INTEL 471 ANNUAL THREAT REPORT 2024 & OUTLOOK FOR 2025

— A Year of Law Enforcement Wins as RansomHub and Infostealer Malware Threats Rise

Contents

Key findings

- Numerous law enforcement operations impacted the underground in 2024, including the disruption of the LockBit ransomware-as-a-service (RaaS), the disruption of the IcedID, SystemBC, Pikabot, SmokeLoader, Bumblebee and Trickbot botnets and the disruption of the RedLine and Meta information-stealer malware infrastructure.
- We reported 3,985 ransomware breach events in 2024. The LockBit group claimed responsibility for more than 10% of the total breaches, followed by RansomHub, Play, Akira, and Hunters International.
- We observed and reported 3,977 claims from initial access brokers (IABs) offering to sell compromised credentials and/or alleged unauthorized access to networks or systems in 2024. Of that total, about 80% fell into the category of wholesale access.
- We reported 516 vulnerabilities in 2024. Of these, 30% were classified as high risk, 46% as medium risk, and 24% as low risk. Among the reported vulnerabilities, 9% were productized, 56% were weaponized, and 19% had proof-of-concept (PoC) code available.
- Our coverage of hacktivist activity in 2024 was dominated by the war in Ukraine and the Israeli-Palestinian conflict. Additionally, many hacktivist groups formed alliances, and NoName057(16) led our coverage in terms of the volume of operations.

Intelligence cutoff date (ICOD) for data analysis: Dec. 15, 2024

Introduction

2024 was a frenetic year for the underground, with law enforcement operations impeding and at times upending mature cyber criminal enterprises. In ransomware, we saw the slow decline of the ransomware-as-a-service (RaaS) leader LockBit following Operation Cronos and consequently the rapid rise of RansomHub in its place. From the very start of the year and throughout, we were reminded of the far-reaching, insidious threat of vulnerabilities and the panic they can engender. This was all the more telling given the frequency with which extortion groups relied on vulnerabilities for initial access. Meanwhile, embattled malware operators sought to mitigate the damages of successful botnet disruptions through the adoption of novel campaigns, and the information stealer cemented its position as the most impactful malware threat. Lastly, a review of 2024 would not be complete without a look at the most exciting, yet sometimes confusing, developing technology — artificial intelligence (AI).

2024 at a Glance

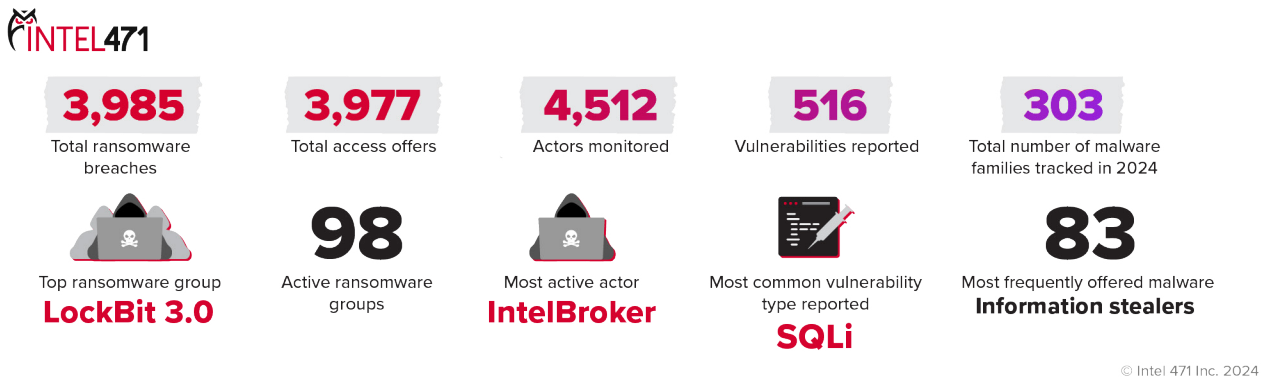


Figure 1: The image depicts an infographic detailing key statistics for 2024.

Major Events of 2024

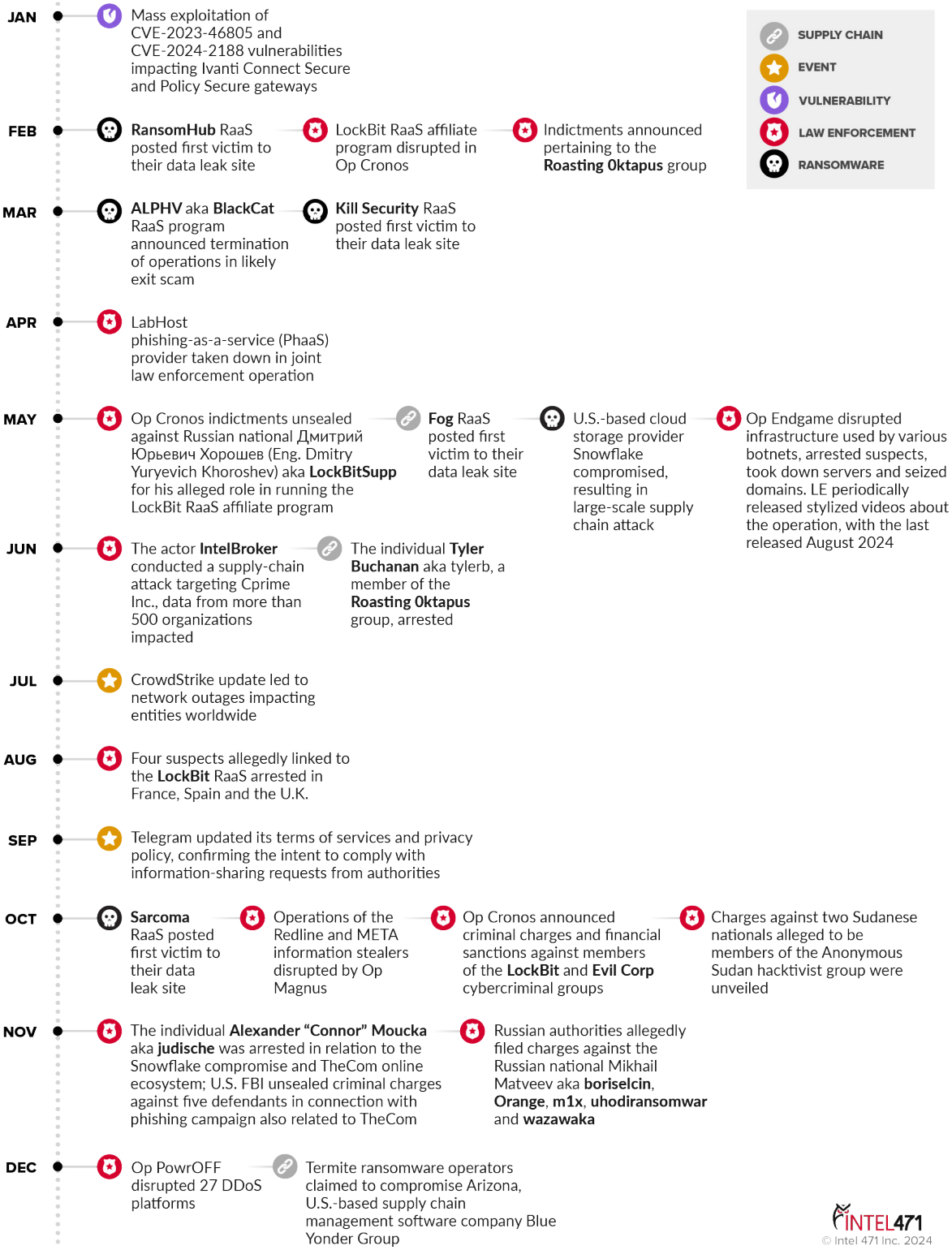


Figure 2: The image depicts a timeline detailing key events for 2024.

Law Enforcement Operations

The cybercriminal underground historically has been shaped by global law enforcement operations that target key actors and infrastructure, and this was never more apparent than in 2024. A consistent cadence of operations throughout the year contributed to a slowing of some of the most maligned cyber threats, including ransomware and the proliferation of malware. The scale of the operations was grand, with the targeting of the biggest name in ransomware and the disruption of some of the most mature botnet operations active in the underground. The impressive impact law enforcement agencies were able to effectuate was in part due to the adoption of aggressive media campaigns where they implemented baiting techniques that were picked up and amplified in open source and the underground. Furthermore, a steady flow of sanctions against cybercriminals — past and present — demonstrated the possible ramifications of a life of crime and thrust those impacted into the limelight.

The most impactful operations witnessed this year included:

Op Cronos

On Feb. 20, 2024, the U.K.'s National Crime Agency (NCA) and the U.S. FBI announced the disruption of the LockBit RaaS as a result of Operation Cronos, a coordinated effort involving law enforcement agencies from 10 countries. This sparked a sequence of events in which the NCA obtained more than 1,000 LockBit ransomware decryption keys, numerous **LockBit** and **Evil Corp** members were indicted, numerous individuals linked to **LockBit** were indicted or arrested across the globe and more than 200 cryptocurrency accounts linked to the group were frozen.[1, 2, 3, 4]

Op Endgame

From May 27, 2024, to May 29, 2024, the European Union Agency for Law Enforcement Cooperation (Europol) and law enforcement agencies from several countries targeted multiple malware droppers including IcedID, SystemBC, Pikabot, SmokeLoader, Bumblebee and Trickbot in the "largest ever operation against botnets." On May 30, 2024, Europol announced the joint operation dubbed Operation Endgame resulted in the disruption of infrastructure used by the botnets, as well as arrests, server takedowns and domain seizures. The operation was initiated and led by officers in France, Germany and the Netherlands and supported by the European Union Agency for Criminal Justice Cooperation (Eurojust) and several other countries. It led to four arrests — one in Armenia and three in Ukraine — 16 location searches, the takedown of more than 100 servers and law enforcement taking control of more than 2,000 domains. Additionally, Europol added eight additional fugitives linked to this criminal activity to Europe's Most Wanted list.

From May 31, 2024, to Aug. 8, 2024, Europol officials released eight stylized videos on its website dedicated to Operation Endgame where they revealed actor names and provided cryptic clues regarding their operations. In September 2024, Europol released a teaser for season two, which appears to indicate underground cryptocurrency exchanges would be the next target.[5, 6]

Op Magnus

On Oct. 28, 2024, we observed discussions on social media about a disruption operation ostensibly by the Dutch National Police and international law enforcement partners against the RedLine and Meta information-stealer malware infrastructure. The following day, Dutch and U.S. authorities confirmed a disruption operation against the RedLine and Meta information-stealing malware dubbed Operation Magnus. The coordinated law enforcement action reportedly resulted in the seizure of two domains and three command-and-control (C2) servers supporting the stealers. Multiple associated Telegram channels were taken offline and millions of compromised victim credentials were recovered. Additionally, U.S. authorities unsealed charges against **Maxim Rudometov**, an alleged developer of RedLine.[7, 8]

TheCom charges, arrests

TheCom is a broad online ecosystem composed of diverse communities and individuals with a significant number of youths operating mostly from Canada, the U.S. and the U.K. that engage in cybercriminal activities such as subscriber identity module (SIM) card-swapping, cryptocurrency theft, online harassment, swatting, bricking and corporate intrusions. This online ecosystem is assessed as the origin of high-profile threat groups over the past years including **LAPSUS$**, **Roasting 0ktapus** and the **Scattered Spider**, **UNC3944**, **Octo Tempest** and **Muddled Libra** intrusion clusters.[9]

Several individuals were charged or arrested in law enforcement operations targeting cybercriminals linked to **TheCom** this year that included:

- In January 2024, the U.S. Department of Justice (DOJ) announced details of an indictment with a series of charges against the individual **Noah Michael Urban** aka **Sosa**, **Elijah**, **King Bob**, **Anthony Ramirez**, linked with the **Roasting 0ktapus** group.
- In June 2024, the Spanish National Police and the U.S. FBI announced a U.K. national allegedly involved in a spree of corporate intrusions was arrested in a joint operation. The individual was identified as **Tyler Buchanan** aka **tylerb**, another member of the **Roasting 0ktapus** group.
- In October 2024, an FBI special agent filed a criminal complaint charging the individual **Remington Goy Ogletree** aka **remi** with wire fraud in relation to alleged crimes linked to the **Scattered Spider** intrusion cluster.

- In October 2024, **Alexander "Connor" Moucka** aka **judische** was taken into custody on a provisional arrest warrant, according to Canada's Department of Justice. The actor was linked to the large-scale supply chain attack impacting the U.S.-based cloud storage provider Snowflake.
- In November 2024, the FBI unsealed criminal charges against five defendants in connection with a phishing campaign — **Ahmed Hossam Eldin Elbadawy** aka **AD**, **Noah Michael Urban** aka **Sosa**, **Evans Onyeaka Osiebo**, **Joel Martin Evans** aka **joeleoli** and **Tyler Robert Buchanan** aka **tylerb**. We previously linked **joeleoli** and **Sosa** to the **Roasting 0ktapus** group.[10, 11, 12]

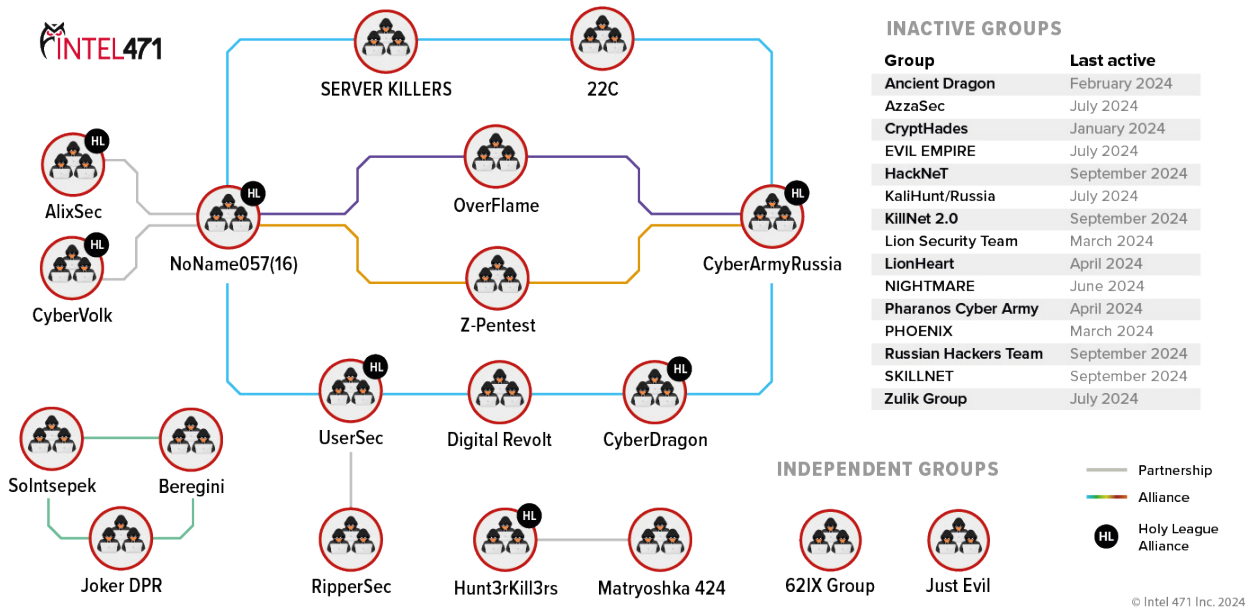
Op Passionflower

On Dec. 3, 2024, Europol announced the results of an international law enforcement operation named Operation Passionflower that targeted the Matrix aka Mactrix, Totalsec, X-quantum, Q-safe encrypted messaging platform. The platform's infrastructure consisted of more than 40 servers and was taken down by Dutch and French authorities with follow-up actions carried out by law enforcement agencies in Italy, Lithuania and Spain. Europol's statement revealed the authorities were monitoring the platform and intercepting communications for three months prior to the takedown. The operation came hot off the heels of Telegram updating its terms of services and privacy policy confirming the intent to comply with information sharing requests from authorities, including IP addresses and phone numbers.[13]

Hacktivism Gets Physical: Now Targeting Critical OT

As is often the case, the hacktivism scene is inextricably linked to global geopolitics. In 2024, there was no shortage of events that dictated the direction of travel for many of the key hacktivist groups we track. The pro-Russian hacktivism fraternity primarily focused on influencing the outcome of the Russia-Ukraine war by targeting governments or institutions that offered support to Ukraine while attempting to degrade Ukrainian infrastructure directly with attacks. The situation in Israel and the Palestinian territories developed into a humanitarian crisis that polarized governments and hacktivists. As a result, Israel was targeted repeatedly by a host of groups proclaiming to be ideologically motivated, however, among those likely were several state-associated groups. Away from conflict, a year of elections, sporting events and divisive politics provided ample opportunity for groups seeking to disrupt.

