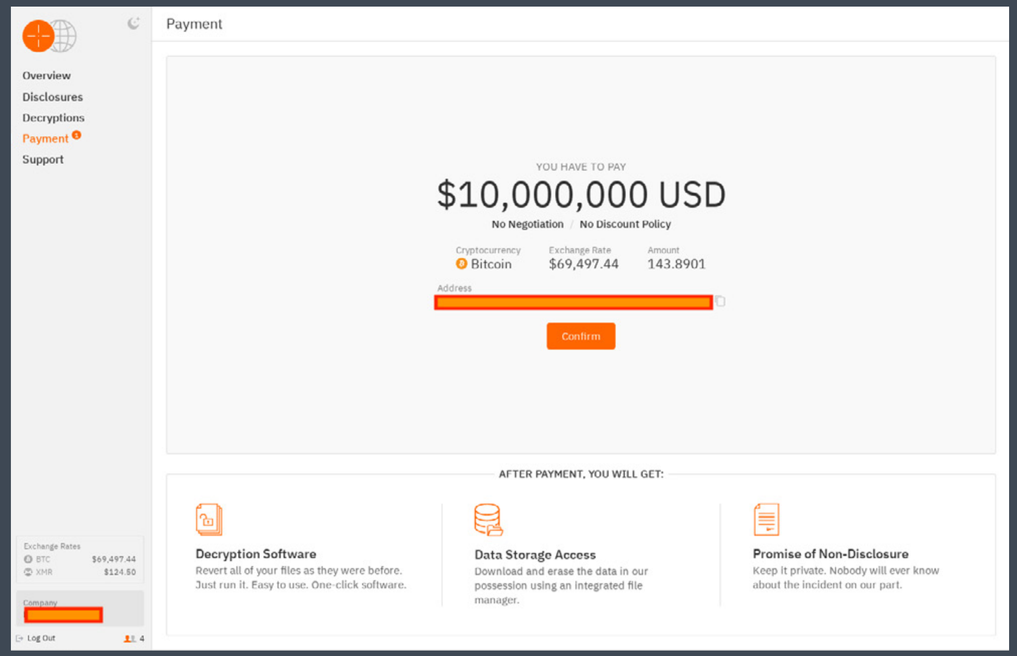


Figure 15: Hunters International victim portal with no price discounts or negotiations.

The non-negotiable price policy is **very uncommon** with ransomware groups, which frequently offer significant discounts from the original ransom demand. This decision by the Hunters team will likely lead to lower overall payment volume, but higher overall payment amounts.

Hunters International continues to launch new attacks and is likely to remain a formidable threat without further arrests and criminal indictments.

[12] US Department of Justice, U.S. Department of Justice Disrupts Hive Ransomware Variant, January 26, 2023.

Top 5 Ransomware_Families to Watch in 2024-2025

As ransomware and other cyberthreats continue to evolve in complexity and sophistication, staying informed about the most prevalent and dangerous ransomware families is crucial for maintaining an effective security posture. This section highlights five ransomware families that pose some of the most significant risks to businesses, providing insights into their tactics, potential impact, and recent activity.

#1 Dark Angels

The Dark Angels ransomware group, which operates the Dunghill data leak site, emerged around May 2022. The group has conducted some of the largest ransomware attacks, yet has managed to attract very minimal attention. In early 2024, ThreatLabz uncovered a victim who paid Dark Angels $75 million, higher than any publicly known amount—an achievement that's bound to attract the interest of other attackers looking to replicate such success by adopting their key tactics (which we describe below). Dark Angels targets various industries, including healthcare, government, finance, and education. More recently, they have been observed launching attacks against large industrial, technology, and telecommunication companies.

The Dark Angels group employs a highly targeted approach, typically attacking a single large company at a time. This is in stark contrast to most ransomware groups, which target victims indiscriminately and outsource most of the attack to affiliate networks of initial access brokers and penetration testing teams. Once Dark Angels have identified and compromised a target, they selectively decide whether to encrypt the company's files. In most cases, the Dark Angels group steals a vast amount of information, typically in the range of 1–10 TB. For large businesses, the group has exfiltrated between 10–100 TB of data, which can take days to weeks to transfer.

The highest-profile attack conducted by Dark Angels was in September 2023, when the group breached an international conglomerate that provides solutions for building automation systems among other services. Dark Angels demanded a $51 million ransom, claimed to have stolen over 27 TB of corporate data, and encrypted the company's VMware ESXi virtual machines. A RagnarLocker ransomware variant was used to encrypt the company's files during the attack. The relationship between RagnarLocker and Dark Angels is not clear, but the group was using the ransomware prior to the law enforcement action against RagnarLocker,[13] which resulted in the arrest of a key member in October 2023. Note that when Dark Angels first appeared, they deployed a Babuk variant before switching to RagnarLocker.

The Dark Angels ransomware group's strategy of targeting a small number of high-value companies for large payouts is a trend worth monitoring. Zscaler ThreatLabz predicts that other ransomware groups will take note of Dark Angels' success and may adopt similar tactics, focusing on high-value targets and increasing the significance of data theft to maximize their financial gains.

[13] Europol, **Ragnar Locker ransomware gang taken down by international police swoop**, October 20, 2023.

