deep instinct™

2025 THREAT REPORT

The Changing Face of Global Threats

2024 Year In Review & 2025 Predictions

deepinstinct.com

Table of Contents

Introduction

In 2024, we witnessed a surge in sophisticated cyber threats. Driven by global digitization, the number of ransomware attacks and breaches continued to grow across multiple industries. Threat actors more frequently exploited zero-day vulnerabilities, targeting both public and private sectors, and leveraged AI to automate reconnaissance, vulnerability exploitation, data exfiltration, and malware generation.

Additionally, Ransomware-as-a-Service (RaaS) has continued to evolve, with a marked rise in AI-generated phishing campaigns that bypassed traditional security measures. In response, organizations adopted more proactive defense mechanisms, including deep learning–based threat detection and real-time anomaly detection.

Key events shaping the threat landscape included the global surge in supply chain attacks and several massive, high-profile breaches, exposing millions of users' sensitive data. In particular, the healthcare and financial sectors faced unprecedented challenges during 2024, with ransomware groups using advanced and constantly evolving malware that adapted in real time to evade signature-based defenses. Additionally, several zero-day vulnerabilities in widely used enterprise software were exploited, underscoring the need for timely patch management and threat intelligence sharing.

Collaborations between cybersecurity firms and government agencies led to the successful takedown of a major ransomware network in late 2024, highlighting the power of global cooperation in cybersecurity. Despite these notable successes, cyberattacks still rose during the final months of 2024, as they do at the end of each year.

The trends observed this year emphasize the need for a paradigm shift in data security strategies.

Organizations must adopt a layered strategy that features preemptive cybersecurity capabilities, combining deep learning models for predictive threat analysis and prevention to effectively fight back against Dark AI. Proactive threat hunting powered by AI-driven insights and continuously improving threat intelligence platforms is crucial in mitigating future threats. As adversaries refine their tactics, the focus must shift to proactive prevention and zero-day data security frameworks to safeguard sensitive data.

The Top Malware Trends of 2024

As cyber threats continued to evolve, 2024 experienced a surge in malware activity, with ransomware remaining a dominant force. While the overall number of attacks has increased, the rate of growth slowed compared to previous years, reflecting both the persistence of cybercriminal tactics and the growing sophistication of organizational defenses.

Ransomware Trends

The total number of ransomware attacks in 2024 was higher than in previous years, but the growth rate slowed, especially compared to the dramatic growth between 2022 and 2023.

Between 2022 and 2023, ransomware incidents skyrocketed due to a confluence of factors, including increased digitization, more sophisticated attack tools, and more widespread targeting of critical infrastructure. Global ransomware payouts also increased significantly.

Reports show a 30% increase in overall global cyberattacks in Q2-24 compared to Q2-23.

While ransomware attacks remain a key driver of these incidents, RaaS and the emergence of AI-enhanced tactics have also contributed to the rise.

Reports show a 30% increase in overall global cyberattacks in Q2 2024 compared to the same period in 2023[1]

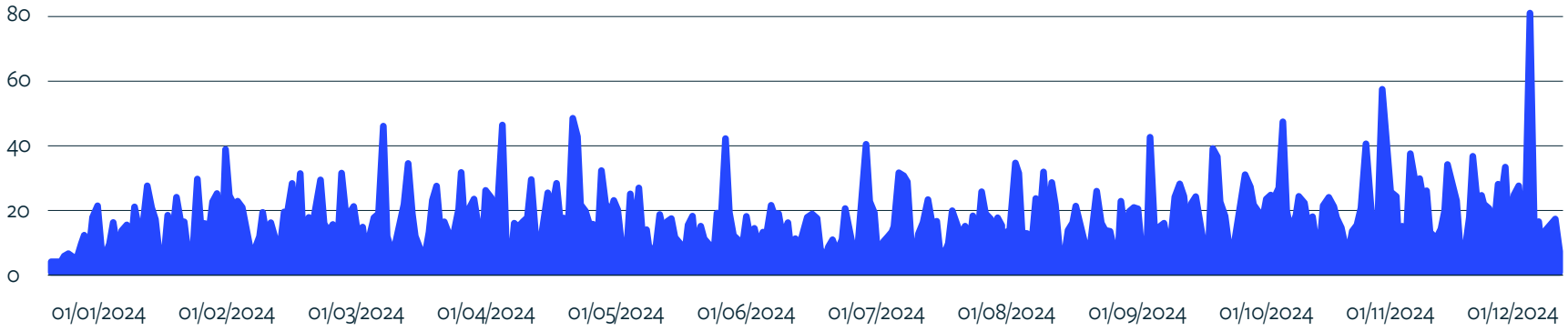
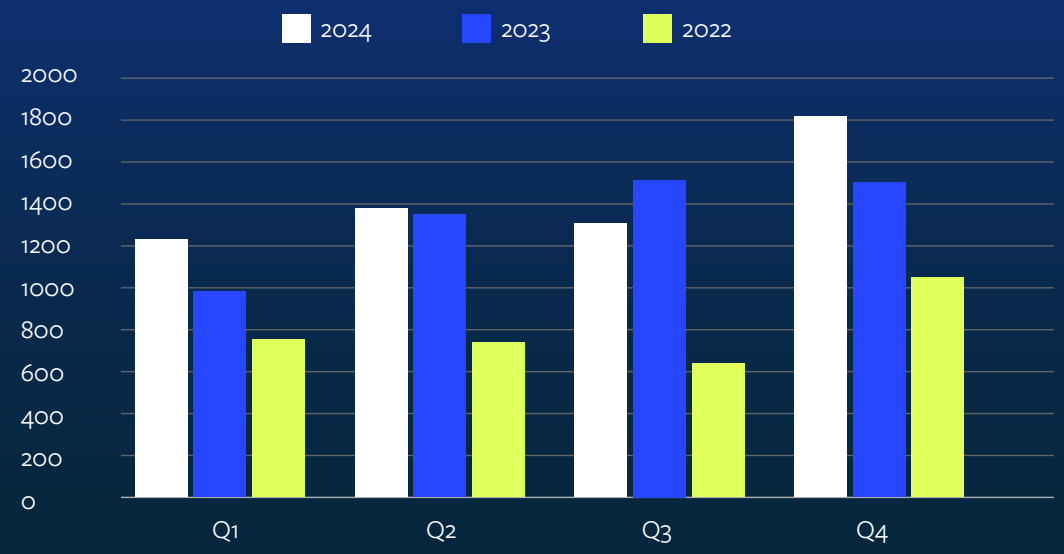


Figure 1: Ransomware attacks 2024

Ransomware Surge

Quarterly ransomware victims discovered over the last 3 years



Industry data reveals a steady increase in ransomware victims from 2022 to 2024, with 2024 showing the highest numbers in Q1, Q2, and Q3, underscoring the growing severity of the threat.

The number of victims in Q2 and Q3 of 2024 was more than double the 2022 numbers during those same quarters.

Notably, across all three years, the highest victim counts were consistently in Q4, indicating a surge in attacks toward the end of the year.

This year-over-year growth highlights ransomware campaigns' expanding reach and sophistication, likely driven by advanced tools, broader targeting methods, and gaps in defenses preventing unknown threats.

Figure 2: Quarterly ransomware victims discovered over the last 3 years.

Global Ransomware Impact:
The Most-Targeted Countries in 2024

The map displays the global distribution of ransomware attacks over the past year. Darker shades highlight countries with more frequent or severe incidents, and lighter tones indicate areas with fewer attacks.