Pro-Russian Hacktivist Groups Reduce in Number, Maintain Operational Output



INACTIVE GROUPS

Group	Last active
Ancient Dragon	February 2024
AzzaSec	July 2024
CryptHades	January 2024
EVIL EMPIRE	July 2024
HackNeT	September 2024
KaliHunt/Russia	July 2024
KillNet 2.0	September 2024
Lion Security Team	March 2024
LionHeart	April 2024
NIGHTMARE	June 2024
Pharanos Cyber Army	April 2024
PHOENIX	March 2024
Russian Hackers Team	September 2024
SKILLNET	September 2024
Zulik Group	July 2024

Figure 3: The image depicts Intel 471's current understanding of the pro-Russian hacktivist landscape.

2024 was another dynamic year for pro-Russian hacktivists, with many groups forging new partnerships and alliances, and others that were active in previous years dropping away. For example, the much publicized **KillNet** and its various splinter groups slowed their operational cadence and came to a halt in September 2024. The spiritual successor **Just Evil**, run by the actor **KillMilk**, continued to demonstrate sporadic activity. One of the most active alliances was the triumvirate of **NoName057(16)**, **CyberArmyRussia** and **OverFlame**. The trio consistently targeted Ukraine and countries that demonstrated material or diplomatic support to Ukraine. The **CyberArmyRussia** group possibly has an association with the Russian state, supported by its leader's claim to have received recognition for its support to the Russian cause.[14] The **NoName057(16)** group most consistently led our coverage in terms of volume of operations, which likely contributed to its success in forging partnerships.

High Impact Hacktivist Operations

We tracked hundreds of operations coined by hacktivism groups in 2024. However, three stood out due to the persistence and number of organizations targeted:

- Op404 — The operation primarily was led by **NoName057(16)** and often used as a catch-all for Russia-Ukraine war-related targeting. Victims were from a variety of countries but most often involved the targeting of Ukraine. The campaign primarily focused on targeting regional and national entities in Ukraine with the most emphasis placed on any entities that fell within critical infrastructure sectors.[15]
- OpIsrael — This is an annual operation we have tracked since 2018. The operation usually takes place in April and historically acted as a vehicle for hacktivist groups to show their support to the Palestinian people. However, given the extraordinary year for Israel, the Palestinian territories and the region at large, the operation has been used throughout as a call to arms for a multitude of hacktivist groups. While the number of groups that have attached themselves to the conflict is in the hundreds, the groups most active this year were **Handala**, **1915 Team**, **Gaza Children's group** and **The Returnees**.
- OpFrance — This year was politically frantic for France. The country underwent a snap election, endured several protests and hosted the Olympics — one of the most watched events globally — all of which provided justification for hacktivist groups to wage disruptive campaigns that often fell under the OpFrance hashtag. Furthermore, French President Emmanuel Macron remained hawkish toward Russian President Vladimir Putin and Russia's intention in Europe, which galvanized many of the pro-Russian groups identified in figure 3.

New Tactics, Techniques, Procedures

Targeting operational technology systems

A trend we observed this year was the increased targeting of operational technology (OT) systems by hacktivist groups. The Islamic Revolutionary Guards Corps (IRGC)-associated **Cyber Av3ngers** group gained notoriety in late 2023 when it impacted both Israel- and U.S.-based infrastructure through the compromise of Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). A similar attack occurred in January 2024 when the **CyberArmyRussia** group claimed access to multiple U.S. water companies' supervisory control and data acquisition (SCADA) systems.[16] In September 2024, members of the Iranian **BLACK MASK TEAM** hacktivist group claimed to compromise 49 SCADA systems and human-machine interface (HMI) displays in multiple countries.[17] Success likely inspired similar attacks as the year wore on.

Sabotage-for-hire

In August 2024, we reported on the growing number of sabotage-for-hire offers on underground forums. The advertisements predominantly targeted individuals within

Ukraine and often would promise large sums of money for a variety of actions, which included conducting arson, border crossing, physical assaults, property damage and surveillance.[18] Later in the year, we witnessed these offers migrate to hacktivism communities — specifically those associated with the actor **KillMilk**, such as the **Just Evil** and **CROK** Telegram channels.[19, 20]

Summary

This year, we witnessed hacktivist groups become more akin to deniable tools of state power than the autonomous disruptive ideologues of the past. Anti-Israeli groups demonstrated this trend more profoundly, as numerous groups reportedly were associated with the Iranian intelligence apparatus. However, it is less clear with the pro-Russian cadre whether their actions are more influenced by the state or by nationalistic sentiment among the disaffected. Regardless, many hacktivist groups demonstrated a genuine understanding of geopolitics and were able to leverage global events to justify their actions. Their aims likely are to sway governmental decision-making and/or incur cost on their targets. In this vein, the trend of targeting OT is a growing concern since it enables hacktivist groups to have greater impact than traditional distributed denial-of-service (DDoS) or defacement attacks and also provides a vector into national infrastructure.

The Rise and Fall of Ransomware Leaders Amid Growing Variants

*The reporting metrics for this section were sourced from Intel 471 Breach Alerts and Information Reports and are not representative of all ransomware instances possibly claimed across the underground.**

Ransomware at a glance

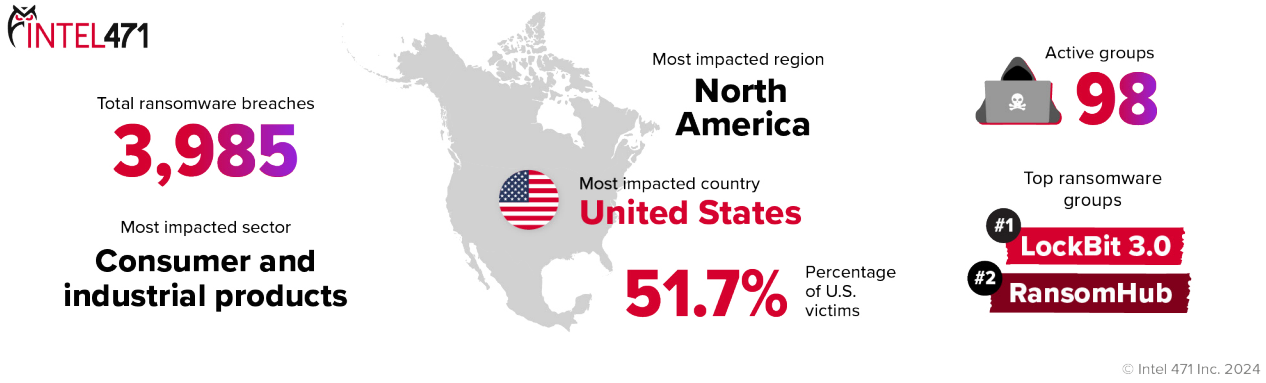


Figure 4: The image depicts an infographic detailing ransomware statistics for 2024.

We reported 3,985 ransomware breach events in 2024. The **LockBit** group stood out as the most prevalent, impacting 407 victims, followed by **RansomHub**, which impacted 395 victims. The next most impactful ransomware variants in descending order were Play, Akira and Hunters International. The U.S. was the most-impacted country at 51.69% of ransomware events, followed by Canada at 5.8% and the U.K. at 4.92%. North America was the most-targeted region with the most victims on a monthly basis, followed by Europe — continuing the trend observed in the previous year. The top three sectors most impacted by these offers in descending order were consumer and industrial products, professional services and consulting, and manufacturing.

The number of observed attacks each month primarily remained on the same level, with October experiencing the most activity and June the least. The RansomHub RaaS affiliate program took the lead as the most impactful group in the second half of 2024, claiming more than 300 breaches, with more than half of them listed from September to November. Additionally, the **Play**, **Akira** and **Hunters** International groups showed consistent activity throughout 2024.

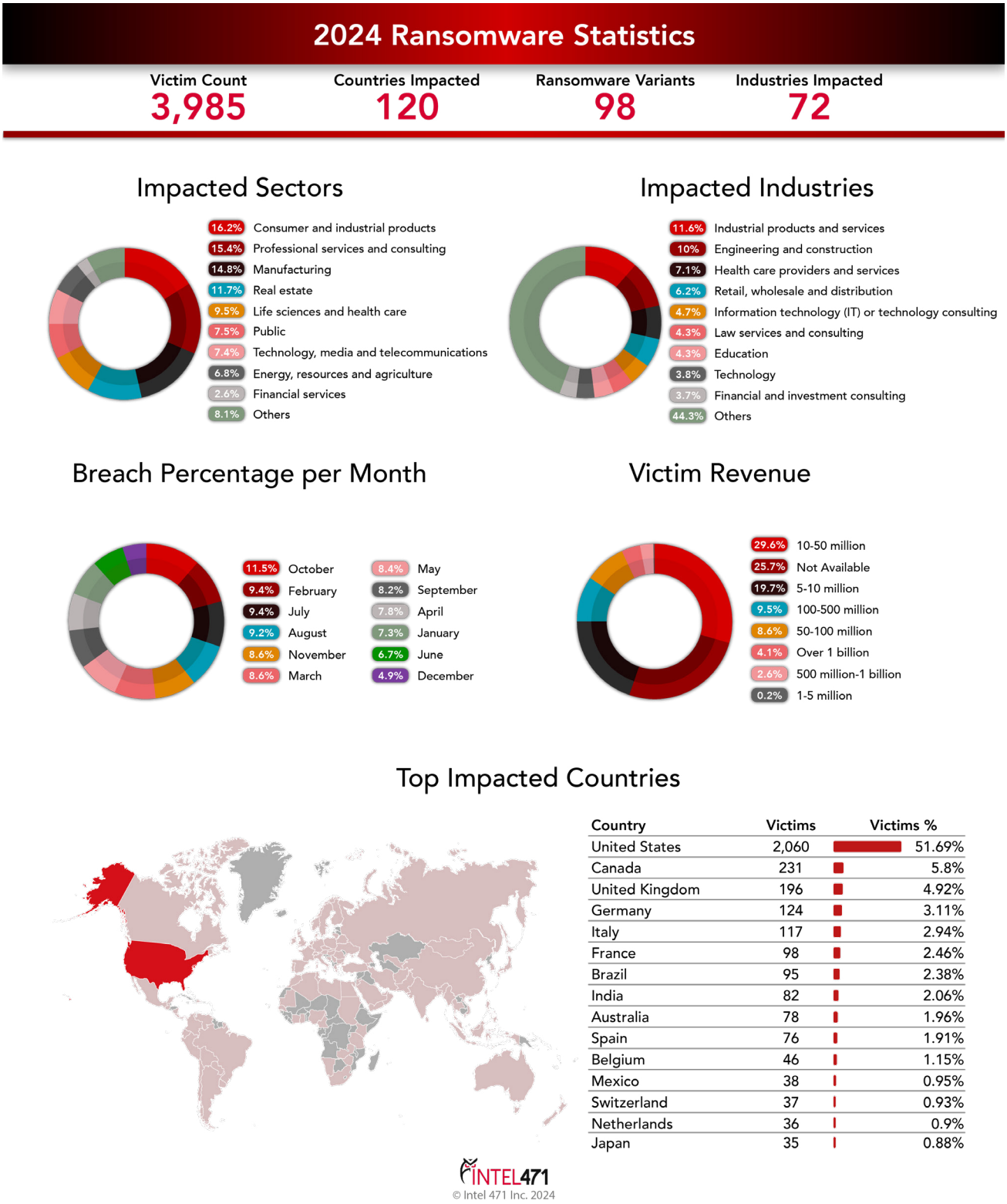


Figure 5: The image depicts a dashboard detailing ransomware statistics for 2024.

Fall of LockBit

In early 2024, the LockBit RaaS affiliate program was disrupted by Operation Cronos, which led to the takeover of the group's victim-shaming and data-leak blog, followed by a series of indictments and arrests of key **LockBit** affiliates, including an unsealed indictment against the Russian national **Дмитрий Юрьевич Хорошев** (Eng. **Dmitry Yuryevich Khoroshev**), an alleged leader of the program. The group relaunched its blog and became the most impactful collective in 2024 with 407 breaches, a significant drop compared to the 940 alleged victims during 2023. However, the legitimacy of the post-disruption victim claims remains questionable, with the NCA stating up to two-thirds of the high-profile victims were fabricated. This is a significant downturn in activity, which almost certainly was driven by reputational damages and the loss of capable affiliates. The group claimed only four victims in the fourth quarter of 2024, suggesting it likely is approaching its demise.