#2 LockBit

LockBit first emerged in September 2019 and quickly rose to prominence due to the group's large ransomware affiliate network. LockBit leverages affiliates to conduct breaches, exfiltrate data, and deploy its ransomware. Infiltration typically starts through spam emails containing malicious attachments or links. Other methods include executing brute-force password attacks that target Remote Desktop Protocol (RDP) or VPN credentials, purchasing compromised stolen credentials through initial access brokers, and exploiting public-facing applications. LockBit's cybercriminal network has targeted critical sectors such as manufacturing, healthcare, and logistics. The group has collectively targeted more than 2,000 systems worldwide and extorted more than $120 million from victims.

Over the last year, LockBit has remained at the top of the pack in terms of attack volume. Using a markedly different strategy from Dark Angels, the LockBit group encourages affiliates to attack as many organizations as possible, regardless of the potential reward. This high volume of attacks often results in small businesses being targeted with relatively low ransom demands.

LockBit ransomware is deployed on Windows and Linux-based systems. There are three versions of LockBit for Windows: LockBit Red (the original), LockBit Black (based on BlackMatter source code), and LockBit Green (based on the leaked Conti source code). As mentioned in the ThreatLabz 2023 Ransomware Report, the LockBit Black builder was leaked, and many cybercriminal groups not affiliated with LockBit have used it for their own ransomware attacks. Interestingly, LockBit Black is still the group's most commonly deployed variant. The specific LockBit ransomware variant used to encrypt a victim's files is now shown in the ransom note next to the victim ID. This enables the threat actor conducting the attack to easily identify the LockBit variant deployed to aid them in providing the proper decryption tool when a ransom is paid. See figure 16 for an example of a recent LockBit Black ransom note.

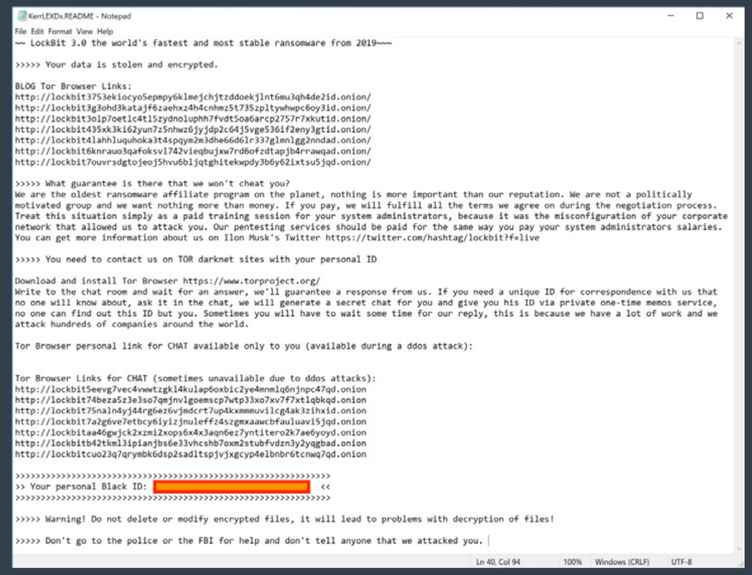


Figure 16: Example of a recent LockBit Black ransom note.

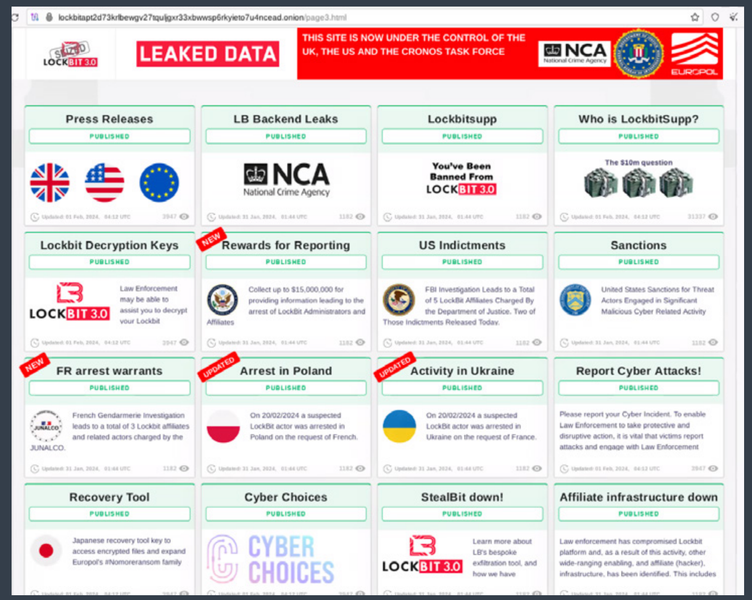


Figure 17: Law enforcement's seizure of LockBit's data leak site.

On February 20, 2024, the FBI and UK law enforcement seized parts of LockBit's infrastructure, which included approximately 7,000 victim decryption keys. After the seizure, law enforcement commandeered the LockBit data leak website and mocked the cybercriminals with a similar rendition of the former site displaying various articles and countdown timers until new information was released, as shown in figure 17 below.

Unfortunately, within days of the takedown, ThreatLabz identified new ransomware attacks perpetrated by LockBit and a new data leak site. The group has remained active and attacked dozens of new entities since the law enforcement action.

On May 7, 2024, the FBI announced the indictment of LockBit developer and operator Dmitry Yuryevich Khoroshev. However, the LockBit operator quickly denied that the FBI correctly identified him. Without further arrests, LockBit attacks will likely continue for the foreseeable future, although at some point ThreatLabz expects the LockBit brand may be retired and the operation resurrected under another name due to increased scrutiny.

#3 BlackCat

BlackCat (a.k.a. ALPHV) ransomware, introduced in November 2021, was one of the most notorious threats until it was shuttered in March 2024. Similar to LockBit, BlackCat leveraged an affiliate network to launch attacks and shared a percentage of the ransom payments.