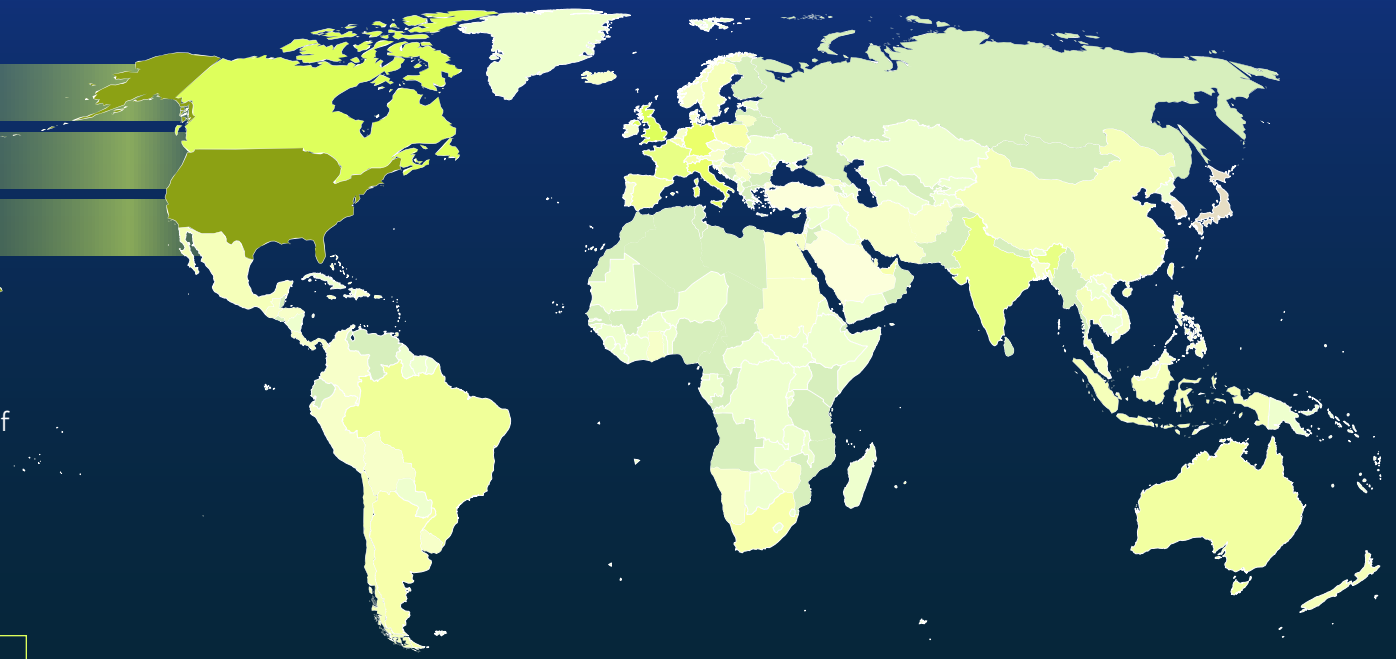
Ransomware attacks have targeted countries worldwide, but some are hit harder than others.

While the United States is targeted more by ransomware than any other country in the world, France is the most affected, with upwards of 74% of organizations reporting ransomware incidents in 2024. South Africa, Italy, and Austria were also heavily affected, with 69% of organizations in each country reporting ransomware incidents.

Top Targets by % of Organizations

74%
France

69%
South Africa, Italy, and Austria



UNITED STATES
Most frequent target of ransomware attacks

Figure 3: Targeted countries by ransomware frequency

Top Sectors Targeted by Ransomware in 2024

The most expensive ransomware attacks of 2024 predominantly targeted the healthcare sector, highlighting its vulnerability to such threats.

India's Regional Cancer Center (RCC):
A ransom demand of $100 million.

Synnovis (UK Pathology Services):
A ransom demand of $50 million.

Change Healthcare (United States):
A ransom demand of $22 million was paid, underscoring the financial impact on healthcare technology providers.

Ann & Robert H. Lurie Children's Hospital:
A ransom demand of $3.4 million was not paid, highlighting ongoing resistance efforts within the sector.

These examples illustrate how ransomware groups prioritize sectors that manage critical services and sensitive data, leveraging operational urgency to pressure victims into paying, showcasing the sector's susceptibility to high-stakes attacks and underscoring the risks to critical healthcare operations.

While other sectors such as technology (e.g., CDK Global – $25 million ransom) also experienced significant attacks, healthcare stood out due to the number of high-profile cases and the operational impact.

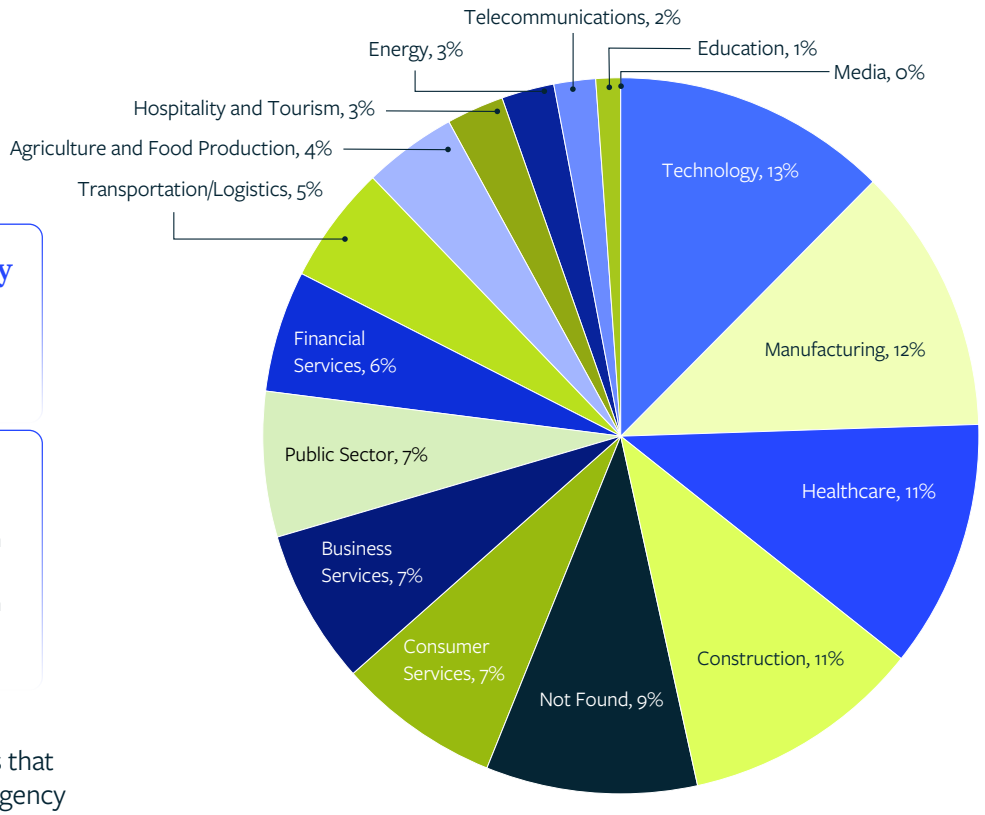


Figure 4: Ransomware targets by sector

Attackers target healthcare for its critical services and often limited cybersecurity measures. They know disruptions can have life-threatening consequences, encouraging prompt ransom payments to restore operations quickly.

Ransomware Threat Actors

The majority of prominent ransomware groups in 2024 operated under a RaaS model, allowing them to scale operations by recruiting affiliates who conduct attacks using the group's infrastructure and tools in exchange for a percentage of ransom payments. This business model has proven highly effective, with groups like LockBit offering up to 80% of ransom proceeds to affiliates, helping explain the continued proliferation of ransomware attacks despite increased law enforcement pressure.