Operation Cronos recap

- The actor **LockBit** aka **LockBitSupp** claimed the CVE-2023-3824 improper restriction of operations within the bounds of a memory buffer vulnerability was exploited to gain access to the group's infrastructure.
- Two suspects allegedly implicated in the **LockBit** gang's activity were taken into custody Feb. 20, 2024, in Poland and Ukraine.
- On May 7, 2024, U.K. and U.S. law enforcement officers unsealed an indictment against Russian national **Дмитрий Юрьевич Хорошев** (Eng. **Dmitry Yuryevich Khoroshev**), born April 17, 1993, for an alleged role in running the RaaS affiliate program.
- Four suspects allegedly linked to the **LockBit** gang's activity were arrested in France, Spain and the U.K. in August 2024. Additionally, the U.K. revealed sanctions against 16 individuals involved in the **Evil Corp** hacking group's criminal activities, while the U.S. sanctioned six individuals and Australia targeted two.[21]

Operation Cronos proved broader in scope than initially suggested and the highly public nature with which it was conducted further amplified the impact. The slow drip of information was further evidence of this method and likely cultivated additional anxiety to **LockBit** affiliates who possibly lost faith in the RaaS and sought to abandon the project. The episodic nature of Operation Cronos likely contributed to its success, as it prolonged the time the disruption was covered by the media. Given the massive reputational damage, additional arrests and further disruption to associated enablers, it is highly likely **LockBit** ceases activity altogether in the coming months. However, we cannot rule out the possibility of a rebrand in the future, of which the success would be uncertain.

Rise of RansomHub

The RansomHub RaaS affiliate program has been among the most active groups since its emergence in early February 2024 with 395 claimed breaches at the time of this report. The program's spike in activity in the first half of 2024 may be explained largely by its favorable cuts, advanced techniques and success in recruiting experienced affiliates, including those who migrated from other groups such as the actor **notchy**. Additionally, the group's victim count in July 2024 doubled compared to June 2024, suggesting **RansomHub** may have recruited new affiliates around that time, including possible former members of the **ALPHV** ransomware group. Moreover, the collective allegedly attracted members of the **Scattered Spider** intrusion cluster to its affiliate base in June 2024, which likely allowed **RansomHub** to use the group's experience and tool set to further enhance its capabilities and maintain a consistently high breach count throughout the year. New additions to the group and the increased law enforcement scrutiny surrounding the **ALPHV** and **LockBit** ransomware groups only bolstered the group's position as the leader of the ransomware market.[22]

> * *Ransomware groups do not typically broadcast ransomware breaches when the victim pays the desired ransom. Therefore, it is important to highlight that our analysis is based on events specifically observed and recorded by Intel 471. Ransomware strains are listed according to their most recent nomenclature at the time of this report. Additionally, we included raw observables as part of the analysis of emerging variants and common tactics, techniques and procedures (TTPs). Since Operation Cronos — the international law enforcement disruption operation against the LockBit RaaS — the LockBit group continued to add victims to its data leak blog. These claims were contested in subsequent Op Cronos statements, which claimed many of the victims were fabricated or falsified. It is not possible to discern which were accurate, therefore, we included all claims in our statistics.*

The collective claimed victims across a multitude of industries and demonstrated a clear preference for entities in Europe and the U.S. while also forbidding affiliates from targeting users in China, Cuba, North Korea, Romania and Commonwealth of Independent States (CIS) countries. Most of **RansomHub's** victims were low-profile entities with low or undisclosed revenues, which suggests the group prioritizes targets that may be easier to attack but likely will pay a minimal ransom. However, **RansomHub** also claimed to compromise at least 29 organizations with revenues of more than US $500 million in 2024, which suggests the group includes experienced ransomware operators capable of conducting attacks against high-profile targets who are likely more willing to pay higher ransoms to avoid operational disruptions and sensitive data leaks. Additionally, the group allegedly attacked at least 47 entities in the life sciences and health care sector, becoming the most impactful group targeting the sector in 2024.

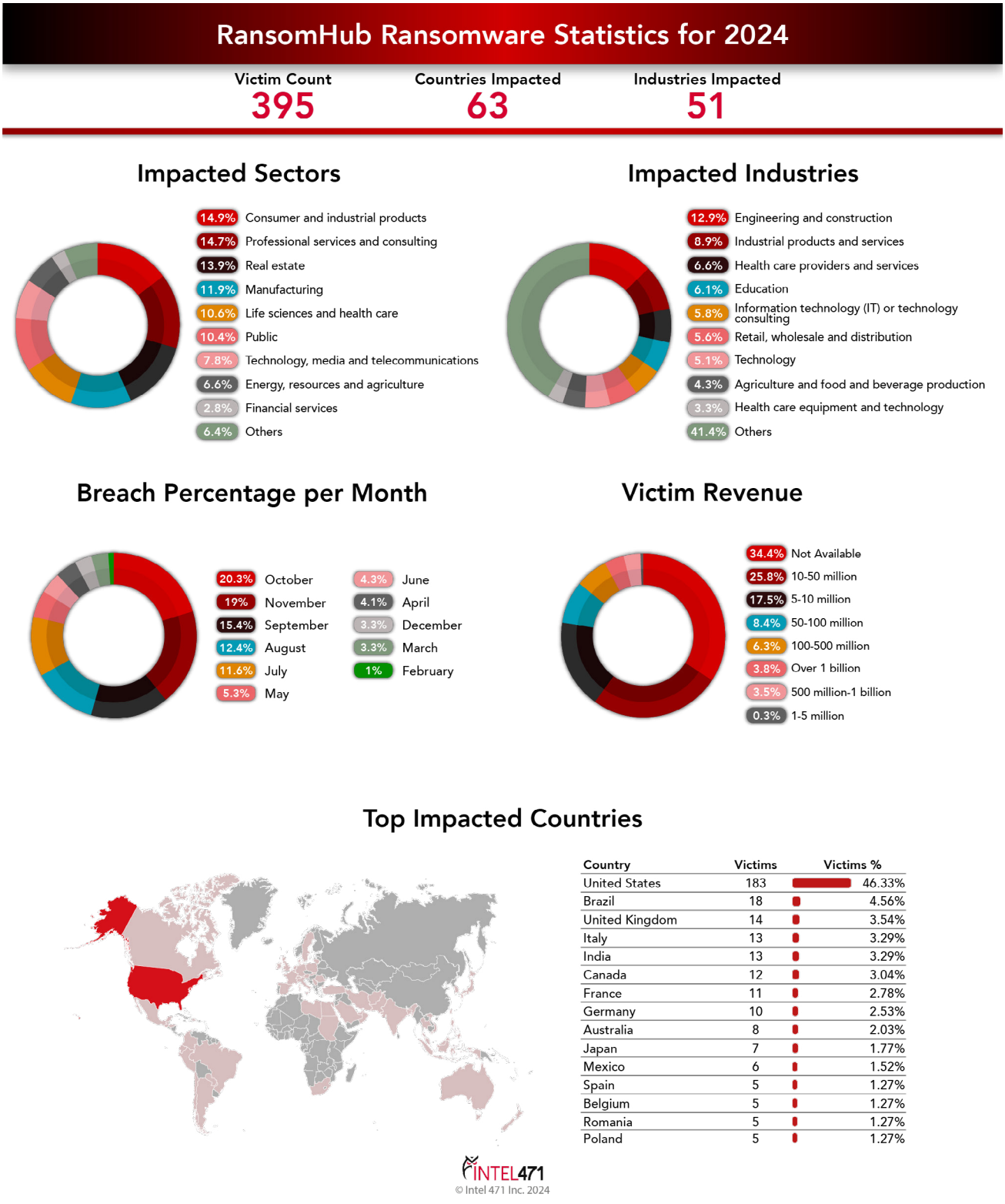


Figure 6: The image depicts a dashboard detailing statistics for the RansomHub RaaS in 2024.

Variants

In 2024, we identified 98 ransomware variants, an increase of 28 variants compared to 2023.

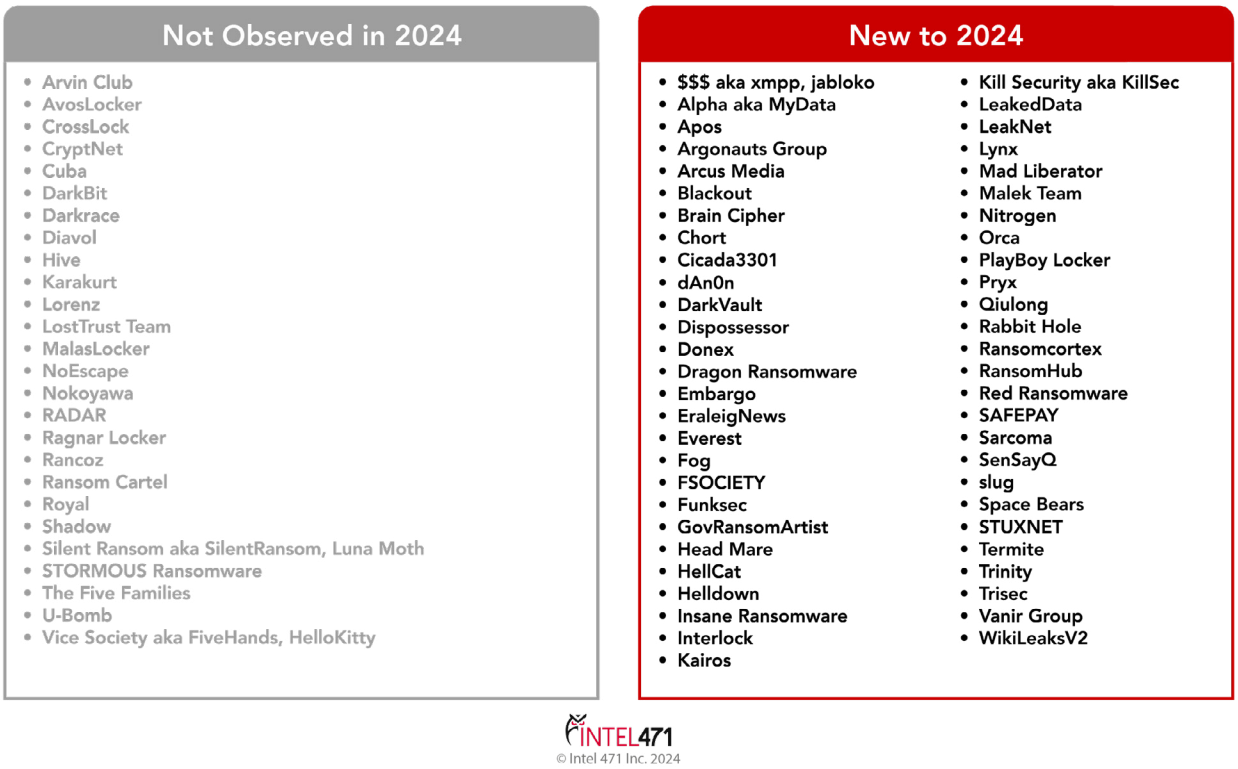


Figure 7: The image depicts new ransomware variants observed and variants not observed in 2024.

Kill Security

The **Kill Security** aka **KillSec** ransomware group was among the top five impactful groups in the second half of 2024 with 94 breaches. Although the group allegedly emerged in 2023, it launched its data leak blog in mid-March 2024 and claimed 101 victims at the time of this report, with about 50% of entities located in Asia. The group's ransom demands ranged from several thousand dollars to much larger amounts with clusters at 10,000 euros (about US $10,829) or from US $5,000 to US $25,000, and perpetrators primarily sought ransom in euros, which is not a common practice among ransomware operators. Group members are not allowed to attack entities from CIS countries and critical infrastructure including health care facilities and pipelines unless an administrator grants permission, however, affiliates could attack government entities.[23, 24]

Nitrogen

The **Nitrogen** ransomware and data extortion group emerged in late September 2024. The group likely is led by Russian-speaking threat actors with extensive backgrounds in ransomware operations and uses Nitrogen ransomware, which reportedly shares similarities with the LukaLocker ransomware previously attributed to members of the **Volcano Demon** ransomware group that has been active since at least mid-2024. Cybersecurity researchers also linked **Nitrogen** group members "to various ransomware attacks, including those involving the BlackCat/ALPHV ransomware" and they likely used malicious advertising (malvertising) or compromised software downloads to penetrate at least one network.[25, 26]

Sarcoma

In early October 2024, we discovered a new Tor-based victim shaming and data leak blog operated by the **Sarcoma** data extortion group. The blog listed more than 50 victim organizations from multiple industries at the time of this report. Group members described themselves as security experts, appeared to target companies opportunistically and welcomed initial access brokers (IABs) and "aggrieved employees" to join the collective.[27, 28]

HellCat

The **HellCat** extortion group emerged in the underground in early November 2024 when it claimed the compromise of the France-based multinational energy and digital automation solutions company Schneider Electric SE. Formerly known as **ICA Group**, **HellCat** operates under the data extortion model and includes a plethora of threat actors with significant underground presences who previously claimed responsibility for confirmed data breaches. The leader of the group is the actor **Brass***, an IAB and data vendor.[26, 29]

Summary

The popularity of ransomware and associated affiliate programs has allowed it to maintain its rank as one of the top threats throughout the year. However, we observed a downfall in ransomware attacks in 2024 compared to 2023, which likely was due to an uncertainty in the ransomware landscape left from law enforcement disruption against **LockBit**, the most impactful ransomware variant for the last two years. The vacant spot was quickly occupied by **RansomHub**, who consistently claimed victims throughout the year, successfully attracted high-profile threat actors and became the most active ransomware group by the end of 2024.

*** Threat actor persona handles have been changed.**

We observed a slight increase in ransomware variants in 2024 compared to the previous year. This may be an indication of a more threatening trend where new or rebranded ransomware strains consistently flood the underground, making the ransomware market more versatile and thus providing threat actors with more diversity to their malicious operations. Despite successful law enforcement operations conducted against high-profile ransomware programs in the past few years, the number of new ransomware groups continues to rise, and we likely will observe them employing robust operational security (OPSEC) measures to increase resilience as well as using more sophisticated TTPs in an attempt to keep up with the sustained success of well-established RaaS programs.

For Sale: Access to Enterprise Networks

*The reporting metrics for this section were sourced from Intel 471 Breach Alerts, Information Reports and auction offers made on the Exploit forum.***

Access at a glance

Figure 8: The image depicts an infographic detailing access offer statistics for 2024.

In 2024, we observed and reported just shy of 4,000 claims from IABs offering to sell compromised credentials and/or alleged unauthorized access to networks or systems. Offers of access continue to enable threat actors with the potential to further compromise systems, steal sensitive information, install malware and/or launch additional cyberattacks.