Arguably the most infamous BlackCat affiliate is a group known as Scattered Spider[14] (a.k.a. Star Fraud). Made up of English-speaking members, this group is highly effective in social engineering attacks, often impersonating IT or help desk staff in voice calls and carrying out SIM swapping attacks to defeat multifactor authentication. On June 15, 2024, the alleged ringleader[15] of Scattered Spider, a 22-year-old UK national, was arrested. However, it is too soon to tell what impact this arrest will have on the group's ability to continue its attacks.

BlackCat was one of the most cross-platform compatible ransomware families, partly because it uses the Rust programming language. Figure 18 shows the decryption tools available for all platforms that were supported by BlackCat ransomware just before the group shut down operations. The platforms included Windows, ESXi, FreeBSD, and numerous variants of Linux operating systems and architectures, such as ARM, x86/x64, and PowerPC.

[14] Cybersecurity & Infrastructure Security Agency, **Cybersecurity Advisory: Scattered Spider**, November 16, 2023.
[15] Krebs on Security, **Alleged Boss of 'Scattered Spider' Hacking Group Arrested**, June 15, 2024.

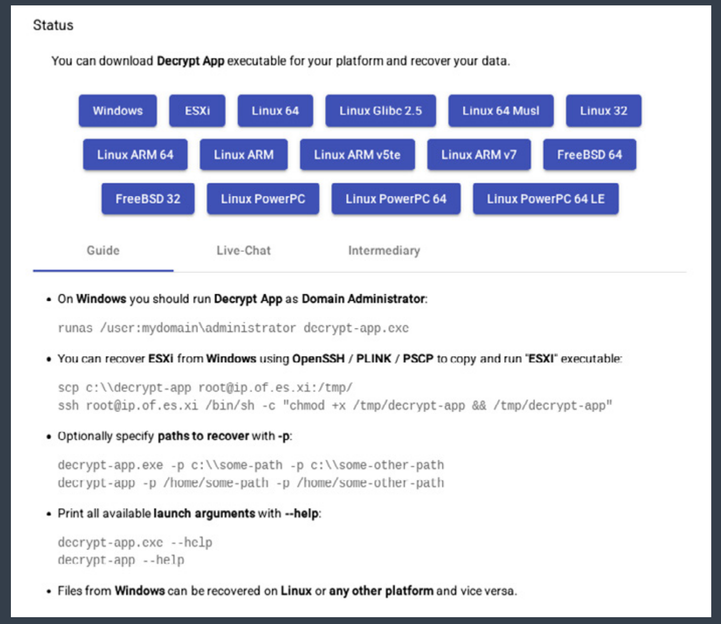


Figure 18: BlackCat decryption tools were provided for 15 different operating systems, architectures, and platforms.

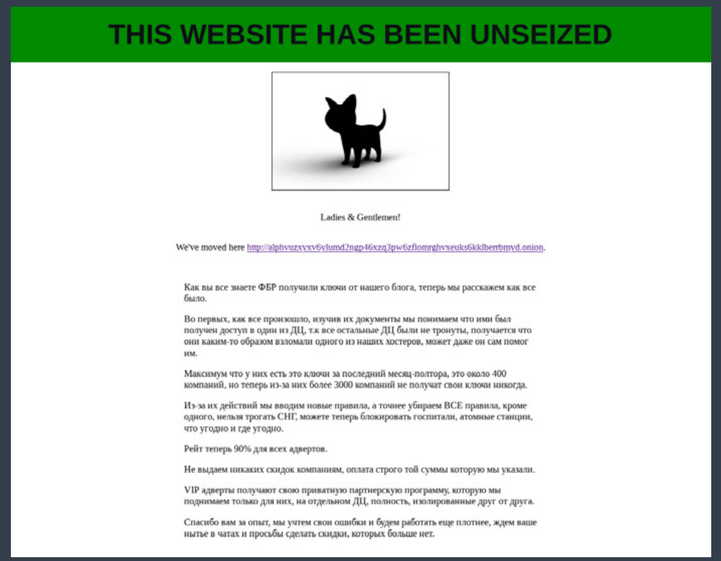


Figure 19: BlackCat's "unseized" data leak site after law enforcement action.

This level of cross-platform compilation is unusual in comparison to other ransomware families that typically only support Windows, ESXi, and a small number of Linux-based platforms. This indicates that BlackCat affiliates may have requested support for additional platforms in order to encrypt files on as many systems as possible.

In December 2023, the FBI gained access to some of BlackCat's infrastructure. The FBI attempted to seize the group's Tor-based websites, including the ransom negotiation portals and data leak sites. However, in a swift turn of events, BlackCat posted a message that they had "unseized" the data leak website and provided a link to a new data leak website that the FBI could not manipulate, as shown in figure 19 below.

This back and forth between the FBI and BlackCat occurred over a few days until BlackCat was confident that the new data leak site was sufficiently advertised. Note that "seizing" a Tor-based website is not as trivial as a traditional DNS-based website because it relies on cryptographic secrets rather than a central authority that is subject to court orders.

In March 2024, the BlackCat group announced their disbandment, citing the compromise of their infrastructure by the FBI, which supposedly rendered them unable to continue their operations. However, suspicions arose due to the timing of their shutdown occurring immediately after receiving a $22 million ransom and then performing an exit scam on an affiliate who assisted them in breaching a healthcare provider (discussed earlier in this report).