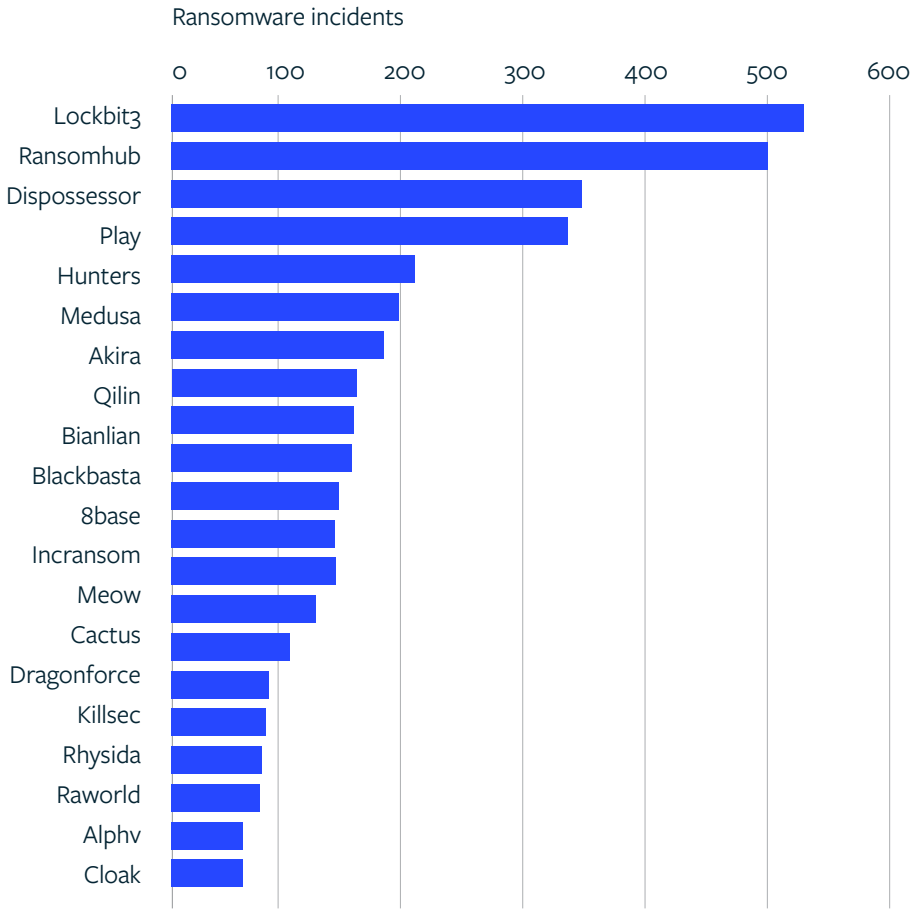


Figure 5: Top ransomware threat actors of 2024

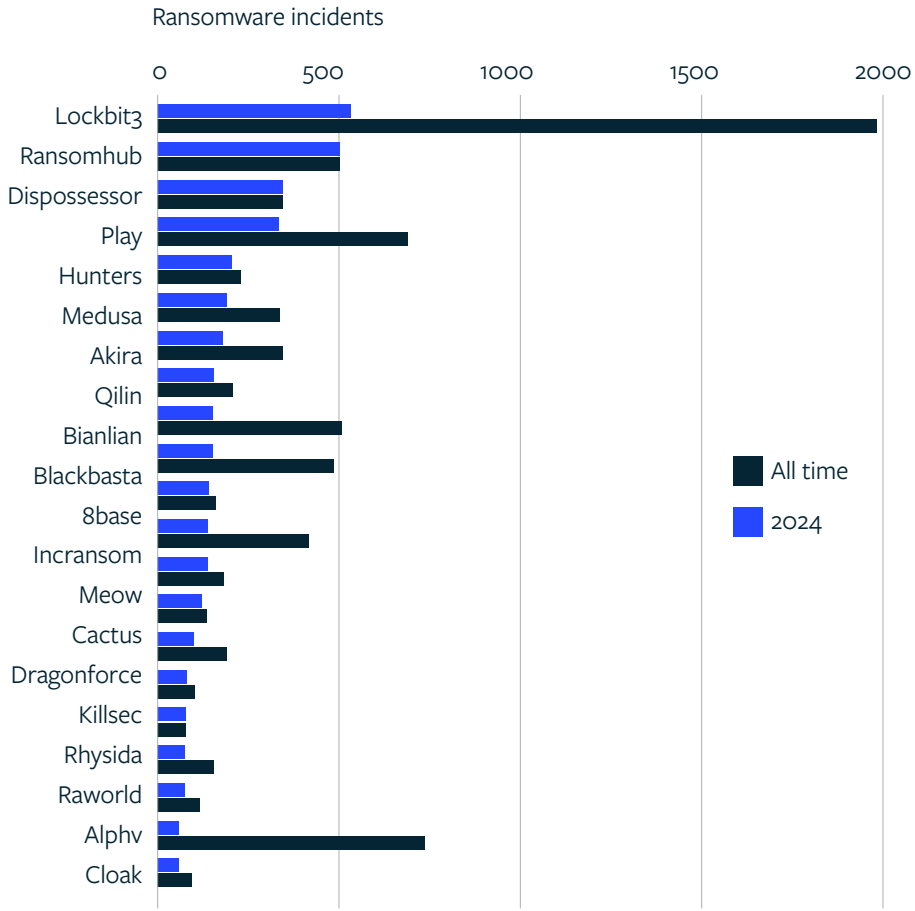


Figure 6: Top ransomware threat actors of 2024 with comparison to their all-time activity

Top Ransomware Groups in 2024

Lockbit 3.0

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

LockBit is a sophisticated ransomware group known for its highly targeted attacks on businesses, critical infrastructure, and government entities worldwide.

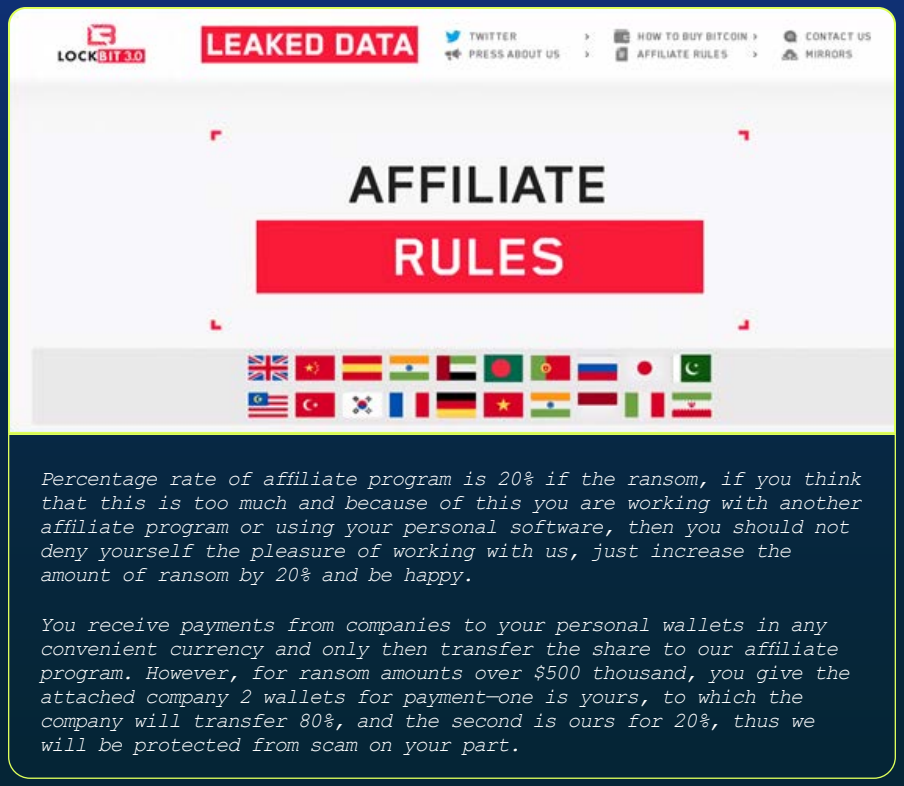


Figure 7: Affiliate rules Source: LockBit RaaS Website

Operating under a RaaS model, LockBit provides malicious affiliates with tools and infrastructure to compromise victims, encrypt their data, and demand substantial ransoms.

Their tactics frequently include double extortion— first encrypting critical files and then threatening to leak sensitive information if payment isn't made. This creates substantial pressure for organizations to comply.

LockBit has been active since at least 2019. It has refined its malware over time, improving evasion techniques, and continuously adapting to security measures, making it one of the more persistent and formidable ransomware threats in the cyber landscape.

In response, international cybersecurity disclosures have provided technical details, indicators of compromise, and defensive measures to help organizations detect and prevent LockBit infections. In parallel, governments and regulatory bodies imposed sanctions on individuals and entities linked to LockBit, aiming to freeze assets, disrupt financial operations, and deter future attacks. Combined with law enforcement actions and cross-border cooperation, these measures seek to weaken LockBit's influence and reduce the profitability of the ransomware ecosystem.

LockBit's influence stems from its affiliate program, which operates as a RaaS model, providing cybercriminals with access to its ransomware toolkit and infrastructure in exchange for a modest share of the proceeds. Notably, LockBit only takes 20% of the ransom payments, allowing affiliates to keep the remaining 80%, making it one of the most attractive profit-sharing models in the cybercrime ecosystem. This profit-sharing model, meshed with user-friendly tools and robust technical support, has contributed to LockBit's widespread appeal among cybercriminals.

RansomHub

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

RansomHub is a relatively new, rapidly evolving ransomware group that appears to have emerged as an updated iteration of the older Knight ransomware operation.

RansomHub is one of three new entrants this year—alongside Dispossessor and KillSec—that have placed among the top 20 ransomware operators in 2024.

They have garnered attention for their use of sophisticated attack techniques, including leveraging the Zerologon vulnerability (CVE-2020-1472) to gain an initial foothold in targeted environments. A key differentiator in RansomHub's approach is the introduction of a unique affiliate prepayment model, requiring would-be partners to pay upfront for access to their ransomware strains, command-and-control (C2) infrastructure, and negotiation portals. This approach, combined with their marketing efforts in cybercriminal forums, has attracted former affiliates from established groups like ALPHV (BlackCat), effectively broadening RansomHub's network and increasing their operational capacity.

As a RaaS provider, RansomHub assists affiliates in conducting "double extortion" attacks—first encrypting victims' files and then threatening to leak stolen data if the ransom demand isn't paid. This pressure tactic, coupled with the group's ongoing efforts to refine its tools, distribution methods—and negotiation strategies—makes RansomHub an emerging and concerning player in the ransomware ecosystem. Victims range from small businesses to larger organizations in various sectors.

Dispossessor

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

The formerly globally active criminal ransomware group Radar/Dispossessor, which targeted dozens of companies in various industries, including healthcare and transportation, was taken down in early 2025 following an FBI investigation.

Dispossessor appeared to follow a RaaS model, similar to LockBit. This approach allows RaaS groups to distribute ransomware through affiliates, who then execute attacks on various targets. The decentralized nature of this model makes it challenging for law enforcement to completely dismantle their operations.