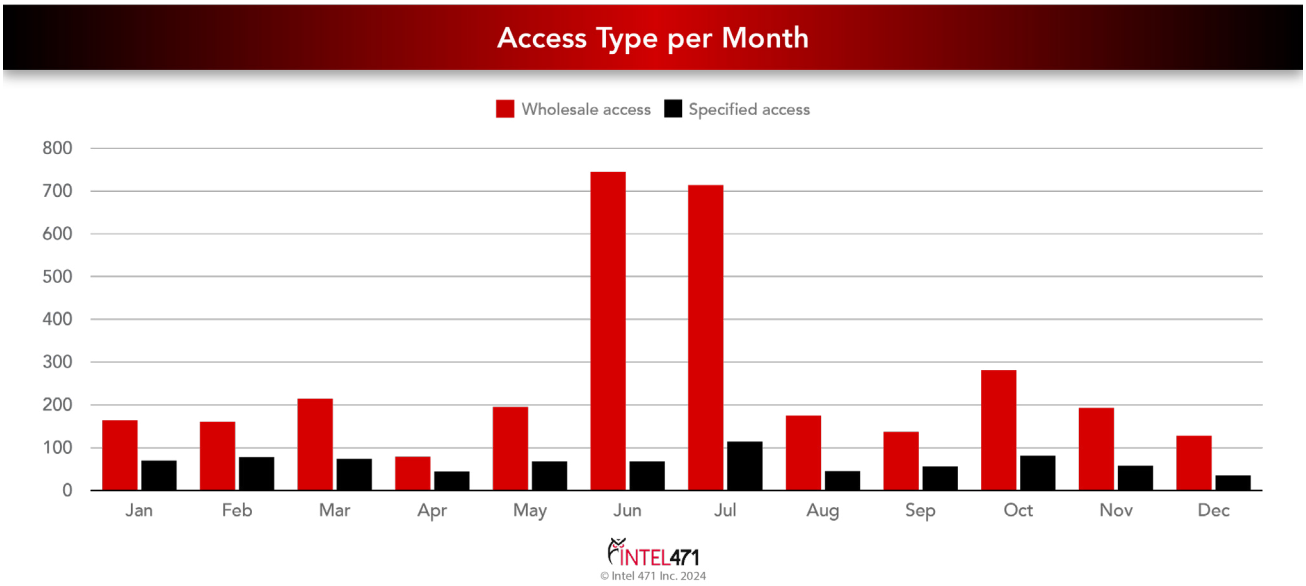


Figure 9: The graphic depicts the number and type of access offers per month.

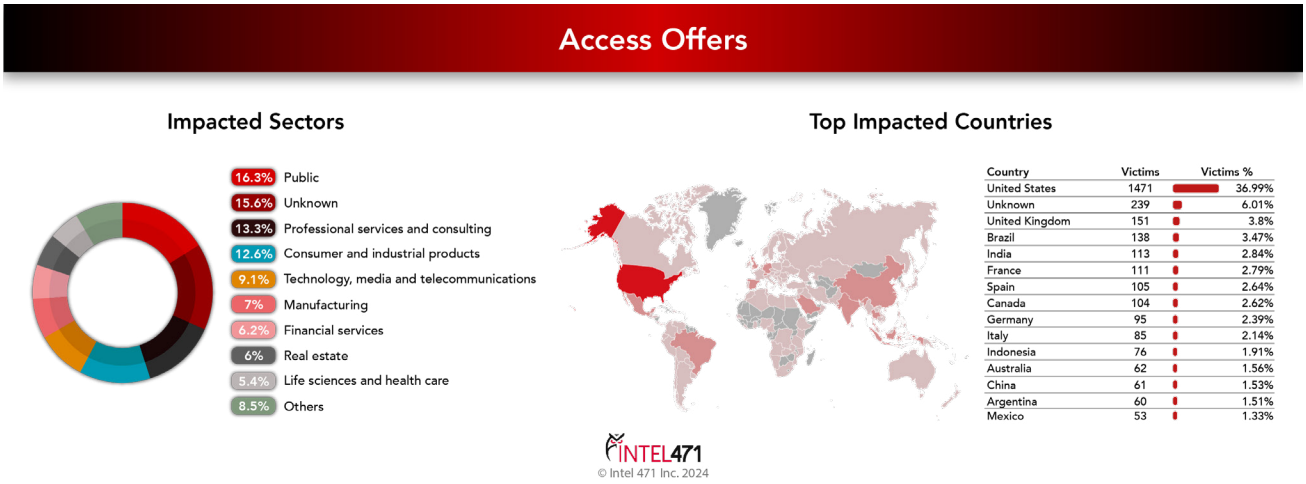


Figure 10: The image depicts the sectors and countries most impacted by all access offers in 2024.

In 2024, we observed and reported just under 800 claims of specified access listed for sale in the underground. The top three sectors most impacted by these offers in descending order were consumer and industrial products, professional services and consulting, and public. The top three regions most impacted by these offers in descending order were the U.S., India and the U.K.

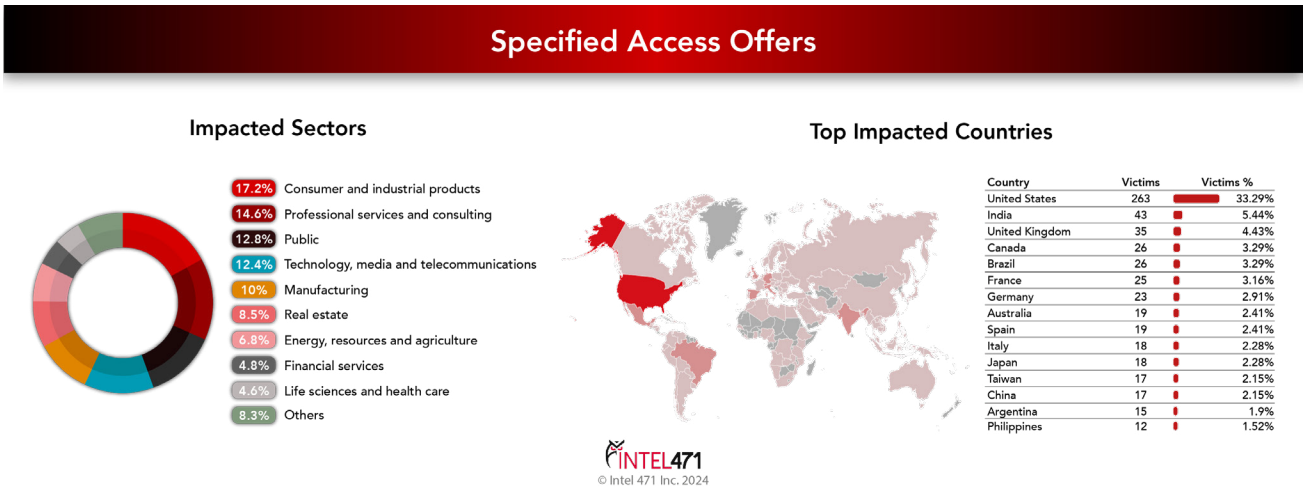


Figure 11: The image depicts the sectors and countries most impacted by claims of specified access in 2024.

Wholesale Access Offers

In 2024, we observed almost 3,200 wholesale access offers from vendors in the underground marketplace. The top three sectors most impacted by these offers in descending order were public, professional services and consulting, and consumer and industrial products.

The top three regions most impacted by these offers in descending order were the U.S., the U.K. and Brazil.

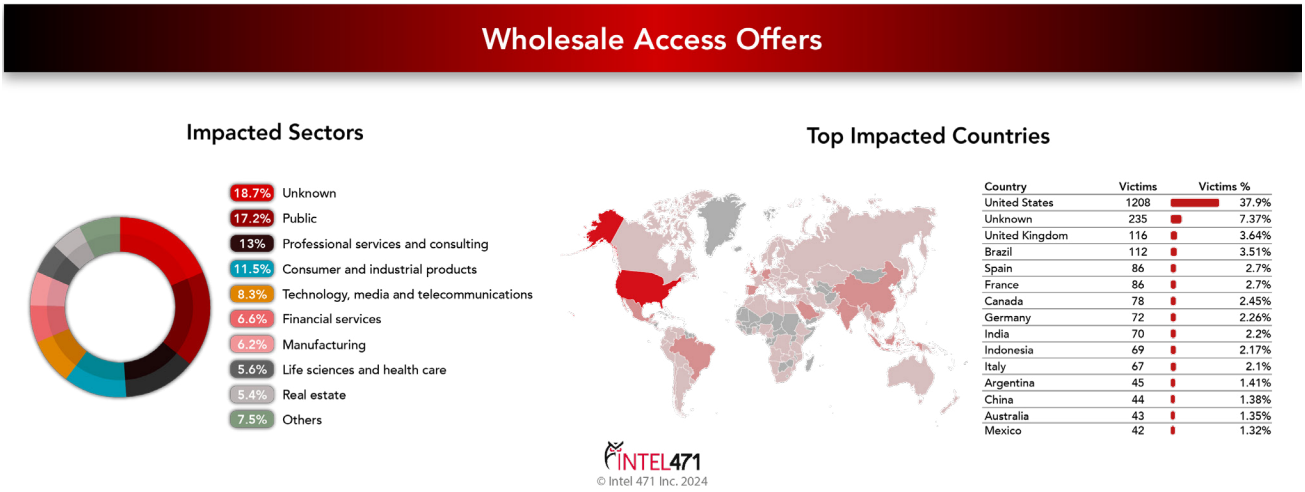


Figure 12: The image depicts the sectors and countries most impacted by wholesale access offers in 2024.

Notable Access Brokers

Actor IntelBroker

The actor **IntelBroker** achieved the status of one of the most impactful threat actors in 2024 and was responsible for the most wholesale access offers with just over 500. The actor assumed the administration of the BreachForums underground forum and moved across different underground groups. The actor was directly or indirectly involved in dozens of breaches including supply chain attacks impacting the cloud services provider Cprime Inc. and the digital agency Born Group Inc. The actor demonstrated a variety of methods to achieve initial access to organizations and commonly targeted cloud-based services, leveraged social-engineering techniques to compromise employees, used compromised login credentials and conducted brute-force attacks to obtain valid credentials. [30]

Actor sandocan

In 2024, the actor **sandocan** had the second most wholesale access offers with 322. The actor first appeared in January 2020 on the Exploit cybercrime forum and was observed constantly shifting TTPs to either conduct brute-force attacks or harvest compromised login credentials from public and private collections of malware logs. The actor primarily targeted RDWeb technologies and claimed to have more than 10 years of experience in

spamming and phishing operations. The actor primarily targeted the U.S. with 80 alleged victims and the public and professional services and consulting sectors.[31]

Actor mont4na

The actor **mont4na** led the year for specified access with 199 offers, even after the actor's sudden disappearance in August 2024. While the sudden cease in activity is peculiar, this is not the first time **mont4na** has gone missing. The reasons for the actor's absence remains unclear, however explanations such as law enforcement intervention or underground persona changes cannot be ruled out at this time since the actor has been known to frequently change aliases and contact information.[32]

Tactics, techniques, procedures observed

In 2024, we observed actors leveraging multiple techniques to achieve initial access to victim networks or systems. The top three most used techniques were brute-forcing corporate resources, use of malware logs and conducting structured query language-injection (SQLi) attacks. Adversaries offered access to several corporate resources throughout the year. The top five most observed targeted resources were RDWeb, Windows RDP, the Outlook Web App email platform, Fortinet VPN and secure shell (SSH) remote access protocol.

One notable technique that proved particularly effective in 2024 was the compromise of cloud-based service providers and, consequently, unauthorized access to datasets operated by their customers, essentially configuring a supply chain attack. Examples of companies breached throughout the year included Cprime, Snowflake and Born Group.

Another trend observed in 2024 was adversaries conducting credential-stuffing and social-engineering attacks to gain access to cyber threat intelligence (CTI) and law enforcement platforms and leveraging their access to submit emergency data requests (EDRs) in social media platforms.

Summary

We observed a decrease of 26% in overall access offers in 2024 compared to 2023, with about 36% of total offers attributable to three threat actors — **IntelBroker**, **mont4na**, and **sandocan**. Wholesale and specified offers decreased about 26% and 27%, respectively. The drop in numbers likely can be attributed to the dynamic changes in the underground this year, with major breaches influencing the number of offers and actors moving between threat groups, impacting their focus of underground activity.

Despite the downturn, the provision of unauthorized access to corporate networks and resources remained an effective cybercriminal activity in 2024 and likely will continue to

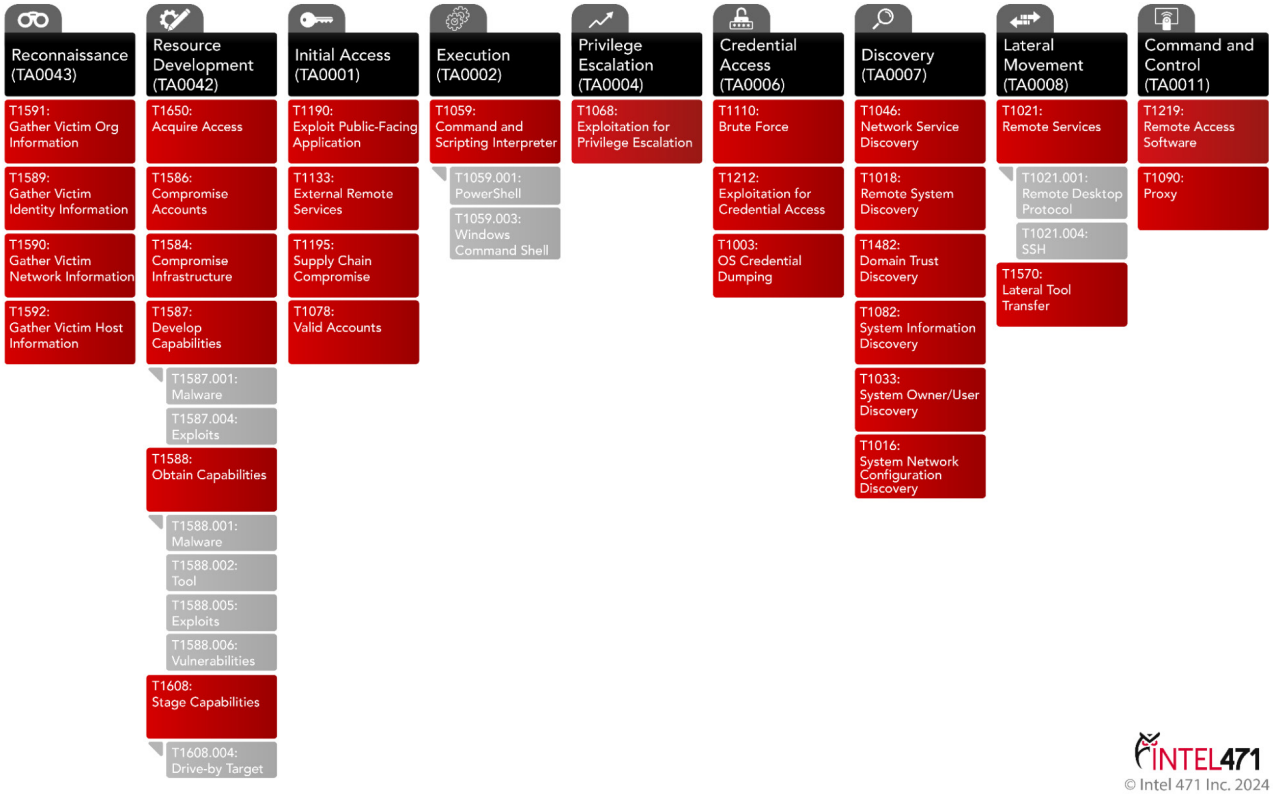


Figure 13: The image depicts the observed TTPs from threat actors offering compromised access in 2024.

be relevant in 2025 as it allows adversaries to profit while maintaining a certain level of anonymity since attributions made for cyberattacks are more commonly associated with those who conducted the final stages.