While BlackCat ransomware is no longer active, the affiliates behind the group's attacks have likely migrated to other ransomware-as-a-service networks such as RansomHub (where the data stolen from the healthcare provider who paid the $22 million ransom has since been leaked). Furthermore, the BlackCat ransomware group itself is unlikely to have truly ceased their operations and will likely reemerge under a new brand name.

#4 Akira

Akira ransomware burst onto the scene in April 2023, quickly gaining infamy for the volume of attacks conducted by affiliates. The Akira threat group is likely another offshoot from the defunct Conti group. In fact, Akira's ransomware code originally shared many similarities with the leaked Conti source code. However, the group has more recently developed a Rust–based ransomware that contains references to Power Rangers characters such as Megazord.

Affiliates of Akira ransomware have employed various initial access mechanisms, including through the exploitation of CVE–2023–20269.[16] The threat group operating Bumblebee, which has ties to Conti ransomware, has also been known to be an initial access broker for Akira. As mentioned earlier in the report, Operation Endgame dismantled Bumblebee but had a minimal impact on Akira's operations.

To better understand Akira's attacks, we can learn directly from the information that Akira provides to victims that pay a ransom. ThreatLabz captured the following chat message from Akira, which contains details about how they initially gained access to the company's network through an initial access broker, and also offered tips for preventing ransomware attacks in the future:

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate:

1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer.

2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources.

3. Install 2FA wherever possible.

4. Use the latest versions of operating systems, as they are less vulnerable to attacks.

5. Update all software versions.

6. Use antivirus solutions and traffic monitoring tools.

7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one.

8. Use backup software with cloud storage which supports a token key.

9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

Although this advice comes directly from Akira, the recommendations are valid and provide a foundation for understanding and thwarting such attacks.

Akira is one of the only major ransomware groups that has not directly been subject to a law enforcement disruption. As a result, Akira is now one of the most active ransomware groups that will likely continue to launch new attacks over the next year.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

#5 Black Basta

Black Basta ransomware, first identified in April 2022, is another successor to the Conti ransomware group. Black Basta affiliates have employed diverse methods to gain access to corporate networks. Prior to Operation Duck Hunt (August 2023), Qakbot was a major initial access broker for Black Basta. As mentioned earlier, Pikabot stepped in to fill the void after the takedown. However, Pikabot was shuttered following Operation Endgame in May 2024.

ThreatLabz has since been tracking new activity from the Qakbot threat group, which has pivoted and changed its TTPs significantly. Instead of using spam email to infect systems with Qakbot, the threat group is currently using a combination of social engineering techniques. Instead of sending spam emails to millions of addresses, the threat group is performing targeted attacks. These attacks start with the threat group sending spam emails to a small number of targeted companies. The group then calls an employee at these companies pretending to be from their own IT department. The caller instructs the victim to join a screen sharing session using remote desktop software such as Microsoft's Quick Assist to "update the company's spam filters" for the employee. Once the employee gives access to the threat actor, a Windows batch script is executed to perform reconnaissance, steal credentials, and install a backdoor on the victim's system. The backdoor continues to change but has included Qakbot, Cobalt Strike, and a SOCKS proxy tool. The batch script contains a command line interface that appears similar to that shown in figure 20.

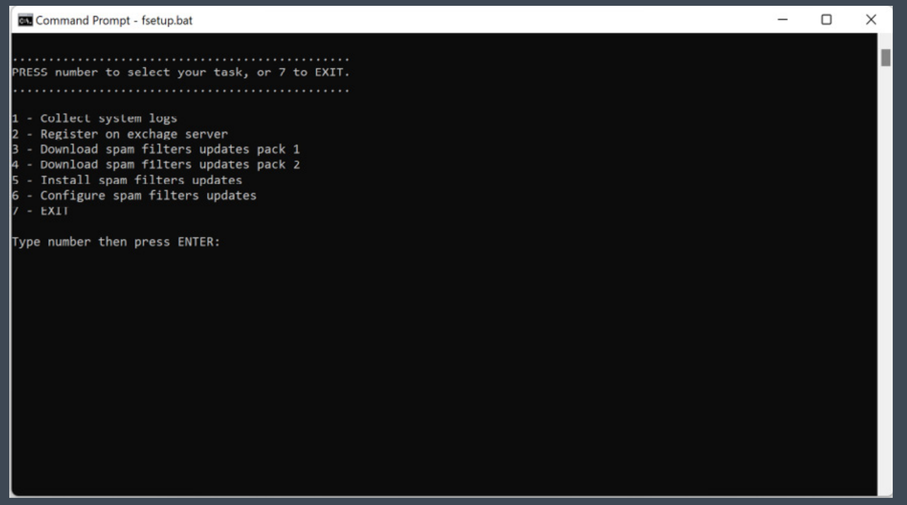


Figure 20: Malicious Windows batch script interface used to establish a backdoor on a victim's system as a precursor to a Black Basta ransomware attack.

