
INTEL471
THE 471
CYBER THREAT REPORT 2024
Tracking threats to inform the future

Contents

Foreword

As we navigate the complex and ever-evolving cyber threat landscape, it is with both vigilance and anticipation that we present our annual 471 Cyber Threat Report. At a time when the digital world dominates nearly every aspect of our lives, the threat of prolific and persistent adversaries looking to disrupt, deny, degrade and profit from their illicit gains continues to rise. Organizations across the world are struggling to keep up with the rapidly changing threat environment, forcing defenders and decision-makers to operate in an endless state of reaction and uncertainty.

This report serves as a beacon of insight, offering a comprehensive analysis of the emerging trends, evolving techniques, varied motivations and techniques employed by threat actors from January 2023 to March 2024. Curated by our globally diverse intelligence team, this report is a testament to Intel 471's collective commitment to understand your adversaries, expose their tactics and empower you to win the fight against them.

May this report act as a catalyst for proactive, threat-informed decision-making, creating an intelligence advantage for you and ensuring the safety and security of our digital world now and into the future.

Key Takeaways

Prominent Cybercrime Trends

- **Hacktivism**
  - The most active pro-Russian hacktivist group was **NoName057(16)**, accounting for almost 60% of all hacktivist incidents during the year. The next most active groups were **Anonymous Sudan**, **CyberArmyRussia**, **Anonymous Russia** and **KillNet**.
  - From October 2023 to March 2024, the most active pro-Palestinian group was **Cyber Toufan**. The next most active groups were **Cyber Av3ngers**, **GhostSec** and **BEN M'HIDI 54**.
- **Ransomware**
  - We observed a significant global surge in ransomware attacks this year. We noted 4,429 attacks in 2023, almost double the 2,344 observed in 2022.
  - The top five most prominent ransomware variants in 2023 were LockBit 3.0, ALPHV, CLOP, Play and 8BASE.

- **Access**
  - Throughout 2023, we observed and reported 5,347 instances of access vendors offering to sell compromised credentials and/or alleged unauthorized access to networks or systems.
  - Threat actors observed with the largest number of specified access offers were those using the ***Red**, ***Blue**, ***Green** handles.[1]
- **Vulnerabilities**
  - The National Vulnerability Database (NVD) noted a significant rise in the total number of documented vulnerabilities from 2022 to 2023 — an increase from 25,081 to 28,831.
  - In 2023, Intel 471's Vulnerability Intelligence team noted 88 zero-day vulnerabilities exploited by threat actors, a 43% increase from the 50 exploited in 2022.
- **Malware**
  - Throughout 2023, we observed a substantial volume of stealers, remote access trojans (RATs) and drainers on the market. Specifically, stealers accounted for 21% of all malware-related offerings, with RATs following at 13.4% and drainers at 11.2%.
  - The dominance of information-stealer malware in the cybercrime market is expected to persist in 2024. This malware type is favored for its efficiency in extracting valuable data, profitability and the relatively low technical knowledge required to use it.

Looming Cyber Trends

- **Artificial Intelligence**
  - The advent of artificial intelligence (AI) will likely result in several threats becoming more sophisticated, less detectable and overall more convincing over time. The aspects of the threat landscape most altered by AI are social-engineering campaigns, deepfakes, know-your-customer (KYC) verification bypass and chatbot abuse.
- **"TheCom"**
  - Operators within groups of the online ecosystem known as "TheCom" are likely behind a wave of phishing campaigns, having targeted more than 100 companies. There was a focus on the U.S. based telecommunications, technology and business process outsourcing (BPO) industries.

1 *The actor's name has been redacted for operation security reasons.

Prominent Cybercrime Trends

Hacktivism

Throughout 2023, the hacktivism scene was largely influenced by two conflicts — the ongoing war in Ukraine and the reignition of war in Gaza. We observed an ebb and flow of pro-Russian hacktivism, with activity largely targeted at organizations in countries whose governments provided economic, military and political support for Ukraine and made public declarations against Russian leaders. However, the onset of the Israeli-Palestinian conflict in the last quarter of the year saw increased pro-Russian involvement, mainly in support of Palestine, before tapering off toward the quarter's conclusion. There also are several ardent groups associated with each side of the conflict in Gaza that remain active.

Pro-Russian Hacktivism

Russia's war against Ukraine continued to reverberate in the cybercriminal underground in 2023. Moreover, the conflict shows no sign of ending in the near term. As the war progresses into a third year, it is important to understand the ways in which we see the conflict play out in the underground and how the former helps to shape the latter.

Statistics

We recorded 5,368 entities impacted by alleged hacktivist attacks throughout 2023. The most active pro-Russian group was **NoName057(16)**, accounting for almost 60% of all hacktivist incidents during the year. The next most active groups were **Anonymous Sudan**, **CyberArmyRussia**, **Anonymous Russia** and **KillNet**. The top five most-impacted countries in descending order were Ukraine, Poland, Sweden, the Czech Republic and Germany. The most-impacted industries were government, transportation, banking and securities, aviation, and health care providers and services (see Figure 1).

Two Years of Evolution

In the second year of the Ukraine conflict, many pro-Russian groups were established in the underground. While their activity remained largely consistent with that observed in the first year, the infamy gained by some groups and their prominent members led to self-serving decisions and rifts among delicate alliances.

Distributed denial-of-service (DDoS) attack campaigns remained the weapon of choice for most hacktivist groups. These groups continued to target countries that showed support for Ukraine or aggression toward Russia, with Western and NATO-aligned countries receiving the brunt of these attacks.