> *** The reporting metrics for this section were sourced from Intel 471 Breach Alerts, Information Reports and auction offers made on the Exploit forum and are not representative of all access possibly offered across the underground. It is important to highlight that our analysis is based on events specifically observed and recorded by Intel 471. Some access offers captured in our data points remain unverified at the time of this report. Additionally, we included raw observables as part of the analysis of emerging threats and common TTPs.*

Malware: Infostealer Logs Feed Demand for Access Credentials

*The malware landscape is an ever-changing environment where metrics vary greatly based on several factors.****

Malware at Glance

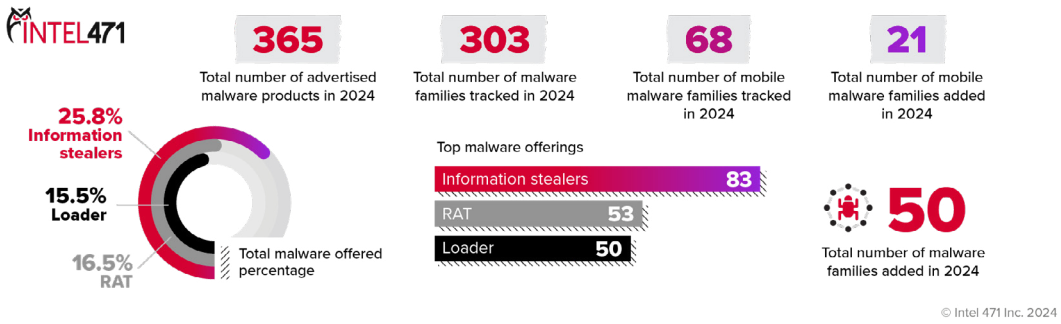


Figure 14: The image depicts an infographic detailing malware statistics for 2024.

In 2024, we documented 365 advertisements promoting malware products. Over the course of the year, there was a notable presence of stealers, remote access trojans (RATs) and loaders on the market. Stealers represented 25.8% of all malware-related offerings, followed by RATs at 16.5% and loaders at 15.5%. Additionally, we expanded our monitoring capabilities by adding support for 50 new malware families and 21 mobile malware families, increasing the total number of tracked malware families to 371 in 2024.

Technical malware overview

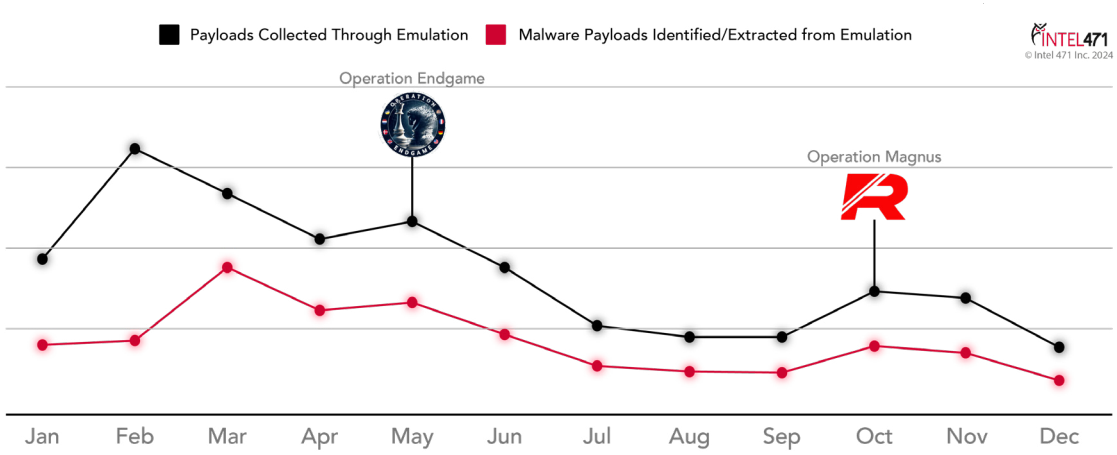


Figure 15: The impact of both Operations Endgame and Magnus contributed to a decline in both observable metrics.

Downloader Malware Metrics

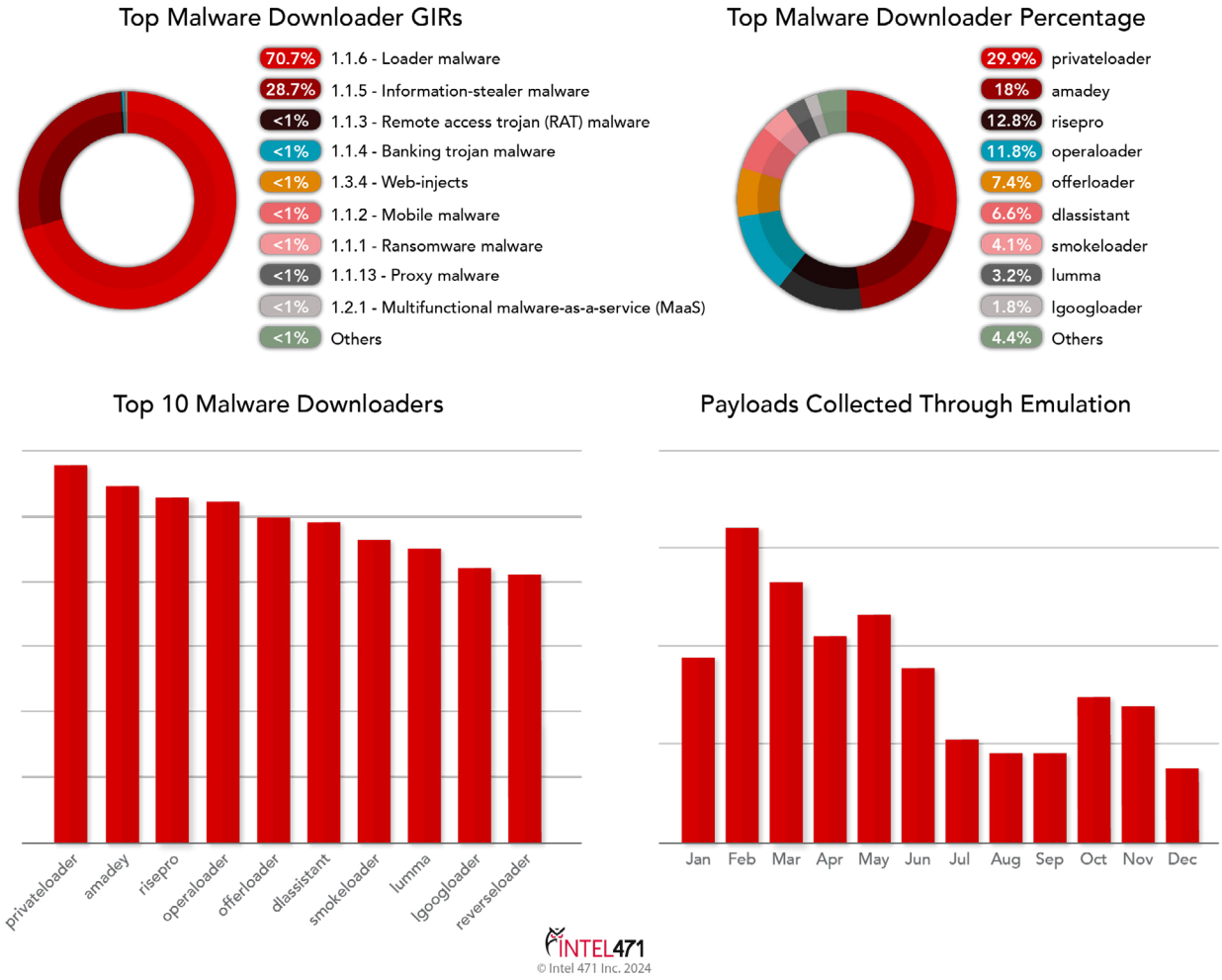


Figure 16: The image depicts the most active downloader malware variants and their percentage of the total monitored.

Of the malware observed downloading further malware from January 2024 to Dec. 15, 2024, 70.7% was loader malware, 28.7% was information stealers and the remaining 0.6% was a broad mix. The most popular malware families used as first-stage loaders this year can be seen in the graphic above, many of which are dispersed by install services. Tracking these malware families allows us to quickly collect and identify new or updated malware builds that malware operators pay these install services to disseminate. The most popular tools this quarter supporting the aforementioned install services in descending order were Privateloader, Amadey, RisePro and Operaloader.

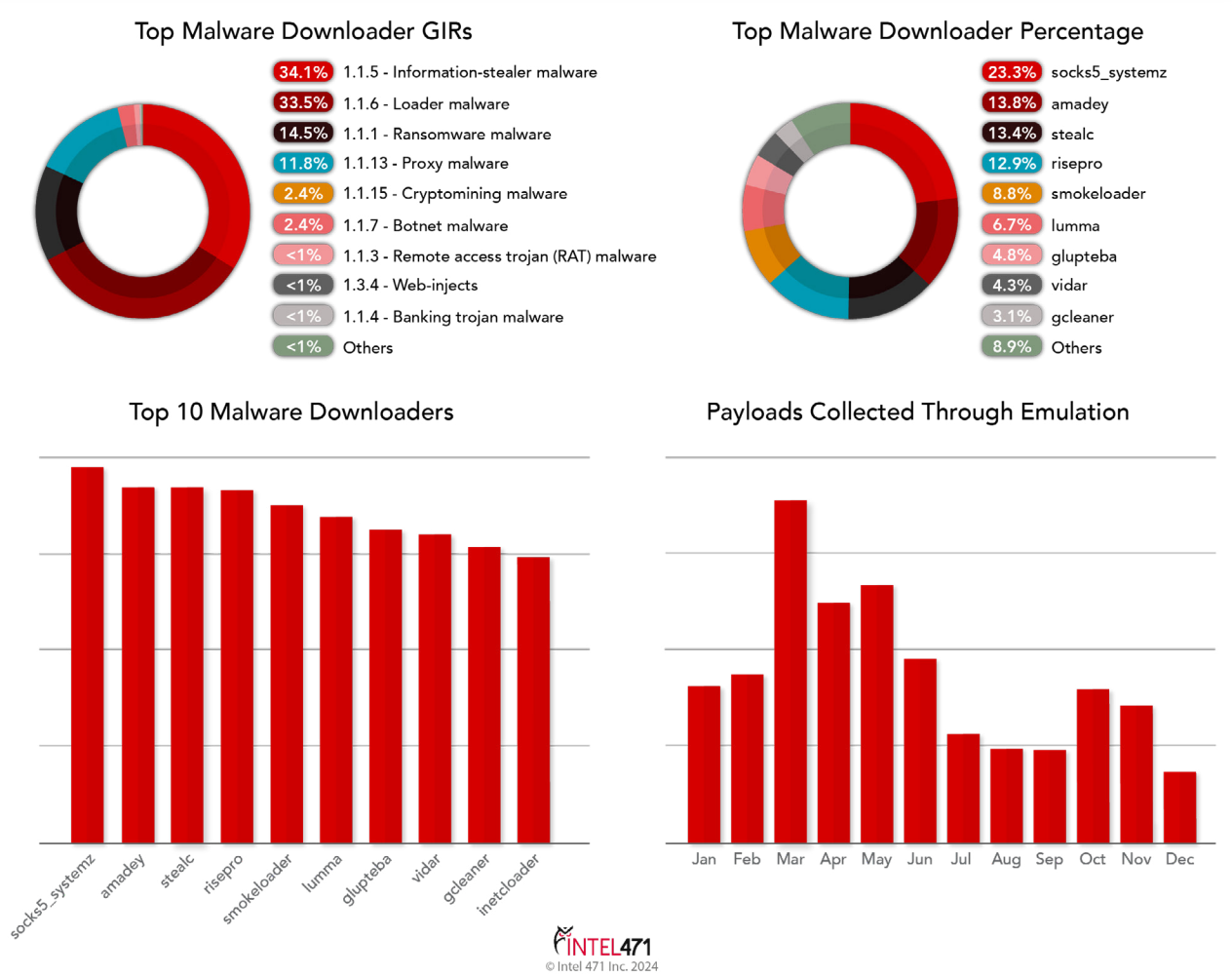


Figure 17: The image depicts the most frequently downloaded malware variants and their percentage of the total monitored.

Threat actors also continue to leverage loading malware to deliver additional malware payloads, which typically are designed to have an impact on the victim. From January 2024 to Dec. 15, 2024, 34.1% of the malware downloaded was information-stealing malware, 33.5% were loaders, 14.5% was ransomware malware, 11.8% was proxy malware and the remaining 6.1% consisted of a variety of other malware types. Information stealers likely feature prominently due to an increasing demand for malware logs and the access credentials derived from them. The most downloaded information-stealer malware in descending order was Stealc, RisePro and Lumma.