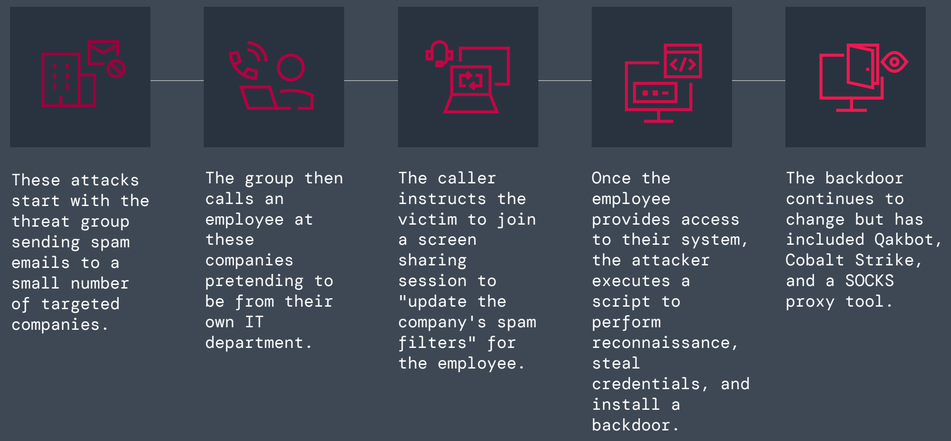


Figure 21: Black Basta ransomware attack chain with initial access brokered by Qakbot threat group.

Once this backdoor access has been established, the Qakbot threat group hands off access to a penetration testing team responsible for lateral movement and the ultimate deployment of Black Basta ransomware.

While Operation Duck Hunt had a significant short-term impact, the threat group remains active and continues to innovate and experiment with new techniques to compromise organizations. Over the next year, the Qakbot threat group is likely to remain a major initial access broker for ransomware attacks such as Black Basta.

ThreatLabz Ransomware_Notes Archive

Zscaler ThreatLabz has been maintaining a **public GitHub repository** that, as of this writing, tracks 391 ransomware families and contains a total of 945 ransom notes, adding 19 families and 55 ransom notes between April 2023 and April 2024. This archive can be valuable for tracking ransomware groups over time, including their data leak websites and negotiation tactics, and for linking ransomware groups that rebrand by using stylometric analysis.

Figure 22 shows a stylometric comparison between a Conti ransom chat (top) and a Black Basta ransom chat (bottom). This demonstrates that members of Black Basta are almost certainly former members of Conti as apparent in the similarities in their sentence structure, word choice, and even specific instructions.

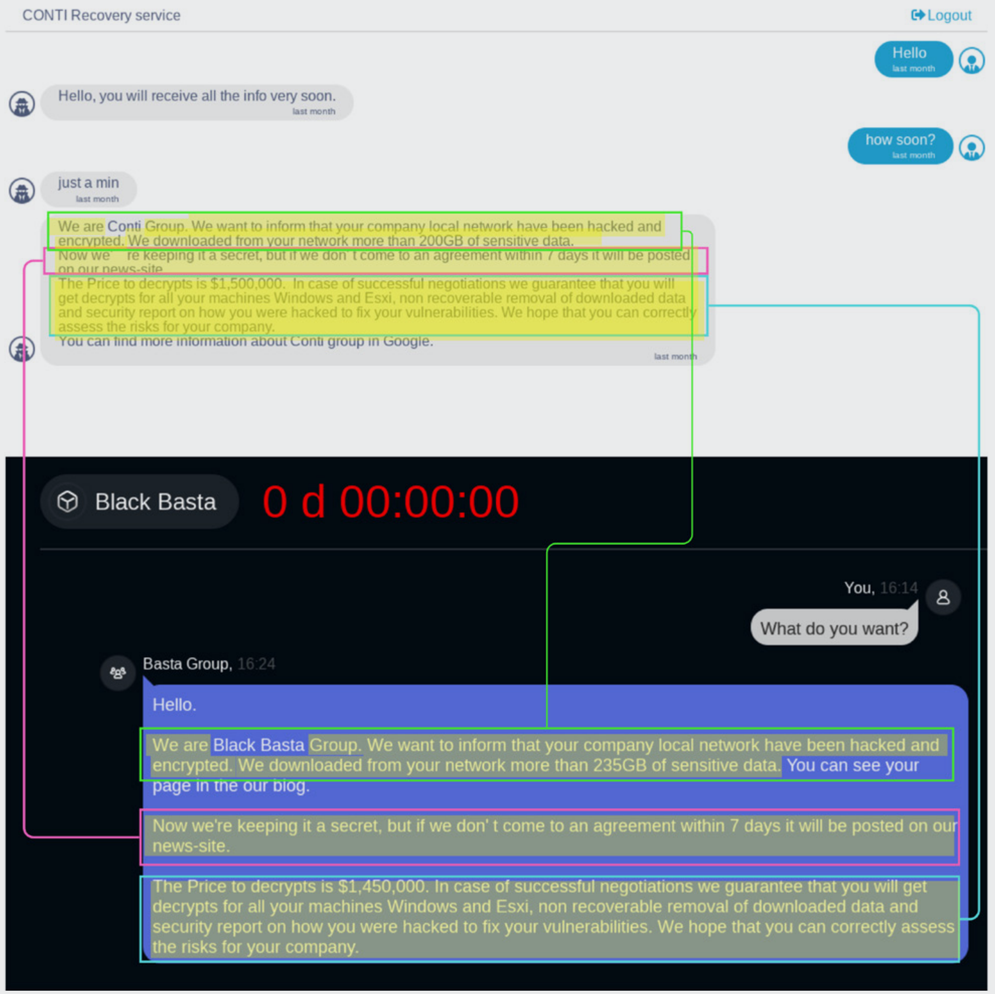


Figure 22: Stylometric comparison between Conti (top) and Black Basta (bottom) ransom chats.