Dispossessor does not appear to have actually possessed ransomware capabilities; instead, it functioned more as a data broker. Since no instances of their ransomware have been observed, it is clear that they were primarily publishing data leaks from other groups, including those that are now defunct or have been shut down. This makes them "opportunistic" rather than "direct" threat actors.

The group, founded in August 2023 and led by the online moniker "Brain," targeted small- to medium-size companies, first focusing on the US before expanding globally.

Play

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

The Play Ransomware group, often simply referred to as "Play," is a financially motivated threat cluster that has monetized access via PLAYCRYPT (aka "Play") ransomware. Play has been active since at least March 2023, with suspected activity dating to September 2022.

Known for leveraging vulnerabilities and employing stealthy infiltration methods, the group quickly encrypts victims' data and appends a distinctive ".play" extension to compromised files. Victims are pressured into paying large ransoms not only for file decryption keys but also to prevent the public release of sensitive stolen information. This double-extortion tactic increases the urgency to comply. With a range of targets and shifting tactics, Play Ransomware exemplifies the fluid, evolving threat landscape that modern enterprises face.

Hunters

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

Hunters International is a RaaS group that emerged in late 2023, coinciding with international law enforcement's disruption of the Hive ransomware group.

Despite their recent inception, they have quickly risen to prominence, claiming responsibility for at least 134 attacks in the first seven months of 2024, making them the 10th-most active ransomware group during this period.

One of the notable tools in their arsenal is SharpRhino, a custom Remote Access Trojan (RAT) written in C#. SharpRhino is distributed through typosquatting domains, impersonating legitimate tools like IP Scanners and aiming to deceive IT professionals into downloading the malware.

Despite the claims, Hunters International denies being a rebrand of the defunct Hive group. It states that it is an independent entity that acquired Hive's source code and infrastructure.

Akira

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

Akira is a RaaS group that has been especially active throughout 2024. Last year, Akira compromised over 250 organizations across North America, Europe, and Australia, amassing more than $42 million in ransom payments early in 2024.

Initially, Akira targeted Windows systems, but in April 2023, the group expanded its operations by deploying a Linux variant aimed at VMware ESXi virtual machines. In August 2023, they introduced "Megazord," a Rust-based encryptor that appends the .powerranges extension to encrypted files while continuing to use their original C++-based ransomware with the .akira extension. Both variants have been used interchangeably in their attacks.

Medusa

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

Medusa is also a RaaS group that has significantly intensified its operations throughout 2024. Unlike many ransomware operators, Medusa maintains a presence on both the dark web and the public web, publicizing its activity on platforms like X and Telegram.

Once inside a network, Medusa employs sophisticated tactics to maintain persistence and evade detection. They utilize compromised Remote Monitoring and Management (RMM) tools, such as ConnectWise and AnyDesk, which are often trusted within organizational environments, allowing them to operate without raising immediate suspicion.

Medusa's ransom demands have been substantial, with the average ransom in 2024 reported to be approximately $668,000. The group employs a double-extortion strategy, not only encrypting victims' data, but also exfiltrating sensitive information and threatening to publish it if the ransom is not paid.

Qilin

RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

Qilin, also known as Agenda, is a suspected Russian-speaking ransomware group that focuses on high-value targets and demands steep ransom prices. Qilin operates as a RaaS and employs double-extortion tactics.

The first instances of Qilin, originally developed in the Go language, surfaced around August 2022. In December of that year the malware was rewritten in Rust. It usually infiltrates the system via phishing and exploits exposed applications like Citrix and RDP.

Security researchers found code similarities with the Black Basta, Black Matter, and REvil ransomware families, implying a possible link.

The group is also known for being politically motivated: Following attacks on hospitals in the UK, it stated the attacks were executed to protest the British government's involvement in an unspecified war (presumably Russia–Ukraine).

BianLian

DOUBLE-EXTORTION RANSOMWARE GROUP

The BianLian Group targets public-facing applications on Windows and ESXi infrastructure. It gains access to victims' systems primarily through valid Remote Desktop Protocol (RDP) credentials. Once inside, they use a combination of open-source tools and command-line scripts to perform system discovery, harvest credentials, and exfiltrate sensitive data. Data is typically exfiltrated via protocols like File Transfer Protocol (FTP), Rclone, or Mega. Before exfiltration, the group often runs PowerShell scripts to compress or encrypt the collected data.

BianLian actors have exploited CVE-2022-37969, a vulnerability impacting Windows 10 and 11 systems, to escalate their privileges. They use external proxies like Rsocks to establish SOCKS5 network tunnels, masking the destination of their C2 traffic.

The group initially operated under a double-extortion model, encrypting systems after data exfiltration. However, starting in January 2023, they shifted primarily to an exfiltration-based extortion approach and moved to exclusively extorting victims through data theft around January 2024. They typically threaten to release stolen data unless the victim pays a ransom.

BianLian's ransomware is written in Go and includes several anti-analysis techniques. For example, they rename binaries and create scheduled tasks that mimic legitimate Windows services or security products. Additionally, they often pack executables using UPX to conceal their code and evade heuristic detection.

For persistence and lateral movement, the group created domain admin accounts, compromised Azure AD accounts, and used them to move across networks. They have also installed web shells on compromised Exchange servers to maintain access.

Black Basta

DOUBLE-EXTORTION RANSOMWARE GROUP

Black Basta has impacted over 500 organizations across multiple industries—including critical infrastructure—in North America, Europe, and Australia. The group typically gains initial access through phishing and exploiting known vulnerabilities, then employs a double-extortion tactic, encrypting systems and exfiltrating data. Ransom notes generally don't include a payment demand but provide a unique code and a .onion URL for victims to contact the group via Tor. Victims are given 10–12 days to pay before their stolen data is published on the Black Basta site, Basta News.

Victims are given 10–12 days to pay before their stolen data is published on the Black Basta site, Basta News.

In May 2024, Black Basta affiliates launched a social engineering campaign targeting users with spam emails from legitimate sources, such as subscriptions and website registrations. They followed up with phone calls, posing as technical support, and persuaded victims to download remote access tools such as AnyDesk or Microsoft Quick Assist.

By October 2024, this campaign expanded to include Microsoft Teams. Attackers used legitimate Teams accounts to message victims, once again posing as technical support and urging them to install remote access tools. The goal remained consistent: to gain unauthorized access to victim's systems.

BlackSuit

DOUBLE-EXTORTION RANSOMWARE GROUP

BlackSuit is a high-profile double-extortion ransomware group that emerged in early April 2023 and is known for attacking healthcare and educational sectors, along with various other industries.

It shares many code similarities with the Royal ransomware, which is itself an offshoot of the infamous Conti ransomware used by WizardSpider, an advanced, financially motivated Russian cybercrime group responsible for countless attacks since 2016.

BlackSuit uses advanced encryption and stealth techniques that evade most security tools by implanting shellcodes in legitimate software. An example can be found in our blog.

They also operate a dark web leak site where they publish stolen data from their victims to add extortion pressure to pay the ransom.

8base

DOUBLE-EXTORTION RANSOMWARE GROUP

8Base's malware gains access to target systems primarily through phishing emails. Once infected, it acts as double-extortion ransomware, encrypting and stealing data. It enumerates connected drives, identifies data files, and encrypts them with AES-256 in CBC mode, appending the .8base extension to the files. The group then threatens to expose the stolen data if the victim refuses to pay.

8Base employs a

"NAME-AND-SHAME"

tactic, claiming to target organizations that have neglected data privacy and security.

They use their leak site to release confidential information in an attempt to damage the victim's reputation and brand.

Most of 8Base's targets are in the professional services industry, including accounting, legal services, and business service providers. However, companies in retail, manufacturing, construction, finance, insurance, and healthcare have also been affected.

8Base has drawn attention for its similarities to the RansomHouse ransomware group, particularly regarding its ransom notes and content on its leak sites.

Top Banking Trojans/Stealers/Spyware

Banking Trojans, stealers, and spyware remained persistent threats throughout 2024, with threat actors continuously evolving their tactics to bypass security measures and steal sensitive financial data. These malware families primarily focused on credential theft, banking information extraction, and cryptocurrency wallet targeting, with some variants incorporating advanced evasion techniques and modular architectures to enhance their effectiveness.