Major Events: Campaigns, Updates, Takedown Announcements

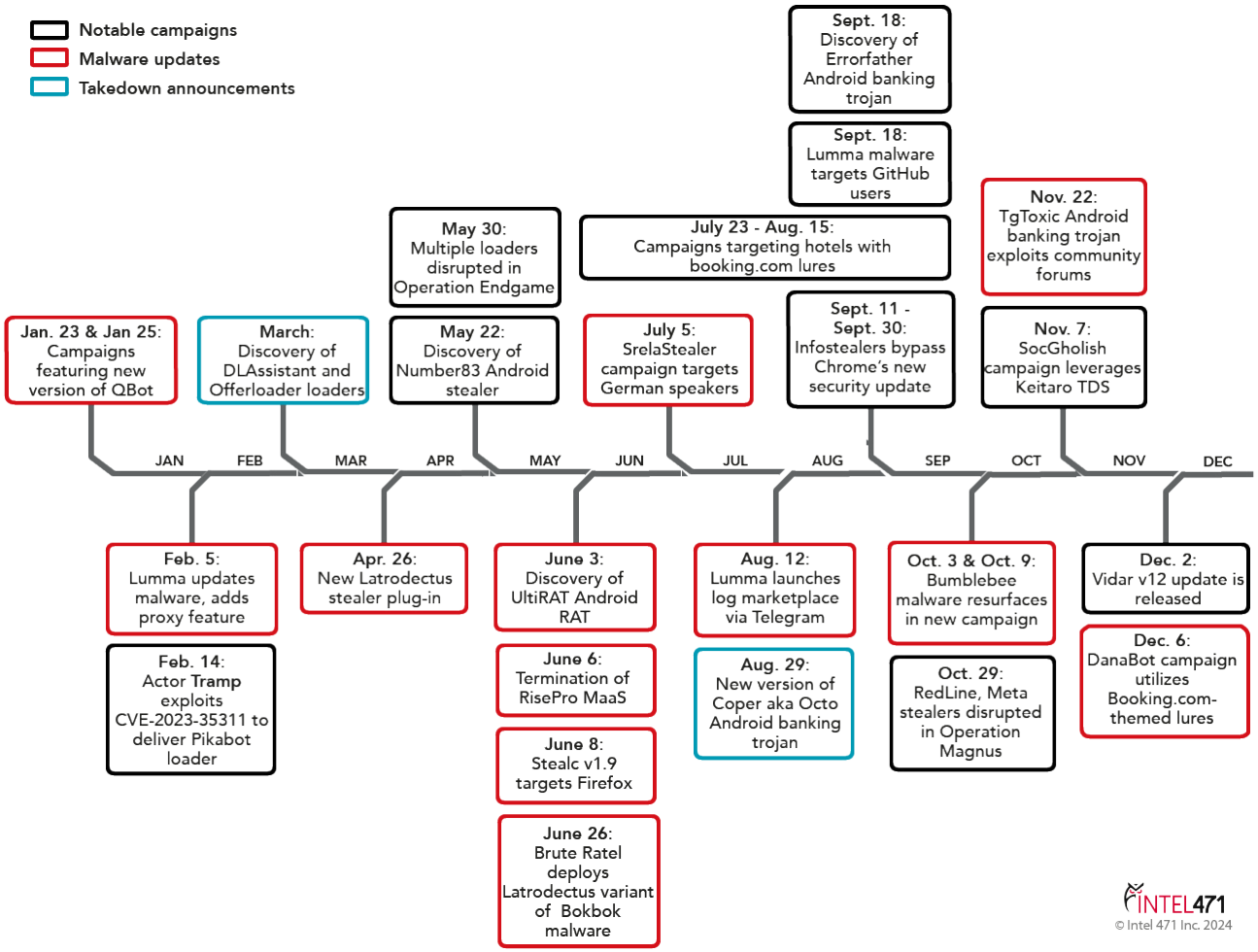


Figure 18: The image depicts a timeline of major malware-related events in 2024.

Notable campaigns

- Between July 23, 2024, and Aug. 15, 2024, we observed nine spam waves targeting hotels with Booking.com lures.[33] Threat actors employed sophisticated phishing schemes to bypass detection mechanisms and deceive hotel managers into providing their Booking.com partner account credentials.
- On Sept. 18, 2024, we observed a campaign targeting GitHub contributors and subscribers to public repositories designed to distribute the Lumma information stealer.[34] Threat actors used fake GitHub user accounts (bots) to open new "issues" in open source repositories. These issues claimed the project contained a security

vulnerability and directed users to contact websites at github-scanner.com or github-scanner.shop for further instructions.

- On Oct. 3, 2024, and Oct. 9, 2024, we observed the resurgence of campaigns deploying new samples of the Bumblebee malware after a period of dormancy.[35] Threat actors distributed malicious spam (malspam) emails posing as messages from accounting departments. These emails enticed recipients to download compressed (ZIP) attachments, which contained harmful Windows shortcut (LNK) files. When executed, these LNK files initiated the deployment of the Bumblebee payloads.
- On Nov. 7, 2024, we published a report on SocGholish, highlighting its continued significance as a cybersecurity threat.[36, 37] The report detailed a campaign active since at least Oct. 22, 2024. The campaign used the Keitaro Traffic Distribution System (TDS) version 10.3.7 to reroute user traffic from compromised websites to domains containing malicious JavaScript code. According to our observations, the campaign generated about 1.58 million interactions by Nov. 1, 2024.
- On Dec. 6, 2024, we observed a new wave of malspam campaigns targeting hotels with Booking.com-themed phishing lures. This time, the attackers pivoted from relying solely on the phishing sites for credential collection to actively deploying malware as part of their credential harvesting process. The phishing method was substituted with a fake completely automated public Turing test to tell computers and humans apart (CAPTCHA) puzzle and a social-engineering technique called ClickFix, which ultimately facilitated the deployment of the DanaBot banking trojan.[38]

Notable malware additions, updates

Date	Update
Feb. 5, 2024	The actor **Iron*** announced an update to the LummaC2 information-stealing malware.[39] This update introduced a new feature enabling the use of infected hosts as socket secure internet protocol (SOCKS5) proxies.
March 2024	Intel 471 Malware Intelligence analysts identified two previously undocumented loader malware families — DLAssistant and Offerloader.[40]
April 26, 2024	Intel 471 Malware Intelligence systems detected a new stealer plug-in associated with the Latrodectus variant of the Bokbot aka IcedID malware.[41]
May 22, 2024	Intel 471 Mobile Malware Intelligence researchers discovered a new Android stealer subsequently dubbed Number83.[42]

June 3, 2024	Intel 471 Mobile Malware Intelligence researchers discovered a new Android RAT subsequently dubbed UltiRAT.[43]
June 6, 2024	The actor behind the RisePro information-stealer malware-as-a-service (MaaS) operation announced its termination.[44]
June 8, 2024	The actor **Silver*** announced an update to the Stealc malware to version 1.9. This update introduced the capability to collect data from Firefox-based browser plug-ins, aligning Stealc with features already present in other information stealers such as Lumma and Vidar.[43]
Aug. 12, 2024	The actor **Iron*** launched a new marketplace for selling logs from the LummaC2 information-stealing malware.[45]
Aug. 29, 2024	Intel 471 Malware Intelligence analysts identified new samples of an updated version of the Coper aka Octo Android banking trojan.[46]
Sept. 11, 2024-Sept. 30, 2024	Operators of several information-stealing malware variants, including Meduza, Lumma, Vidar, Luman, Stealc and Metastealer, released updates specifically designed to circumvent a security enhancement introduced in Chrome version 127 and subsequent releases.[47]
Sept. 18, 2024	Intel 471 Mobile Malware Intelligence researchers discovered a new banking trojan subsequently dubbed Errorfather.[47]
Dec. 2, 2024	The actor **Copper*** at a popular cybercrime forum announced the release of version 12 of the actor's Vidar information-stealing malware.[48]

***Threat actor handle names have been changed**

Summary

The cybercriminal ecosystem demonstrated remarkable resilience and adaptability in 2024. The disruption of major botnets temporarily reduced malicious activities, however, a noticeable increase in new campaigns — driven predominantly by the spread of information-stealer malware — highlighted the market's rapid recovery capabilities by the latter part of the year. The pressure applied by law enforcement forced innovation among malware operators, as observed in the use of public forums, code repositories and legitimate cloud services to blend malware into well-trafficked digital environments. Finally, the rise and growing popularity of tactics such as the ClickFix method underscores an interminable reality — human operators frequently represent the weakest link in the security chain.

**** The malware landscape is an ever-changing environment where metrics vary greatly based on several factors including the frequency of execution of our emulation tools and*

the malware family coverage for the detection of those payloads collected through emulation. We believe our monitoring tools offer a more accurate depiction of the real underground use of malware, instead of having data polluted from submissions from malware sharing platforms.

Vulnerabilities

Vulnerabilities at a glance

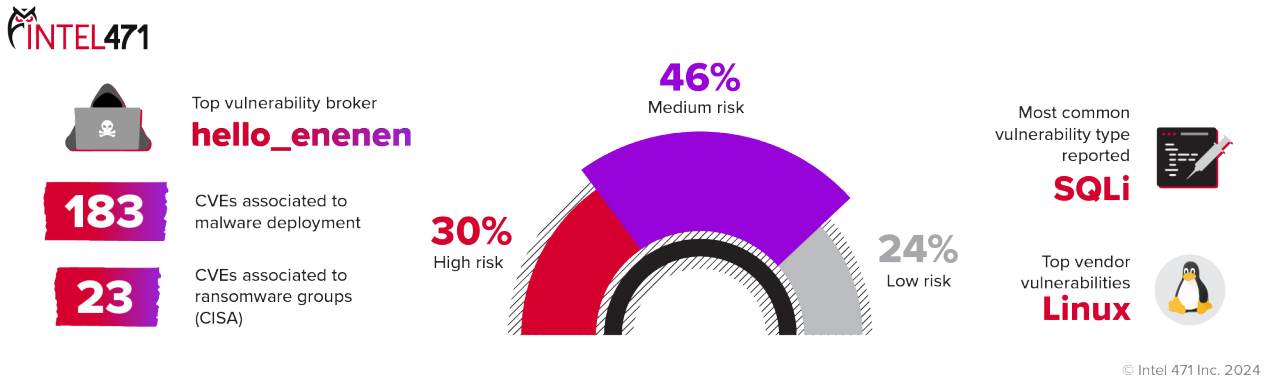


Figure 19: The image depicts an infographic detailing vulnerability statistics for 2024.

In 2024, threat actors exploited a wide range of vulnerabilities — both newly discovered flaws and unresolved issues — to launch sophisticated attacks on global organizations. Leveraging intelligence gathered from open sources, underground forums and in-depth analysis, we observed notable trends when comparing 2024 to 2023 that included:

- Initial access vulnerabilities frequently exploited in malware attacks.
- Newly discovered flaws actively exploited as zero-days.
- An overall increase in observed vulnerabilities.

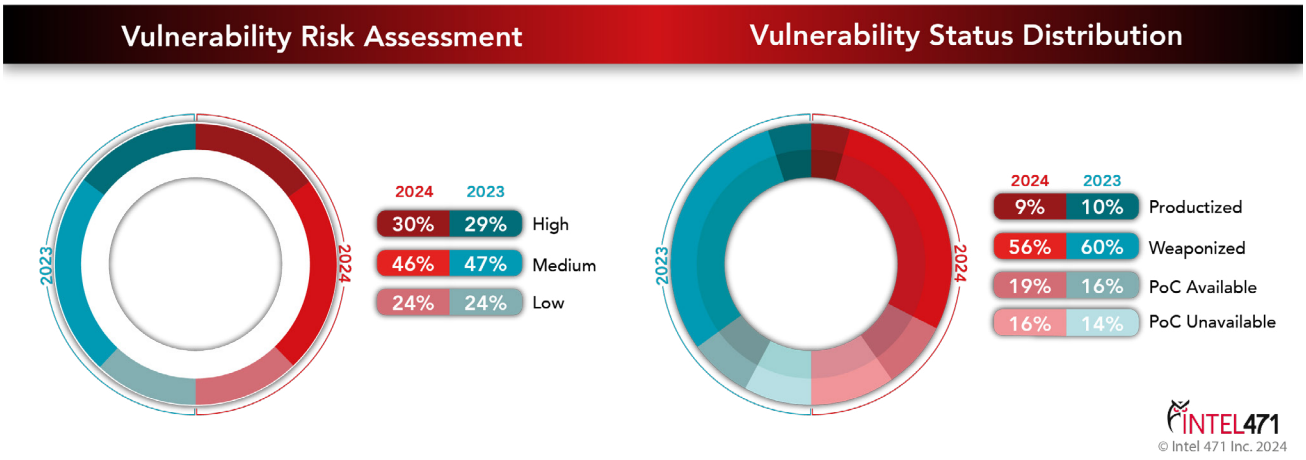


Figure 20: The image depicts the percentage of vulnerabilities we assigned a high, medium or low risk in 2023 and 2024 and the percentage of vulnerabilities we assigned a productized, weaponized, code available or PoC unavailable status in 2023 and 2024.

Prioritized Vulnerability Patching Mattered More Than Ever in 2024

In 2024, we reported 516 vulnerabilities, marking a slight increase from 511 the previous year. In 2024, 30% of vulnerabilities were classified as high risk — up 1% from 2023, 46% as medium risk — down 1% and 24% as low risk, the same as the previous year. Additionally, of the 516 vulnerabilities from 2024, 9% were productized, 56% were weaponized and 19% had proof-of-concept (PoC) code available, whereas the statistics from 2023 consisted of 10% productized, 60% weaponized and 16% had PoC code available.

CVEs Surge by a Third to Almost 40,000

The National Vulnerability Database (NVD) noted a significant rise in the total number of documented vulnerabilities from 2023 to 2024 — an increase from 28,818 to 38,606. However, there was a sharp decrease in critical and high-severity vulnerabilities, which dropped from 15,591 in 2023 to 8,645 in 2024. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) observed a slight decline in the total number of vulnerabilities added to the Known Exploited Vulnerabilities (KEV) catalog from 2023 to 2024, with the count dropping to 176. Similarly, the number of vulnerabilities assigned the CVE-2024 identifier decreased to 111.

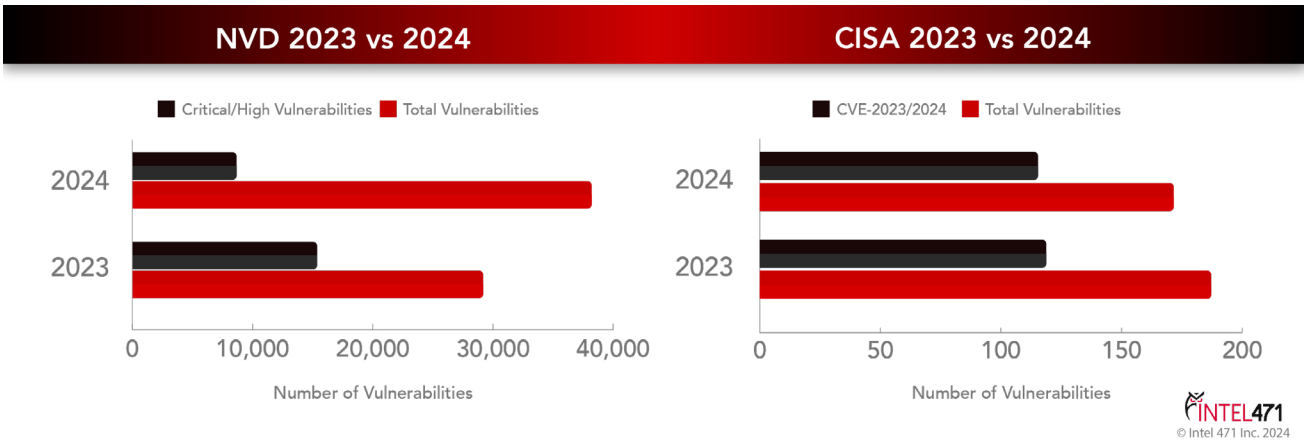


Figure 21: The image depicts the total number of vulnerabilities NVD reported as critical or high in 2023 and 2024, and the number of vulnerabilities with a designator of CVE-2023/2024 vs. all vulnerabilities CISA reported in 2023 and 2024.