2025_ Predictions

1. Ransomware threat actors will adopt highly targeted attack strategies.

Over the last year, Dark Angels has been one of the most successful and least known ransomware groups with a distinct strategy of targeting a small number of multibillion-dollar businesses and extorting them for substantial ransoms. This strategy serves a dual purpose: reduce scrutiny from law enforcement and the security industry, while spending more resources to infiltrate large companies that are willing to pay significant ransoms to protect huge volumes of stolen data. This has led to the group receiving the largest known ransom payment of $75 million, which is bound to attract the interest of other ransomware threat actors in 2025 that may want to replicate their success.

2. Targeted attacks will increasingly involve voice-based social engineering.

In 2025, we expect to see an increase in targeted attacks facilitated by specialized initial access brokers. These brokers, exemplified by the activities of Qakbot and Scattered Spider, employ sophisticated techniques to secure entry, notably utilizing voice-based ("vishing") social engineering attacks to deceive individuals into granting access to a corporate environment, which is then used ultimately to exfiltrate data and deploy ransomware. This emerging trend highlights collaborations within the cybercriminal ecosystem and underscores the need for heightened vigilance and advanced security measures to counter these evolving threats.

3. Ransomware attackers will increasingly adopt GenAI to create more effective, personalized, and localized campaigns.

Increasing adoption of generative AI in 2025 and beyond will enable threat actors to craft spam emails with accurate grammar and spelling as well as use voice cloning to impersonate staff in order to gain privileged access. In the coming years, AI-generated voices may be tailored with local accents and dialects to enhance credibility and increase the likelihood of success—and become a prime example of how ransomware threat actors will make attacks more convincing and difficult to detect.

4. More cybersecurity incidents will be reported in line with new SEC rules.

With the SEC's ruling mandating stricter cybersecurity incident reporting, 2025 will continue to witness an uptick in organizations disclosing ransomware incidents. This will hopefully result in increased transparency and promote a culture of accountability and proactive defenses, driving improvements in cybersecurity practices.

5. High-volume data exfiltration ransomware attacks will be on the rise.

Attacks that exfiltrate large amounts of data, including more encryption–less incidents, will increase significantly in the year ahead. This trend, which started gaining momentum in 2022, sees threat actors focusing solely on exfiltrating data without encrypting systems. The approach allows for quicker, opportunistic operations and capitalizes on the fear of sensitive data being released to coerce victims into paying ransoms. It underscores a continuous shift in ransomware strategies toward more efficient and high–impact methods.

6. Companies in the healthcare sector, especially, will continue to face persistent targeting by ransomware groups.

The high value of healthcare data will continue to attract attention in 2025. Many healthcare companies lag in replacing legacy systems with modern, advanced security measures, making them particularly vulnerable. As a result, these organizations are likely to face repeated breaches and extortion attempts. Those that fail to take appropriate actions to prioritize zero trust defense strategies may find themselves targeted by ransomware groups.

7. International collaboration against cybercrime organizations will build upon existing efforts.

Law enforcement and private industry will continue to collaborate in efforts to combat ransomware attacks, such as disrupting major initial access brokers and ransomware groups. International collaboration will become increasingly vital as global interconnectedness grows, making it easier for cybercriminals to operate transnationally. By sharing intelligence and expertise, these coordinated actions will more effectively disrupt global ransomware networks. Zscaler ThreatLabz has been at the forefront and instrumental in providing technical assistance for several of these operations over the last year.

How Zscaler Simplifies Ransomware Protection

The rising complexity and cost of ransomware attacks underscores the need for comprehensive zero trust defenses. The Zscaler Zero Trust Exchange™ platform simplifies the challenge, offering a holistic approach to stopping ransomware.

The Zero Trust Exchange allows enterprises to deploy smarter defenses at every stage of an attack. This starts with preventing attackers from discovering or exploiting users and applications by making those users and apps invisible, accessible only by authorized users or devices. It inspects all inbound and outbound traffic inline, encrypted or not. Authenticated users and devices connect directly to the applications they need, never to the network—so even if an attacker gets in, they can't move laterally to steal or encrypt data.

WHY ZERO TRUST IS ESSENTIAL FOR RANSOMWARE PROTECTION

Legacy security architectures are ineffective at stopping ransomware attacks.

OUT WITH THE OLD: Traditional security measures and point solutions, including "next-generation" firewalls and VPNs, often introduce blind spots, complexity, and significant costs. These legacy approaches fail to cost-effectively inspect encrypted files and traffic, leaving organizations vulnerable to lateral movement and ransomware attacks that exploit gaps in visibility and control—often with devastating consequences.

IN WITH ZERO TRUST: A zero trust architecture assumes every user, device, and connection is potentially compromised. This approach mandates continuous verification and strict access control. By consistently verifying identities and inspecting all traffic, including encrypted data, zero trust significantly reduces the risk of attacks spreading within the network, neutralizing ransomware threats before they can inflict damage.

ZSCALER STOPS RANSOMWARE AT EVERY STAGE OF THE ATTACK CYCLE—from initial reconnaissance and compromise to lateral movement, data theft, and payload execution.

Minimize the attack surface: Built on a zero trust architecture, the Zero Trust Exchange replaces exploitable legacy VPN and firewall architectures that expand the attack surface. Zscaler effectively minimizes the attack surface by hiding users, applications, and devices behind a cloud proxy, where they are not visible or discoverable from the internet. Similar to a switchboard routing calls to authorized destinations, Zscaler only connects the right, authorized user or device to a particular application.

Prevent initial compromise: The Zero Trust Exchange employs extensive TLS/SSL inspection, browser isolation, advanced inline sandboxing, and policy-driven access controls to prevent users from accessing malicious websites as well as detect unknown threats before they reach your network. This minimizes the risk of compromise in the first place.