8%

Cryxos

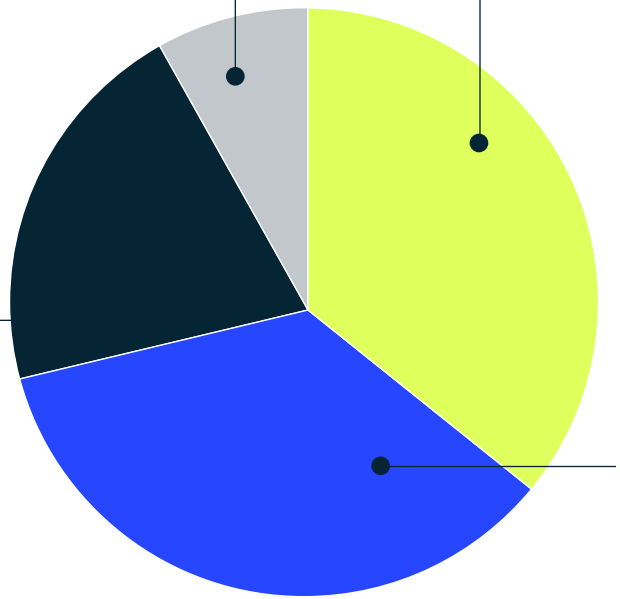
Cryxos is Trojan Scareware malware. It displays alarming notifications in an attempt to fool users into calling tech support scam centers. It uses JavaScript to display messages inside legitimate websites to add a layer of credibility and compel action. This happens after it is deployed by a dropper, another malware responsible for the initial infection.

20.6%

Berbew

Berbew is a Trojan designed to steal user passwords, with a particular focus on banking and financial institutions. It operates as both an infostealer, capturing and transmitting stored passwords to a remote server, and as a proxy, enabling attackers to use the compromised system for C2 functions or to deliver additional malware.

The Trojan spreads through users opening suspicious email attachments, running downloaded programs, or utilizing peer-to-peer file sharing. A notable feature of Berbew is its use of COM hijacking. This technique ensures persistence and allows the malware to escalate privileges on the infected system, giving attackers ongoing access.



35.7%

Pony

Pony Stealer is a dangerous password-stealing malware that can decrypt or unlock passwords for various applications, including VPNs, FTP, email, instant messaging, and web browsers. The malware collects information about the system and users, steals credentials, and can download additional malware or send stolen data to a C2 server.

Since 2011, Pony Stealer has been primarily used by criminal groups aiming to steal data and money. It continues to target users in Europe and America, leveraging its ability to steal credentials, persist on infected devices, and serve as a bot for further attacks.

35.7%

Grandoreiro

Grandoreiro is a banking Trojan that spreads via phishing emails. It often uses malicious attachments or links to fake websites to impersonate legitimate organizations like banks. Operated as a Malware-as-a-Service (MaaS), it has evolved significantly. Updates include improved decryption and domain-generation algorithms, as well as the ability to use Microsoft Outlook on infected machines to send further phishing emails.

In 2024, Grandoreiro targeted 1,800 banks and crypto wallets across about 50 countries, accounting for about 5% of banking trojan attacks. The malware has improved its evasion tactics, mimicking real user behavior by recording and replaying mouse movements to bypass machine learning–based security systems. It also introduced a CAPTCHA mechanism before executing its main payload to avoid detection by sandbox analysis tools.

Other Notable Malware

Expiro

Expiro is a family of file-infecting malware that embeds itself into legitimate executables. It often enables the theft of sensitive data and grants unauthorized access to infected systems.

IFramer

iFramer is malware that silently injects hidden iframes into compromised websites, redirecting unsuspecting visitors to harmful content or exploit kits.

Cobalt Strike Beacon

Cobalt Strike is a commercial red-team penetration testing tool that is frequently misused by cybercriminals to gain unauthorized access, deliver malicious payloads, and coordinate sophisticated attacks.

Snojan

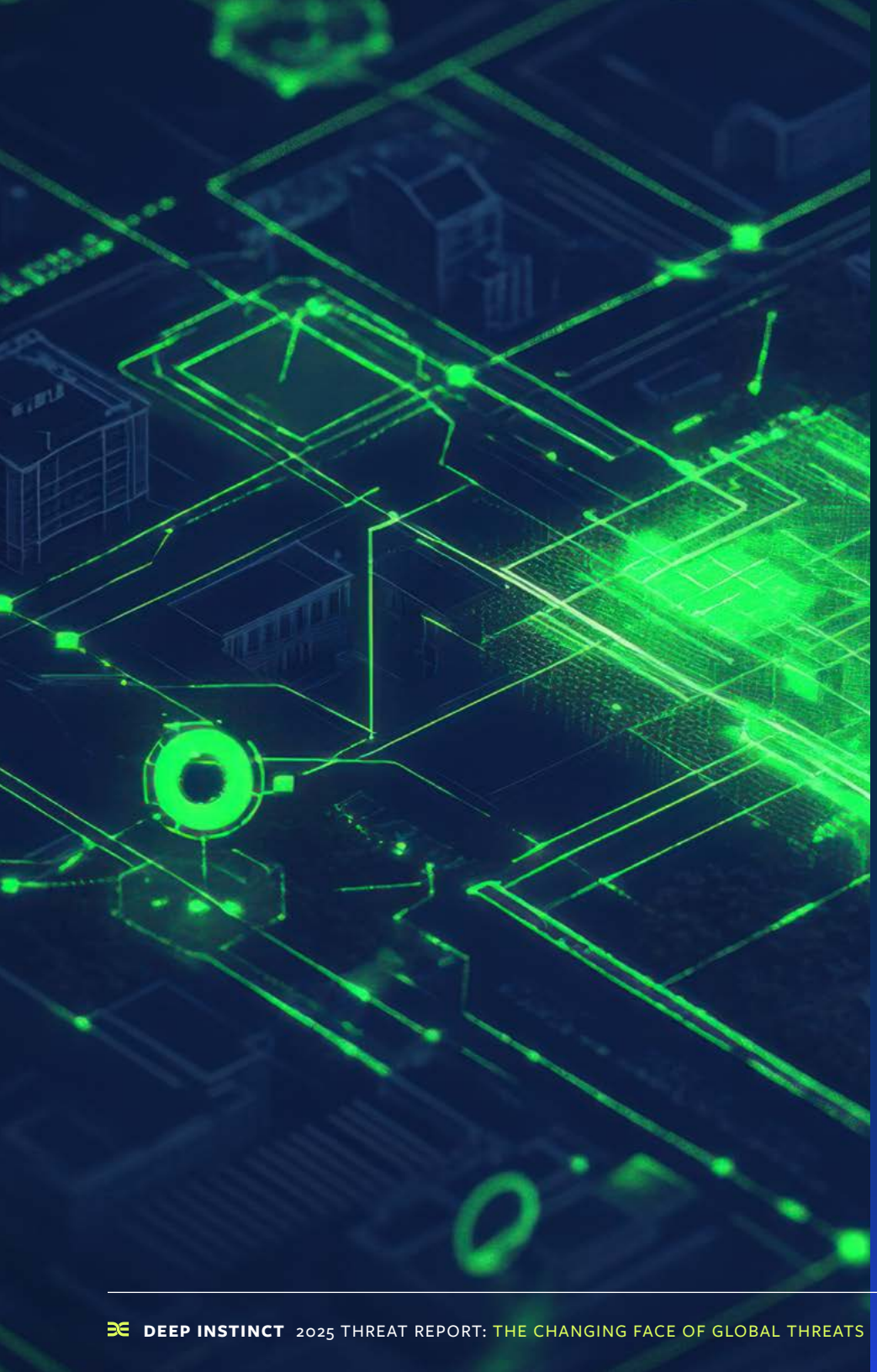
Snojan is a type of Trojan malware that infiltrates systems to steal sensitive data and enable remote attackers to access compromised devices. It disguises itself within legitimate software, making detection and removal more difficult for users and security tools.

Cosmu

Cosmu is a Trojan malware family that typically downloads malicious components, collects sensitive information, and provides attackers with unauthorized remote control over compromised systems.

Top Takeaways

The cybersecurity landscape of 2024 was marked by several significant shifts in how threat actors operate and how the global community responds. The following key developments highlight the evolving nature of cyber threats and the increasing sophistication of both attacks and defensive measures.