Linux Vulnerabilities Dominated in 2024

Data regarding the top five vendors impacted by security vulnerabilities in 2024 compared to 2023 provides valuable insight into the shifting dynamics of threat landscapes. Linux emerged as the most impacted vendor in 2024 with 2,027 reported vulnerabilities. This underscores both its widespread adoption and the inherent challenges of managing security in open source systems. Google, which topped the list in 2023 with 1,677 vulnerabilities, experienced a significant reduction in reported vulnerabilities, dropping to just 350 in 2024. This marked Google as the least affected vendor among the top five in 2024. Microsoft, Adobe and Apple filled in the two through four spots, with the number of vulnerabilities impacting them remaining relatively consistent with the previous year.

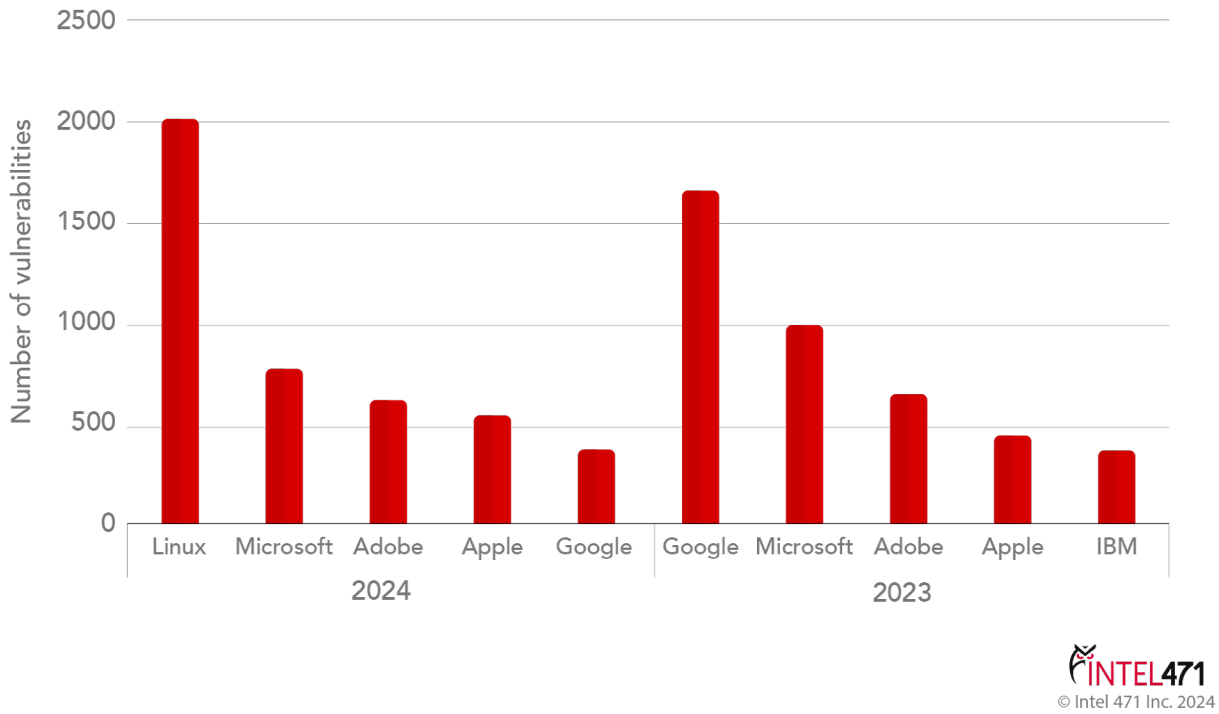


Figure 22: The image depicts the top five vendors impacted by vulnerabilities in 2023 and 2024.

Analysis of vulnerabilities reported in 2024 also revealed several trends regarding vulnerability types. The top five vulnerability types identified were cross-site scripting (XSS) at 6,843 occurrences, followed by SQLi at 2,844, missing authorization at 1,623, out-of-bounds write at 1,543 and cross-site request forgery (CSRF) at 1,270. The data shows a shift in vulnerability trends compared to the previous year, with missing authorization emerging as a significant issue in 2024, while improper out-of-bounds read vulnerabilities decreased. XSS and SQLi continue to dominate, indicating persistent risks in web application security.

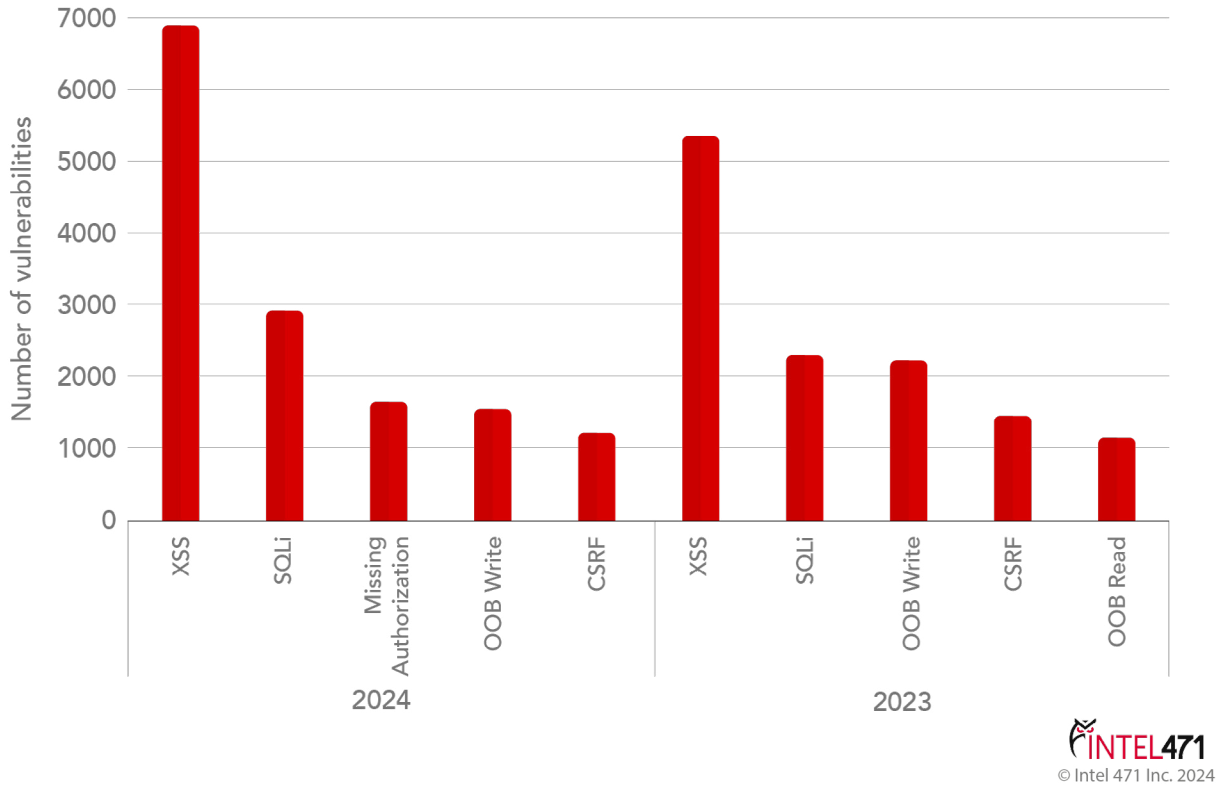


Figure 23: The image depicts the top five vulnerability types in 2023 and 2024.

Underground Vulnerability Offers Focus on Enterprise IT

In comparison to open source findings, our underground vulnerability data analysis shows Microsoft remained the most targeted vendor in 2024 with mentions rising to 75, up from 62 in 2023. Google moved up to the second position with 23 mentions, reflecting a significant year-over-year increase. Ivanti made its first appearance in the top five, taking the third spot with 19 mentions, indicating growing focus from threat actors. Apple, which held second place last year, slipped to fourth with 12 mentions, while Apache secured the fifth spot at 11. Notably, VMware and Cisco — both key players in 2023 — fell out of the top five this year. This data, drawn from threat actor discussions and vulnerability sharing on underground forums, highlights shifting priorities and emerging risks, offering organizations critical insights to enhance their security posture for the year ahead.

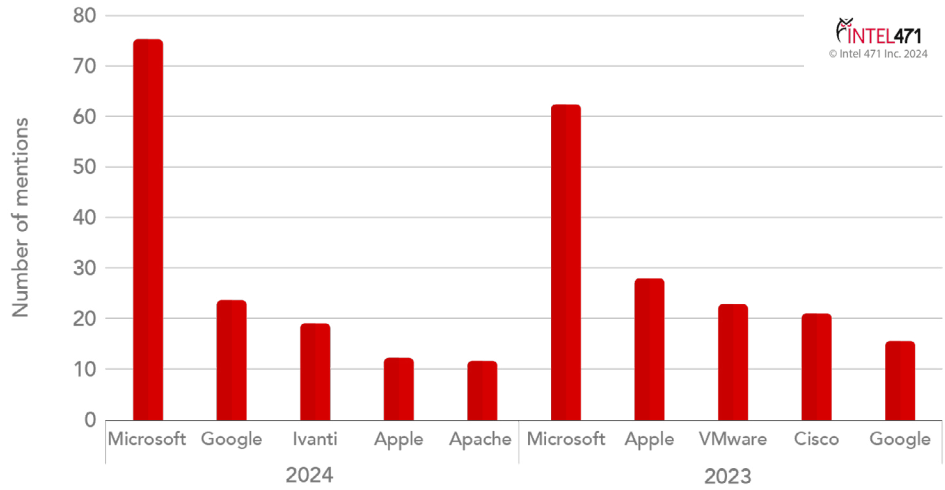


Figure 24: The image depicts the top five vendors impacted by vulnerabilities observed in the underground in 2023 and 2024.

Analysis of vulnerabilities discussed and shared on underground forums revealed a strong focus on vulnerability types that enable full system access or database breaches. SQLi led the way with 45 mentions, followed closely by shell injection at 38. This was a shift from 2023, where shell injection topped the list with 53 occurrences, followed by privilege escalation (PE) and XSS. The change highlights how threat actors are prioritizing vulnerabilities that offer greater rewards, such as full control over systems or access to sensitive data. These vulnerabilities often pave the way for ransomware attacks, data theft or long-term persistent access to networks.

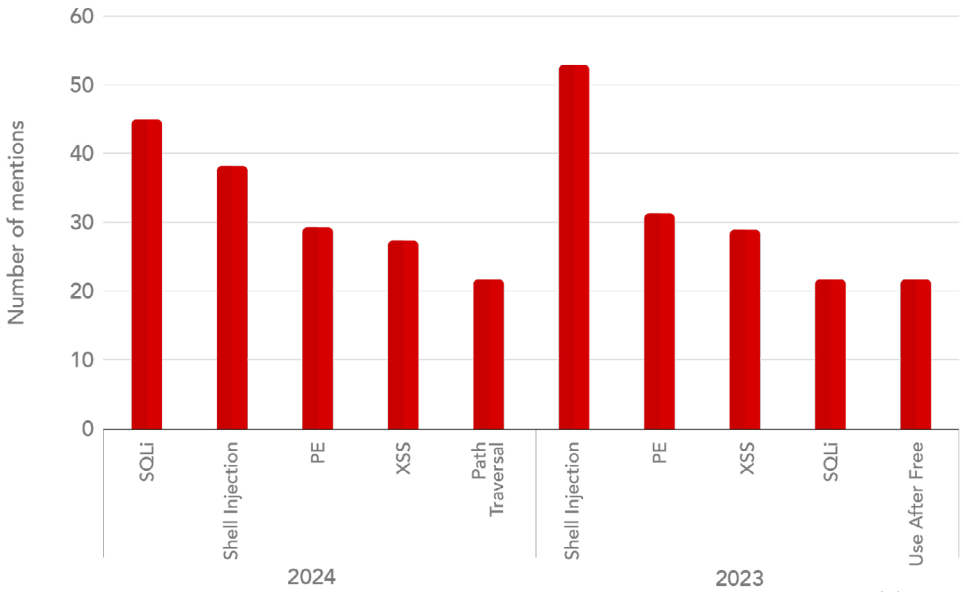


Figure 25: The image depicts the top five vulnerability types observed in the underground in 2023 and 2024.

Vulnerabilities Exploited in Malware, Ransomware Campaigns

Malware campaigns

Over the past 12 months, we observed vulnerabilities that allowed malicious actors to execute remote commands and deploy malware within internal networks. Our analysis identified 23 key vulnerabilities actively exploited by adversaries to gain initial access. Although it can be challenging to attribute these attacks to specific threat actors based solely on the malware used, these findings highlight the common malware leveraged to compromise corporate networks via certain vulnerabilities. The five most notable vulnerabilities based on adversary interest were CVE-2024-1708 and CVE-2024-1709, CVE-2024-21887, CVE-2024-3400, CVE-2024-37085 and CVE-2024-34102. Specific details regarding the top five vulnerabilities are provided in the table below:

CVE ID	Weakness	Threat observed	Vendor	Products Impacted	Observed date
CVE-2024-21887	Command injection	- **UTA0178** Chinese-nexus group - GIFTEDVISITOR web shell - XMRig cryptocurrency miner - **Magnet Goblin** group - Raptor Train botnet - Nosedive malware - **Flax Typhoon** Chinese-nexus group	Ivanti	Connect Secure and Policy Secure gateways	Jan. 10, 2024
CVE-2024-1708 CVE-2024-1709	Path traversal, Authentication bypass	- LockBit ransomware - Black Basta ransomware - BI00dy ransomware - **Kimsuky** North Korean-nexus group - XWORM malware - ToddlerShark malware	ConnectWise	ScreenConnect	Feb. 27, 2024
CVE-2024-3400	Operating system (OS) command injection	- **UTA0218** - **Pioneer Kitten** Iran-nexus group - NoEscape ransomware - RansomHouse ransomware - ALPHV ransomware - UPSTYLE Python backdoor	Palo Alto Networks	PAN-OS	April 12, 2024

CVE-2024-37085	Authentication bypass	- Black Basta ransomware - Akira ransomware - **Storm-0506** - **Storm-1175** - **Octo Tempest** - **Manatee Tempest**	VMware	ESXi	July 30, 2024
CVE-2024-34102	Improper restriction of XML external entity reference	- **Bobry** group - **Polyovki** group - **Surki** group - **Burunduki** group - **Ondatry** group - **Khomyaki** group - **Belki** group	Adobe	Multiple products	Oct. 1, 2024

The use of vulnerabilities and malware incidents fluctuated throughout the year, with a noticeable increase toward the end of the first quarter of 2024 and the beginning of the second quarter. Activity slowed during the third quarter but gained momentum in the fourth quarter, with November recording the highest number of malware incidents and vulnerabilities exploited. The most active groups throughout the year included **APT28**, **Black Basta**, **BlackCat** and **Akira**.