Eliminate lateral movement: Leveraging user-to-app or app-to-app segmentation, users connect directly to applications (and apps to other apps), not the network, eliminating the risk of lateral movement. By centralizing access control policy management, Zscaler acts like a security checkpoint for internet traffic, removing pathways for lateral movement. Zscaler can also identify and stop potential attackers from moving laterally, whether external threats or malicious insiders, through identity threat detection and response (ITDR) and deception capabilities.

Stop data loss: Inline data loss prevention measures, combined with full TLS/SSL inspection, effectively thwart data theft attempts. Zscaler ensures that data is secured both in transit and at rest.

FIGHTING AI-DRIVEN THREATS WITH AI + ZERO TRUST INNOVATION

These AI-driven capabilities enable Zscaler to offer robust protection against ransomware, ensuring comprehensive security for enterprises in the evolving threat landscape:

- ***AI-powered 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 command-and-control (C2) infrastructure.
- ***AI-powered sandboxing*** offers comprehensive malware and zero-day threat prevention by analyzing suspicious files in a controlled environment.
- ***AI-powered segmentation*** provides automated access policy recommendations to minimize the attack surface and prevent lateral movement, using user context, behavior, location, and private app telemetry.
- ***Dynamic, risk-based policy*** continuously analyzes the risk associated with users, devices, and applications to enforce dynamic security and access policies.
- ***AI-powered browser*** isolation creates a secure gap between users and malicious web content by rendering pages as streams of picture-perfect images, preventing data leaks and the delivery of active threats.
- ***AI-driven data discovery and classification*** provides instant data visibility and classification out of the box across endpoint, inline, and cloud data, making it more difficult for ransomware to target and encrypt sensitive data.

Holistic prevention at each stage of the attack chain

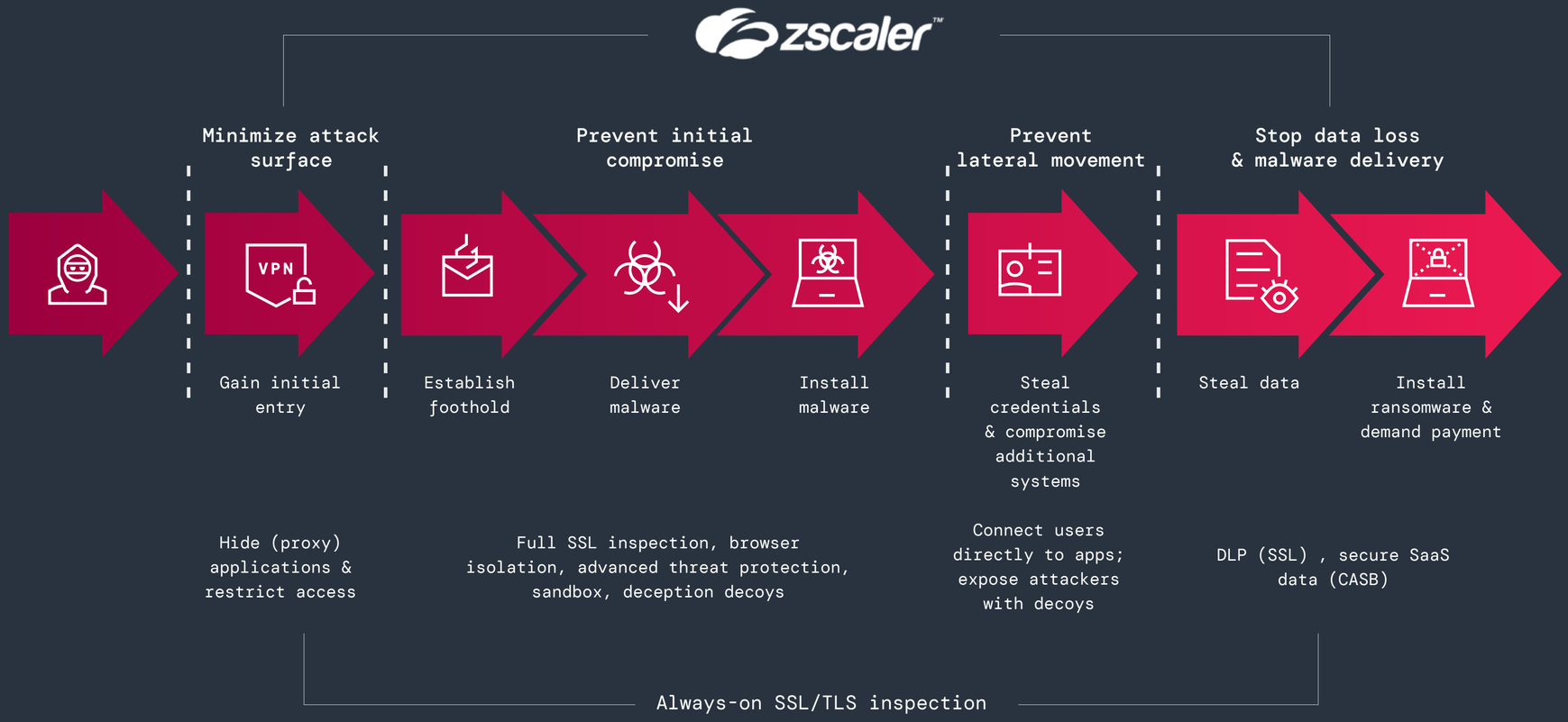


Figure 23: Mapping zero trust architecture across the ransomware attack chain.