TOP TAKEAWAYS

Ransomware Disclosures, Sanctions, and Their Impact on Criminal Groups

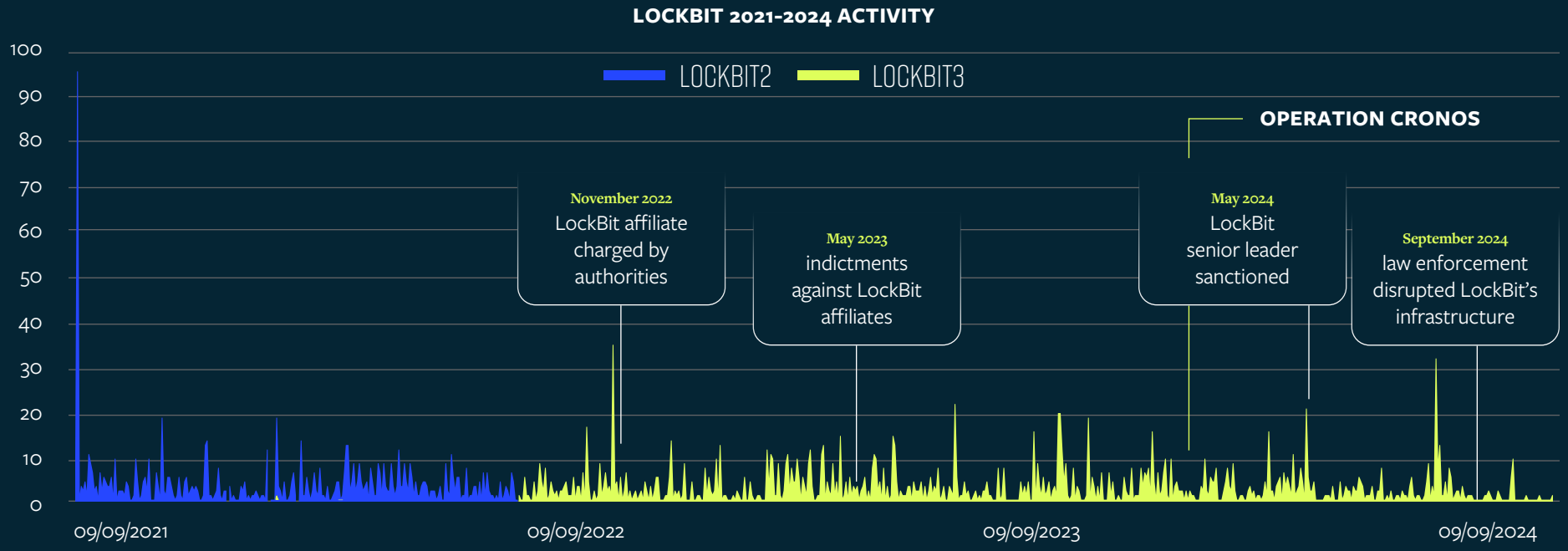
Governments use ransomware disclosures and sanctions to combat cybercriminal groups.

Disclosures by agencies like the U.S. Department of Justice (DOJ) and international partners provide public information about ransomware tactics, operations, and specific threat actors. These efforts often accompany sanctions, such as freezing assets, blocking cryptocurrency transactions, and targeting infrastructure used by ransomware groups.

Sanctions aim to disrupt these groups' financial networks, making it harder for them to profit from attacks. High-profile actions, like dismantling Hive's infrastructure and sanctions against LockBit affiliates, weaken groups' operational capabilities and deter affiliates. However, these measures are not foolproof; many groups adapt, rebrand, or shift operations to evade law enforcement.

While disclosures and sanctions do not eliminate ransomware, they reduce its effectiveness and signal increased accountability for cybercriminal activities.

The Impact of Sanctions and Disclosures on the LockBit Ransomware Group



November 2022

Mikhail Vasiliev, a LockBit affiliate, was charged by U.S. authorities for his involvement in LockBit ransomware operations.

May 2023

The U.S. Department of Justice unsealed indictments against Mikhail Matveev for deploying LockBit ransomware and other ransomware variants. He was tied to attacks on various entities, including the Washington D.C. Metropolitan Police Department. A $10 million reward was announced for information leading to his arrest.

In a coordinated operation across 11 countries called "Operation Cronos," law enforcement agencies delivered a major setback to the notorious LockBit ransomware group through a joint initiative.

May 2024

The U.S. Treasury, in collaboration with the U.K. and Australia, sanctioned Dmitry Khoroshev, a senior leader of LockBit. This included unsealing an indictment and revealing his role in developing and deploying LockBit ransomware.

September 2024

A coordinated U.S. and U.K. law enforcement operation disrupted LockBit's infrastructure, including U.S.-based servers used to facilitate data exfiltration. This operation was presented as a major blow to LockBit's global operations

Figure 11: Activity timeline with key actions and publications about the LockBit ransomware gang

Sanctions and public disclosures about the group do make an impact. However, typically, each time a task force targets LockBit, the group quickly bounces back, much like a persistent game of whack-a-mole.

Since the recent sanctions and publications in the Cronos operation, however, we have seen a steady decline in the group's activities. From this, we can conclude that it can be effective when a coalition of countries works together to target ransomware groups, and not all hope is lost in the fight against cybercrime.

Figure 12: Law enforcement announcement on "Operation Cronos"

The Rise of Data Brokers as an Adaptation to Sanctions and Disclosures

As government enforcement measures, sanctions, and arrests target ransomware groups, the criminal ecosystem adapts by employing specialized data brokers to handle stolen data. These brokers serve as intermediaries, facilitating the sale of sensitive information on darknet markets and reducing the operational complexity for smaller or fragmented criminal crews. This shift in roles and compartmentalization helps the ransomware economy persist despite heightened pressure from international law enforcement.

As shown earlier in this report, Dispossessor, one of the top ransomware players this year, does not appear to have ransomware capabilities. Instead, it functions more accurately as a data broker. Since no instances of their ransomware have been observed, it is evident that they primarily publish data leaks from other groups, including those that are now defunct or have been shut down. This positions them as opportunistic threat actors.

Although the group never maintained active ransomware capabilities and primarily publicizes attacks carried out by affiliates of dismantled groups, there are still actions that can be taken. On August 12, 2024, the FBI's Cleveland office announced the disruption of the group, which included the dismantling of three U.S.-based servers, three UK-based servers, 18 German servers, eight U.S.-based criminal domains, and one German-based criminal domain. German authorities have identified twelve suspects from Germany, Ukraine, Russia, Kenya, Serbia, Lithuania, and the United Arab Emirates.

TOP TAKEAWAYS

The Rise in Cyberattacks Driven by Geopolitical Events

Major geopolitical conflicts in 2024 have increasingly moved into the cyber domain, with state and non-state actors weaponizing digital capabilities to advance their strategic objectives.

From the Israel–Hamas war to ongoing Russia–Ukraine and China–Taiwan tensions, cyber operations have become a critical theater of modern warfare, enabling everything from infrastructure disruption to information warfare. These cyber campaigns demonstrate how digital attacks now serve as both a precursor to and extension of physical conflict, while also providing nations with options for achieving strategic goals without direct military engagement.

Israel–Hamas War

Cyberterrorism has become a key element in the conflict between Israel and Hamas. Attacks from hackers and nation-state-backed groups, often operating through proxies influenced by Iran and others, have sharply increased. These cyberattacks target Israel's critical infrastructure, including media, energy, utilities, telecommunications, and transportation. Following the October 7th escalation, there has been a rise in cyber operations and threats directed at Jewish, Muslim, and Arab-American communities and institutions as well.

Hamas's cyber activities have been heavily supported by Iran, which has provided funding and assistance to bolster Hamas's online capabilities. In addition, international hacking groups from countries such as Sudan, Pakistan, and Russia have participated in cyberattacks against Israel.

Before the October 7, 2023, attacks, Hamas's cyber unit, Gaza Cybergang, gathered critical intelligence on Israeli military targets, which helped facilitate the assault. Hamas also employed phishing campaigns to steal personal data.

Other tactics included deploying wiper malware to destroy data, breaching databases to expose personal information, and hijacking digital billboards to display Palestinian flags and spread false news about military victories. These cyber efforts are designed to disrupt Israel and manipulate public opinion through misinformation.

Israel, a global leader in cyber warfare with advanced capabilities, has faced challenges in using these tools effectively against Hamas, as the group does not rely heavily on the internet. Israel's primary strategy has been to control Gaza's internet connectivity, as it oversees the region's electricity and internet infrastructure.

On October 27, 2023, Israel imposed a 34-hour telecommunications blackout in Gaza, severely disrupting communication and medical services, which drew criticism from international organizations. Since then, similar internet shutdowns have occurred, leaving Gaza with only 15% of its usual internet connectivity.

When internet access was available, pro-Israeli hacktivists targeted Palestinian websites, including the Gaza Now news site. According to Cloudflare, denial-of-service (DoS) attacks accounted for 60% of the traffic to Palestinian websites, mostly targeting banks and tech companies.

Russia–Ukraine War

In 2024, Russian operatives intensified their cyber campaigns against Ukraine and its allies, strategically aligning these efforts with their military goals and wider geopolitical objectives. They also significantly escalated their cyberattacks on the UK and other NATO countries, especially those providing military assistance to Ukraine, aiming to weaken global support for Ukraine. The UK, in particular, has faced an increase in attacks and a more sophisticated cyber threat landscape, with state-backed groups like Sandworm and APT29, as well as private groups operating with the Kremlin's approval, focusing their attacks on the UK. These attacks have intensified amid rising geopolitical tensions, focusing on critical infrastructure, government agencies, defense organizations, and supply chains. Tactics have included espionage through spear-phishing, the deployment of destructive malware, and disruptions to supply chains.

In response, the UK's National Cyber Security Centre responded to more than 430 cyber incidents in 2024, highlighting a marked increase in both the scale and severity of these threats.