Ransomware campaigns

Vulnerabilities played a crucial role in ransomware campaigns in 2024, as highlighted by CISA data. Of the 23 vulnerabilities exploited in ransomware attacks, 13 were associated with a CVE-2024 identifier. This accounted for 56% of the total, while the remaining 44% were tied to CVE identifiers from previous years. This suggests threat actors primarily are targeting newly identified vulnerabilities, although the data also demonstrates well-researched, older vulnerabilities can pose problems if left unpatched.

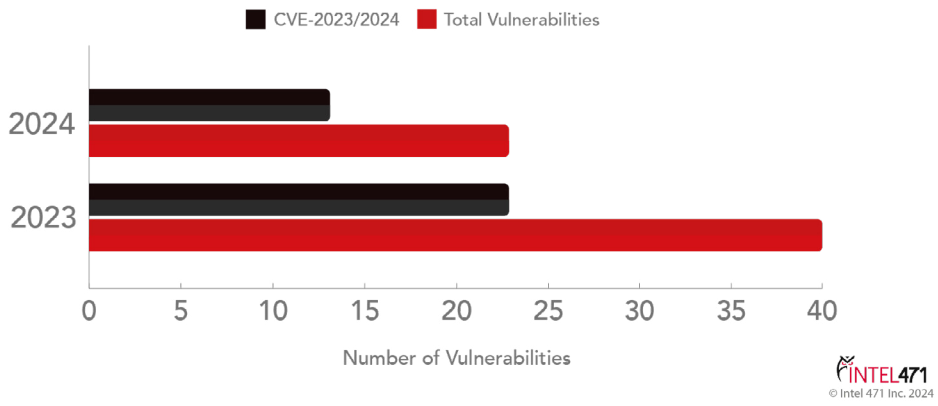


Figure 26: The image depicts the total vulnerabilities vs. CVEs with a designator of CVE-2023/2024 used in ransomware in 2023 and 2024.

Exploited Vulnerabilities That Had the Highest Impact

We analyzed the National Institute of Standards and Technology (NIST) NVD and our underground intelligence collection on adversary operations over the past 12 months to identify the most impactful vulnerabilities abused to achieve initial access to organizations. From an initial list of 737 vulnerabilities, we selected relevant vulnerabilities matching the subject criteria.

CVE-ID	Vulnerability type	Exploitation/ Adversaries	Vendor	Product Impacted	Initial disclosure
CVE-2023-51467	Authentication bypass	Observed	Apache	OFBiz	Dec. 26, 2023
CVE-2024-21893	SSRF	**UNC5325**	Ivanti	Connect Secure, Policy Secure, Neurons for Zero Trust Access	Jan. 31, 2024
CVE-2024-27198	Authentication bypass	Observed	JetBrains	TeamCity	April 4, 2024
CVE-2024-1709 CVE-2024-1708	Path traversal, Authentication bypass	- LockBit, Black Basta Bl00dy ransomware - Kimsuky North Korean-nexus group - XWORM and Toddler-Shark malware	ConnectWise	ScreenConnect	Feb. 19, 2024
CVE-2023-46805 CVE-2024-21887	Authentication bypass, Command injection	UTA0178	Ivanti	Connect Secure, Policy Secure gateways	Jan. 10, 2024
CVE-2024-3400	Command injection	UPSTYLE malware	Palo Alto Networks	PAN-OS	April 12, 2024
CVE-2024-4577	Argument injection	TellYouThePass ransomware	PHP	PHP	June 10, 2024
CVE-2024-37085	Authentication bypass	- Black Basta, Akira ransomware - **Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest**	VMware	ESXi	July 30, 2024
CVE-2024-47176 CVE-2024-47076 CVE-2024-47175 CVE-2024-47177	Improper input validation, Command injection	Observed	OpenPrinting	CUPS	Sept. 26, 2024
CVE-2024-51378	Command injection	PSAUX, C3RB3R and Babuk variant ransomware	CyberPanel	CyberPanel	Nov. 29, 2024

Summary

2024 showed the time-to-weaponize for recently disclosed vulnerabilities greatly reduced, with actors weaponizing vulnerabilities within hours of initial disclosure in many cases. This rapid exploitation highlights the urgent need for streamlined vulnerability management. State-backed actors and ransomware once again dominated the vulnerability exploitation landscape by leveraging critical zero-day and n-day vulnerabilities on critical unpatched enterprise software. Ransomware actors in particular capitalized on enterprise software weaknesses — specifically managed file transfer (MFT) software — demanding high payouts and causing widespread disruption. This year was a lucrative year for top-tier vulnerability brokers who advertised and made successful transactions that impacted widely used enterprise-grade software such as Microsoft Windows, Palo Alto Networks PAN-OS and VMware ESXi.[49, 50, 51]

The use of AI by attackers and security professionals increased this year as well, enabling the automated discovery of vulnerabilities and faster development of exploits. This capability lowered the barrier to entry for less-sophisticated attackers, resulting in an increase in attack volume and variety. Internet-of-Things (IoT) devices remained consistent points of failure, as many IoT devices operated with outdated firmware or insufficient patching for known vulnerabilities, increasing their likelihood of attacks. The interconnected nature of these devices amplifies the potential damage caused by single points of failure, making IoT security a critical area for improvement.

Artificial Intelligence: Separating Fact From Fiction

The advancement of AI remained a topic of interest to underground threat actors in 2024. We observed cybercriminals advertise a handful of AI-based tools this year, including an AI-powered data exfiltration and analysis tool; a tool allegedly powered by AI to analyze, scrape and summarize information about critical vulnerabilities and exposures (CVEs); and an AI-based tool to swap out the details of business invoices that was designed to facilitate invoice fraud in business email compromise (BEC) attacks. The majority of AI implementations we observed supported criminal activities such as know-your-customer (KYC) verification bypass, telephone-oriented attack delivery (TOAD) phishing attacks and chatbots. We also reported the use of AI in disinformation campaigns related to elections, including the Chinese-run information warfare campaign dubbed Green Cicada Network that engaged with contentious political and cultural issues to amplify social discord.[52,53,54,55]

Despite the underground's obvious interest in AI, we still have not seen cybercriminals unlock the technology's power at scale. The lack of reliable malicious chatbots leaves a lot to be desired by threat actors and highlights existing flaws in AI technology as a whole. The shelf life of malicious chatbots has been weeks to months on average, with some becoming too popular and shutting down, while others performed too poorly to attract customers. Legitimate generative AI models continue to hallucinate, confidently providing incorrect or erroneous answers. Additionally, guardrails put in place by reputable technology companies have been mostly successful in restraining actors from leveraging existing AI offers for malicious purposes such as developing malware, aside from creating relatively rudimentary variants. Threat actors likely will not be able to abuse existing generative pretrained transformer (GPT) models for anything beyond beginner-level blackhat requests for some time. The compute power required to create their own large language models (LLMs) suggests only already successful or state-backed adversaries will be able to afford the costs associated with such a task for the foreseeable future.

Predictions for 2025: Victims Will Rethink Ransoms, Infostealers Gain Features and AI Remains Novel

Themes that are likely to dominate the underground and cybersecurity landscape in 2025 include:

The RansomHub group will continue its rise as LockBit's revival fails and anti-ransomware policies will reduce victim payouts.

The sharp rise of **RansomHub** and fall of **LockBit** put into focus the fickle nature of the ransomware landscape. We see this more pronounced with the RaaS business model since these gangs are exposed to external and dynamic forces, while closed groups are far more controlled and stable. It would appear that **RansomHub** gained a large amount of **LockBit's** market share, allowing it to push ahead of its competitors. History tells us that few groups, if any, have been able to weather the headwinds **LockBit** has had to endure. More broadly, ransomware has been the apex threat emanating from the underground for several years. However, as the public becomes desensitized to data breaches and the negative press associated with affected companies lessens, the onus for businesses to pay to avoid the potential fallout also lessens. When you add in policies designed to further expose the actions of ransomware groups, it becomes more likely we will see more companies opting not to pay demands.

Recruitment of top IABs by ransomware groups will adversely affect the quality of public access offers.

Compromised access offers remained a staple of the underground ecosystem throughout 2024 and that is unlikely to change moving into 2025. Interestingly, we have seen an overall decline in the number of specified offers year-on-year for the last three years. This likely is due in part to the recruitment of freelance access brokers by ransomware groups. This possibly contributed to the fact that more than one-third of access offers this year were attributed to just three actors. If these were to disappear in 2025, the trend could ebb ever lower. However, this disparity indicates there is opportunity for newer or lesser-known access brokers to become major players in the space. Traditionally there has been no shortage of actors who seek to make a name for themselves in this domain.

Information stealers will remain the most commonly sought and leveraged malware type.

As the allure of rapid financial gain continues to draw new actors to the scene, the surge in information-stealing malware — led by prominent families such as Lumma, Stealc and Vidar — is expected to continue. These malicious tools stand out for their comprehensive, all-in-

one functionality — combining initial infiltration techniques, loader capabilities and efficient data exfiltration methods into a single framework. This streamlined approach significantly lowers the technical barriers to entry, enabling aspiring cybercriminals to easily purchase and deploy these solutions with minimal technical expertise. By 2025, these types of malware are expected not only to remain a dominant force in the cyber threat landscape, but also to evolve and adapt further, continually challenging cybersecurity defenses. In response, international law enforcement efforts are likely to focus more on identifying and dismantling the infrastructure that supports these operations, as demonstrated by recent takedowns targeting the RedLine and Meta information stealers.

Potential resolution of global conflicts will lead to a further slow down in hacktivism.

Since they began, ongoing global conflicts have galvanized hacktivists and prompted the creation of countless new groups. While many of these groups' lifespans were short, they have contributed to a frantic landscape in which DDoS and increasingly more impactful attacks have sprung from. Many of these groups used religion and nationalism as justification for their creation and attacks. However, without the impetus of conflict, support likely will lessen and the geopolitical-motivated hacktivist domain will become more muted. It is unlikely activity will return to the pre-conflict baseline given the guiding hand nation-states likely have provided, but those without backers or a strong user base could disappear.

The use of AI by threat actors will grow but is unlikely to prove decisive.

2024 was a year of change for both legitimate businesses and their criminal counterparts as both ecosystems experimented with AI capabilities. Looking forward to next year, wider adoption of AI is almost certain to occur, advancing the technology as a whole. As far as AI usage in the underground, threat actors almost certainly will continue to abuse legitimate tools to the best of their abilities, seeking logic flaws to jailbreak existing GPTs or running their own LLM instances to train datasets and serve specific malicious purposes. The use of AI technology in a variety of social-engineering schemes, its use to support the creation of malicious scripts and the appearance of AI-based tools this year suggest illicit actors are beginning to figure it out, but ultimately they still have a long way to go before AI can execute full-chain attacks on their behalf.

Sources

1. 20Feb2024 NCA press release: The NCA announces the disruption of LockBit with Operation Cronos
   https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
2. 14May2024 Searchlight Cyber article: A Timeline of Events: Operation Cronos and LockBit
   https://slcyber.io/a-timeline-of-events-operation-cronos-and-lockbit/
3. 01Oct2024 Spot Report
   Intel 471 subscription required
4. 01Oct2024 Spot Report
   Intel 471 subscription required
5. 12July2024 Intelligence Bulletin: IcedID, SystemBC, Pikabot, SmokeLoader, Bumblebee, Trickbot botnets dismantled in Operation Endgame — SITREP 12.4
   Intel 471 subscription required
6. 12Dec2024 Operation Endgame website: Operation Endgame
   https://www.operation-endgame.com/
7. 28Oct2024 Spot Report
   Intel 471 subscription required
8. 29Oct2024 Spot Report
   Intel 471 subscription required
9. 03April2024 Intelligence Bulletin: TheCom origins, groups, evolving aspects
   Intel 471 subscription required
10. 20Nov2024 Spot Report
    Intel 471 subscription required
11. 05Nov2024 CyberScoop article: Man arrested in Canada believed to be behind Snowflake customer breach
    https://cyberscoop.com/snowflake-breach-suspected-arrested-connor-moucka-waifu/
12. 06Dec2024 Recorded Future article: Another teenage hacker charged as feds continue Scattered Spider crackdown
    https://therecord.media/another-hacker-scattered-spider-charged
13. 03Dec2024 Spot Report
    Intel 471 subscription required

14. 30Sep2024
    Intel 471 subscription required
15. 06Dec2024 FINTEL: Intelligence BulletinHacktivism highlights reviewed — November 2024
    Intel 471 subscription required
16. 21Feb2024 IR: Major pro-Russian threat actors, groups conduct hacktivist operations in January 2024
    Intel 471 subscription required
17. 24Sep2024 IR: Iranian Black Mask Team hacktivist group members claim to compromise 49 supervisory control, data acquisition systems in multiple countries
    Intel 471 subscription required
18. 1Aug2024 IR: Actors on several Russian-language cybercrime forums recruit arsonists to target military vehicles in Ukraine
    Intel 471 subscription required
19. 9Dec2024 Telegram: JustEvil
    Intel 471 subscription required
20. 10Dec2024 Telegram: GROK
    Intel 471 subscription required
21. 01Oct2024 Fintel: LockBit ransomware-as-a-service affiliate program suffers law enforcement disruption — SITREP 10.6
    Intel 471 subscription required
22. 06Aug2024 Service Profile: RansomHub ransomware-as-a-service
    Intel 471 subscription required
23. 24Oct2024 Information Report: Kill Security (aka KillSec) ransomware group members customize public ransomware to attack victims worldwide, employ double-extortion tactics
    Intel 471 subscription required
24. 18Nov2024 Information Report: Actor reveals Kill Security (aka KillSec) ransomware group operations, affiliate panel
    Intel 471 subscription required
25. 10Dec2024 Service Profile: Nitrogen ransomware, data extortion group
    Intel 471 subscription required
26. 03Dec2024 Breach Report: Ransomware breach claims reviewed — November 2024
    Intel 471 subscription required

27. 05Nov2024 Breach Report: Ransomware breach claims reviewed — October 2024
    Intel 471 subscription required
28. 31Oct2024 Information Report: Actor claims to operate Sarcoma ransomware, seeks to partner with initial access brokers
    Intel 471 subscription required
29. 19Nov2024 Information Report: reveals HellCat hacking group members' recent activity, alleged future plans
    Intel 471 subscription required

Intel 471 subscription required: 30 – 51.

52. 18April2024 Information Report: intelligence-powered data exfiltration, analysis tool, possibly cooperates with ransomware operators
    Intel 471 subscription required
53. 26April2024 Information Report
    Intel 471 subscription required
54. 06May2024 Information Report
    Intel 471 subscription required
55. 14Aug2024 Spot Report
    Intel 471 subscription required

intel471 intel471Inc intel471Inc intel471 intel471_Inc

INTEL471

1209 N Orange St, Wilmington, DE 19801