Related Zscaler products

Zscaler Internet Access™ (ZIA™) provides secure and direct access to the internet, offering inline threat protection. ZIA's advanced threat prevention and sandboxing capabilities help thwart ransomware downloads, and command-and-control (C2) communications, preventing ransomware infiltration.

Zscaler Private Access™ (ZPA™) enables secure access to internal applications without internet exposure, employing a zero trust model. ZPA ensures that only authorized users and devices can access critical applications, thus reducing the attack surface and preventing ransomware attempts.

Zscaler Zero Trust Firewall intercepts and inspects TLS/SSL traffic to detect malware hidden in encrypted traffic, preventing its infiltration into the network.

Zscaler Deception detects and contains attackers attempting to move laterally or escalate privileges by luring them with decoy servers, applications, directories, and user accounts.

Zscaler Sandbox analyzes suspicious files and executables in a controlled virtual environment, helping to identify and block malicious code, keeping organizations ahead of file-based ransomware and zero-day attacks.

Zscaler Cloud Browser isolates web sessions and streams only pixels to devices to effectively eliminate the risk of drive-by downloads and zero-day exploits that may be used by ransomware operators.

Zscaler ITDR (Identity Threat Detection and Response) detects and defends against identity-based attacks such as credential theft and privilege abuse, Active Directory assaults, and risky entitlements.

Zscaler Data Protection provides consistent, unified security for data in motion and data at rest across SaaS and public cloud applications, reducing the likelihood of data exfiltration while mitigating the potential impact of ransomware attacks.

Ransomware Prevention Guidance

A defense strategy rooted in zero trust architecture is a proven security measure for stopping ransomware, but tackling this multifaceted threat demands proactive planning, ongoing collaboration, and strategic investments.

ThreatLabz experts have compiled the latest best practices to help reduce ransomware risks and safeguard your organization against existing and emerging threats.

- **Implement regular and secure data backups.** Ensure all data is backed up regularly and securely, including offline backups. Adapt backup strategies based on evolving threats.
- **Keep software updated.** Apply the latest security patches promptly to address known vulnerabilities. Use AI-driven threat intelligence platforms to prioritize and manage security patches effectively.
- **Enable multifactor authentication (MFA).** Add an extra layer of security to user accounts with MFA to mitigate the risk of unauthorized access. Integrate MFA solutions to detect and prevent account takeovers effectively.
- **Establish a consistent corporate security policy.** Ensure all users follow consistent security procedures, including MFA and regular security updates, to help prevent initial compromises. With a distributed workforce, it is even more important to implement a security service edge (SSE) architecture to protect users no matter where they are.
- **Bolster application security.** Remove applications from the public internet to prevent ransomware actors from exploiting vulnerabilities. Implement a zero trust architecture for internal applications to safeguard them against ransomware attempts.
- **Enforce least-privileged access.** Implement least-privileged policies to restrict user access to only the resources necessary for their roles. Utilize AI-powered solutions to dynamically analyze user behavior and adapt access privileges accordingly.
- **Strengthen identity protection.** Use ITDR tools to gain visibility into identity misconfigurations, remediate vulnerabilities in Active Directory that adversaries exploit to escalate privileges and move laterally, and detect stealthy identity threats.
- **Inspect all traffic.** Today, 86% of threats are delivered over encrypted channels, which are often not inspected, making it easy for even moderately sophisticated attackers to bypass security controls. It's essential to inspect all traffic, encrypted or not, to prevent compromise.
- **Implement zero trust network access (ZTNA).** Deploy granular user-to-application and application-to-application segmentation, brokering access via least-privileged access controls to eliminate lateral movement, minimize data exposure, and enhance your overall security posture.

- **Utilize AI-driven browser isolation.** Protect users from web threats with AI-based isolation of suspicious internet content and high-risk users. By isolating the browser experience and restricting potentially harmful actions (like inputting credentials), users can safely access suspicious URLs and files without risking their system's security.
- **Employ AI-powered advanced sandboxing.** Stop never-before-seen and elusive malware with a sandbox that automatically detects and quarantines unknown threats and suspicious files leveraging AI/ML analysis.
- **Deploy inline data loss prevention (DLP).** Safeguard against data exfiltration and exposure by deploying inline DLP measures.
- **Leverage deception technology.** Employ deception tools and honeypots to misdirect attackers, fortifying defenses against system infiltration.
- **Utilize a cloud access security broker (CASB).** Control and monitor cloud application usage with a CASB to prevent malicious activities like file downloads and data exfiltration.
- **Provide ongoing employee training.** Conduct regular security awareness training to educate employees about ransomware threats. Employ simulations of real-world ransomware scenarios to enhance employee preparedness.
- **Develop a comprehensive ransomware response plan.** Create a response plan encompassing data recovery, incident response, and communication protocols to act swiftly and effectively in the event of a ransomware attack.

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

Report Methodology

The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The report team collected data from a variety of sources between April 2023 and March 2024, including:

- **The Zscaler global security cloud,** which processes more than 500 trillion daily signals, blocks more than 9 billion 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.
- **External intelligence sources.** We also collected data from external intelligence sources, such as threat intelligence feeds, open source research, and law enforcement reports, which provided additional information about ransomware attackers, their targets, and their methods.
- **The ThreatLabz team's own analysis of ransomware samples and attack data.** The ThreatLabz Threat Intelligence team tracks ransomware families at scale through reverse engineering and automating malware analysis to develop effective response strategies. ThreatLabz also works closely with international law enforcement agencies and has played a significant role in recent actions, including Operation Duck Hunt and Operation Endgame.

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**.

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 150 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.**

Experience your world, secured.™