China–Taiwan Tension

The conflict between China and Taiwan revolves around China's claim that Taiwan is part of its territory. China is pursuing what it claims is reunification, while Taiwan prioritizes its independence and sovereignty. As tensions rise, cyberattacks have escalated, primarily because China is attempting to influence Taiwan and achieve its goal of annexation without resorting to military invasion. The Chinese People's Liberation Army (PLA) considers cyber dominance essential, not just in the early stages of a conflict, but as a continuous advantage to maintain.

Taiwan has been targeted by numerous cyberattacks from Chinese hacking groups such as Earth Lusca and RedJuliett, with a particularly sharp increase in attacks during Taiwan's January 2024 elections. This ongoing cyber strategy aligns with China's broader goal of reunification, using cyber tactics to weaken Taiwan's defenses, influence its political landscape, and discourage international support.

Taiwan is primarily focused on improving the defense of its systems and networks, and occasionally, Taiwanese hacking groups launch attacks against China. One group, known as "Anonymous 64," has targeted China, Hong Kong, and Macau, executing attacks to disseminate anti-China messages.

TOP TAKEAWAYS

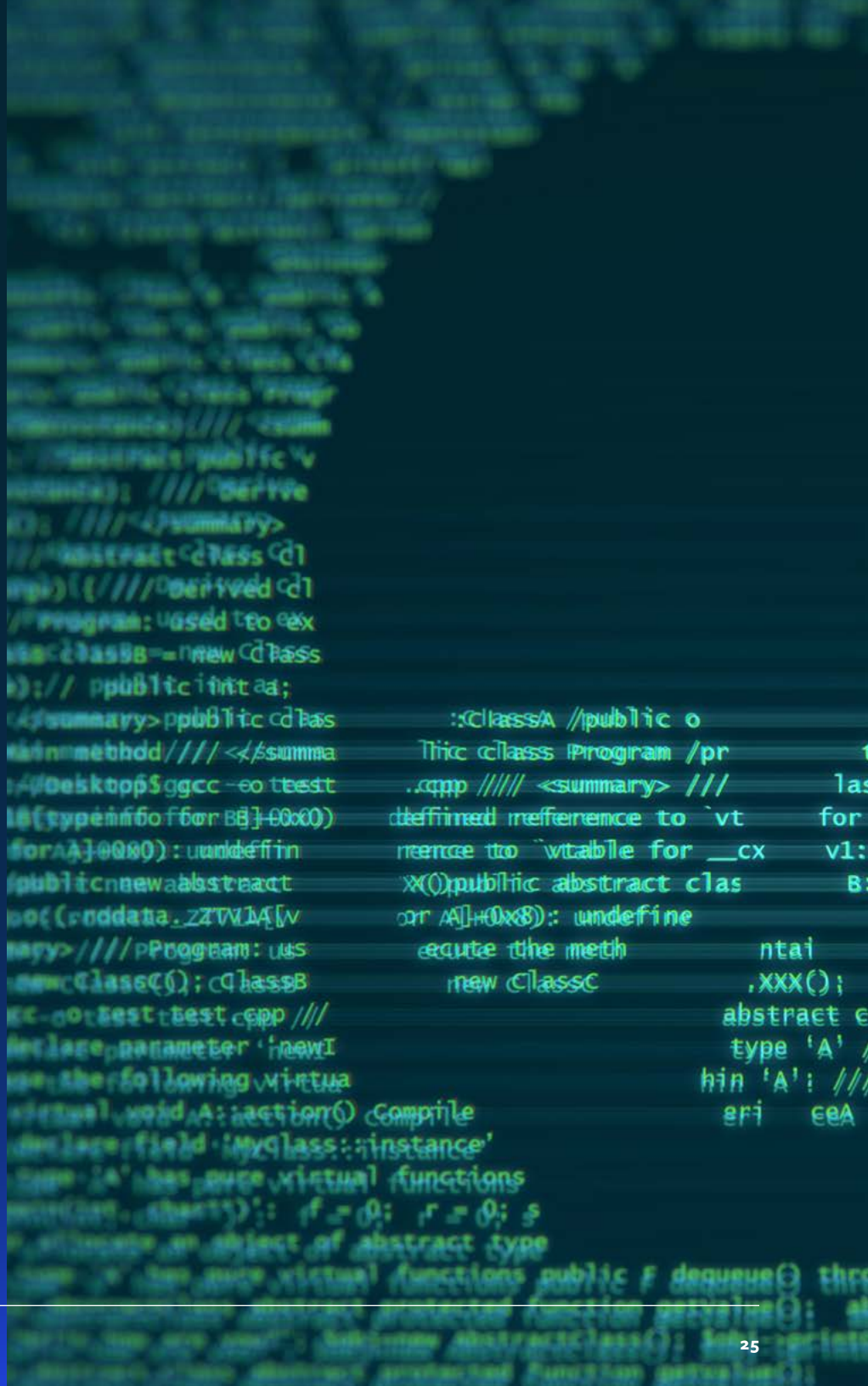
AI-Based Attacks

Artificial Intelligence (AI) and Large Language Models (LLMs) have revolutionized various industries by enabling unprecedented efficiency and innovation. However, cybercriminals are increasingly exploiting these capabilities to conduct more sophisticated, efficient, and scalable attacks, representing a growing threat.

AI enables attackers to automate tasks that previously required human expertise. For instance, AI-powered malware can dynamically adapt to evade detection by learning from the behavior of security tools. Attackers are also leveraging AI to identify vulnerabilities in networks and systems, reducing the time required for reconnaissance. Phishing campaigns have also benefited from the use of AI, becoming more convincing and personalized as AI models analyze social media and other public data to craft highly targeted messages.

AI-driven malware represents another alarming trend as AI helps generate polymorphic malware that changes its code structure to bypass detection mechanisms, making it increasingly difficult for traditional antivirus and endpoint detection tools to identify threats. In the beginning of the LLM era, we demonstrated how LLMs can generate evasive malware.

While AI holds immense potential for positive impact, its dual-use nature makes it a double-edged sword. The cybersecurity community must remain vigilant and innovative to counteract the growing sophistication of AI-driven cyber threats.



Vulnerabilities on the Rise

Overall, there were 186 known exploited vulnerabilities in 2024. The top most-exploited vulnerabilities were in various Microsoft products, representing nearly 20% of all known exploited vulnerabilities. This pattern remains constant due to the vast number of users relying on these systems. However, a concerning trend is the increased exploitation of vulnerabilities in leading network security and IT solutions that touch multitudes of organizations and users.

The top exploited vulnerabilities are related to 64 different vendors. Forty of them are in cyber and IT and the remaining are in the media, hardware, and other similar industries. At least 24 vulnerabilities are known to be used for massive ransomware infection campaigns. This broad range of targets emphasizes the need for a multilayered defense strategy and shift in global cybersecurity paradigms.

As illustrated in the graph below, the latter part of the year saw a noticeable spike in vulnerability exploitation—a trend that has also been observed in previous years. This trend repeats itself every year. As such, we can expect a decrease in vulnerabilities exploited in the wild to start 2025, rising as we get closer to the end of the year. Major geopolitical changes in early- to mid-2025 may affect this trend.

Vulnerabilities Exploited in the Wild

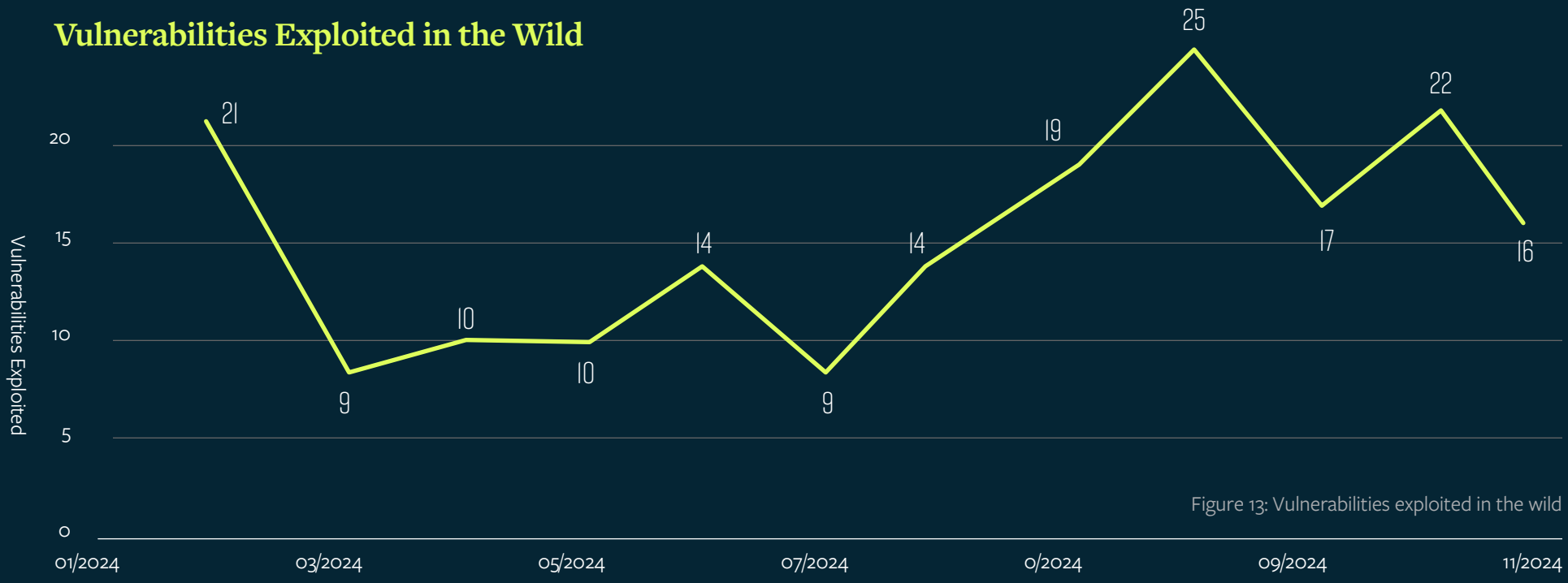


Figure 13: Vulnerabilities exploited in the wild

Predictions

Based on the trends and developments observed throughout 2024, several key patterns are emerging that will shape the threat landscape in 2025. The following predictions highlight areas where organizations should focus their defensive strategies and prepare for evolving challenges.

01 AI-Driven Attacks Will Increase the Amount of "Unknown" Malware

As AI-driven attacks become more common, we will see a big jump in malware that security teams have not encountered before. The old method of catching bad software—relying on known signatures and patterns—won't cut it. AI makes it easy for attackers to continuously change tactics. They can generate brand-new types of malware or endlessly tweak existing ones, so they never look like what we've seen before.

Today's cybercriminals can use machine learning to churn out polymorphic and metamorphic malware. Put simply, this means the malicious code can change every time it runs, making it a nightmare for legacy, signature-based detection tools. On top of that, AI can quickly learn how security systems and people respond and then adapt attacks in real time. So, even if we manage to catch a new type of malware once, the attacker can instantly modify it to slip under the radar next time. The end result? An alarming rise in these "unknown" threats that leave security teams struggling to figure out what they're up against—and how to stop it.

At the end of 2024 we also demonstrated a full attack life cycle operated by an LLM, including a self-guided malware with an LLM-based C2, a tactic which may drastically increase the number of cyberattacks. We have also noticed new threat groups are relying on LLM-generated code. All that may introduce a new type of hacker, an evolution of "Script Kiddies"; let's call them "AI-Hacking Kiddies."

02 Cybercrime Groups Will Increasingly Operate Like Tech Startups

Unsurprisingly, the top threat groups have adopted startup-like organizational structures, complete with HR, standardized hiring processes, finance divisions, developers, contractor networks, and infrastructure. We explored some of these trends in our previously published Conti Report by Deep Instinct Threat Lab Researchers. In the coming years, including 2025, the threat ecosystem will become more collaborative, with "freelancers" offering specialized services like malware development or initial access brokering.

As "affiliate programs" grow in popularity, insider attacks will become more frequent and more difficult to detect during the initial stages.

Ironically, the increasing pressure from law enforcement and government agencies, such as the FBI, Europol, and other cybercrime units, has forced threat actors to maintain operational efficiency, adaptability, and secrecy in the face of heightened scrutiny and takedown efforts. To achieve their goals, threat actors have evolved into sophisticated organizations featuring company-like structures.

During 2024, there were multiple cases where law enforcement arrested key members of threat actor groups, only to see the threat group survive and continue malicious activities due to their flexible structures.

03 Digital Transformation Will Increase Attack Surface

The global digitalization trend over recent years has been characterized by exponential growth in data creation, storage, and utilization, driven by advances in technology, increasing connectivity, and the adoption of digital-first strategies across sectors.

The approximate global data volume exceeded 150ZB in 2024, fueled by the COVID-19 pandemic, which accelerated remote work, e-commerce, and virtual communication.

In 2025, we can expect around 180ZB of global data due to an increase in IoT devices, real-time data growth, and continued digitalization.

Because of this growth, threat actors are more eager to operate and have a broader surface to attack—each cyberattack has a more destructive impact.

04 IoT-Based Attacks Will Surge as Connected Devices Proliferate

Internet of Things (IoT) devices account for more than 30% of all network-connected business endpoints. Concurrently, the rate of attacks on IoT devices has quadrupled in the past two years. This trend will continue as more devices become networked. Some key examples of malware in the IoT field include the following:

Mirai malware infects IoT devices, converting them into remotely controlled bots. These infected devices form a botnet, enabling the execution of large-scale, volumetric DDoS attacks.

The Mirai botnet spreads by exploiting vulnerable IoT devices. It uses two main methods: default credentials (like "admin" and "password") and brute-force attacks, where it tries common username and password combinations to gain access.

Gafgyt, also known as Bashlite or Lizkebab, is another botnet malware (like Mirai) that targets IoT devices. It exploits weak or default credentials to gain control of the device. Gafgyt spreads by scanning for vulnerable devices. It has evolved over time, largely due to the leak of its source code, which has led to the creation of multiple variants and adaptations, making cybersecurity efforts more difficult.

IOCONTROL targets a wide range of devices, including routers, Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), IP cameras, firewalls, and fuel-management systems. It has affected devices from various manufacturers, such as D-Link, Hikvision, Baicells, Red Lion, Orpak, Phoenix Contact, Teltonika, and Unitronics. Amid ongoing geopolitical tensions, IOCONTROL is currently being used to target systems in Israel and the U.S. The malware is associated with an Iranian hacking group, CyberAv3ngers. Recently, OpenAI reported that this group has been utilizing ChatGPT to crack PLCs, create custom bash and Python exploit scripts, and strategize post-compromise activities.

05 Dual-Use Remote Management Tools Will Enable More Sophisticated Attacks

Dual-use Remote Management (RMM) tools have been used in tech support scams that fool users into enabling scammers to transfer funds out of their bank accounts remotely. This trend will continue to rise in 2025 and beyond. Various cyber criminals and APT groups also use them in the initial stages of their attacks. Combined with the use of legitimate cloud storage providers, proprietary encryption tools, and vulnerable drivers, all of these enable attackers with the ability to disguise themselves as legitimate operators to bypass security solutions.

Conclusion

The cybersecurity landscape of 2024 was marked by significant evolution in both attack sophistication and defensive measures. While ransomware remained a dominant threat, with groups like LockBit and RansomHub leading the charge, the emergence of AI-powered attacks and the increasing professionalization of cybercrime groups signaled a concerning shift in the threat landscape. The year also demonstrated how geopolitical conflicts increasingly spilled into the cyber domain, with state-sponsored attacks and hacktivism becoming more prevalent in conflicts such as the Israel–Hamas war and ongoing tensions between Russia and Ukraine.

Looking ahead, organizations must prepare for an increasingly complex threat environment where AI-driven attacks will generate more unknown malware variants, IoT devices will face heightened targeting, and cybercrime groups will continue to operate with greater sophistication and business-like efficiency. Success in this evolving landscape will require a paradigm shift in security strategies, emphasizing preemptive threat postures, comprehensive security frameworks, and the adoption of zero-day data security strategies capable of detecting and preventing both known and unknown threats before they can impact operations.

Organizations must prepare for an increasingly complex threat environment where AI-driven attacks will generate more unknown malware variants

Research Methodology

As a customer-centric research team, Deep Instinct is uniquely positioned to monitor the threat landscape, providing our customers with actionable insights and intelligence as a trusted vendor. Our team's ongoing efforts to monitor and analyze the world's most sophisticated threats help us better understand how attacks evolve, enabling us to anticipate and prepare for emerging ones. Through our proactive research and analysis, we identify new threats and trends before they impact our customers.

Each year, we publish a biannual and annual threat report to shed light on these findings, helping our customers become better prepared for the threats they can see—and the ones they can't. This year's report combines publicly available data and proprietary research into threat groups and ransomware.

We identify new threats and trends before they impact our customers

ABOUT DEEP INSTINCT

Deep Instinct, the first and only zero-day data security company built on a deep learning cybersecurity framework, prevents unknown threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct Data Security X (DSX) secures data at-rest or in-motion—across cloud, NAS, applications, and endpoints.

Fight AI with the best AI. DSX Brain, Deep Instinct's deep learning framework, prevents zero-day threats that no one else can find, with >99% accuracy and a <0.1% false positive rate. DIANNA, the DSX Companion, leverages GenAI to provide unparalleled explainability into unknown threats in <10 seconds.

www.deepinstinct.com | info@deepinstinct.com