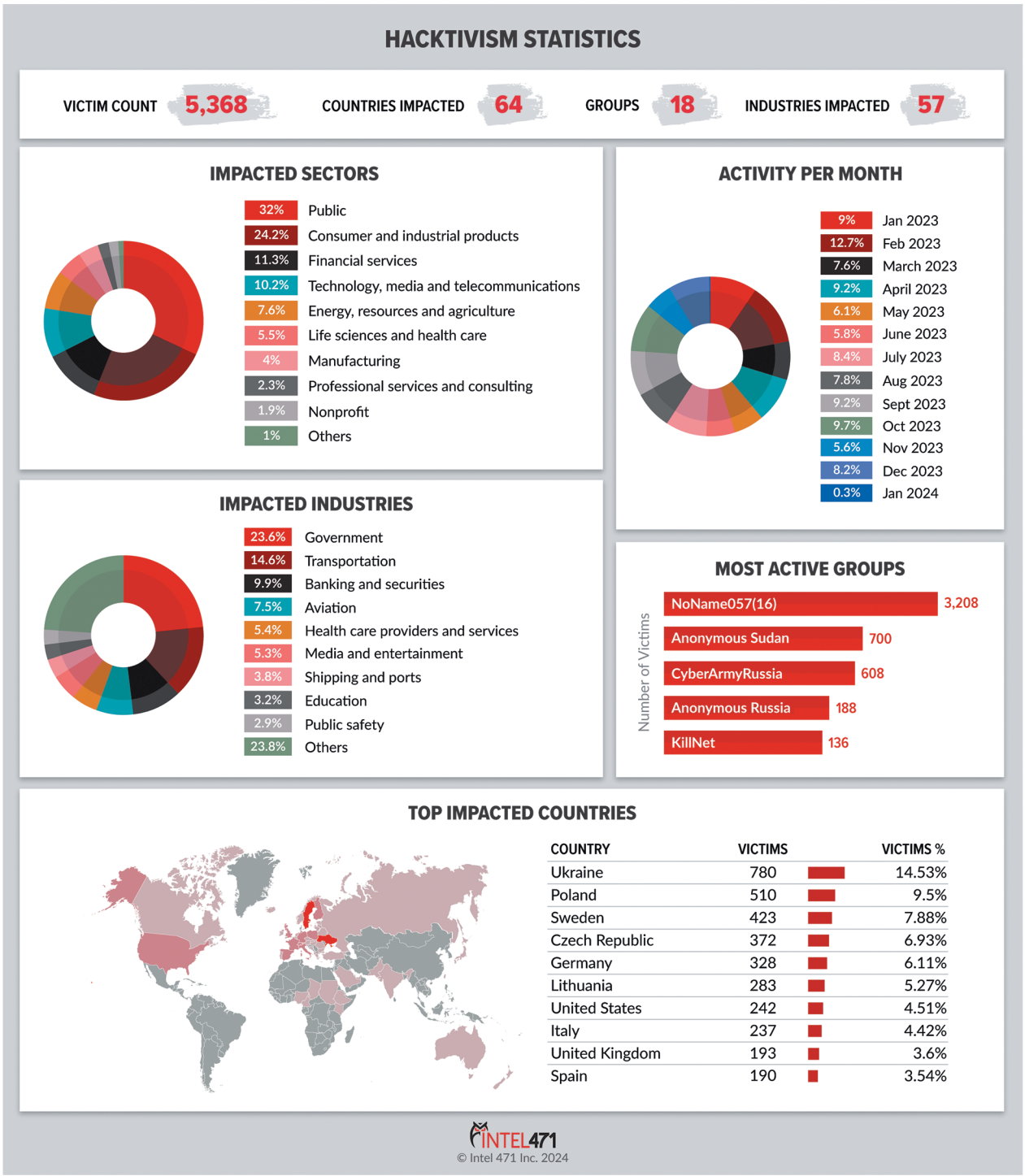


Figure 1: The graphic depicts a breakdown of hacktivist activity from Jan. 1, 2023, to Jan. 1, 2024.

Throughout the year, we observed cases of misinformation and propaganda being spread through Telegram channels. Specifically, messages of alleged "successes" of Russian armed forces on the battlefield and those of Russian hackers in cyberspace were shared. This provided evidence of a possible overlap with underground actors and the Russian state. The latter was likely keen for its propaganda to be disseminated by a myriad of sources. Collaboration with the Russian state was possibly even

sought-after by some groups as a tacit relationship would likely be perceived to confer prestige upon the affiliated group, resulting in additional capabilities, funding and membership. However, since the Russian government is highly unlikely to publicly announce any cooperation with hacktivist groups, it is difficult to determine the extent of Russian state involvement.

Additionally, alliances within the pro-Russian domain were formed more frequently during the second year of the conflict compared to the first (see Figure 2). The **CyberArmyRussia** group formed a partnership with leaders of the Russian hacker groups **22C, CyberDragon, Federal Legion, NoName057(16), PHOENIX** and **SKILLNET**. The alliance's initial agenda was to target multiple entities in Ukraine, but this expanded to Western and NATO countries that aligned with Ukraine. The **UserSec** group also announced their cooperation with **Anonymous Sudan** and claimed to take aim at European airlines as well as conduct large-scale defacement attacks. These alliances allowed member groups to coordinate more closely and magnify the impact of their attacks, potentially targeting numerous entities from one country or conducting protracted attacks against a specific organization.

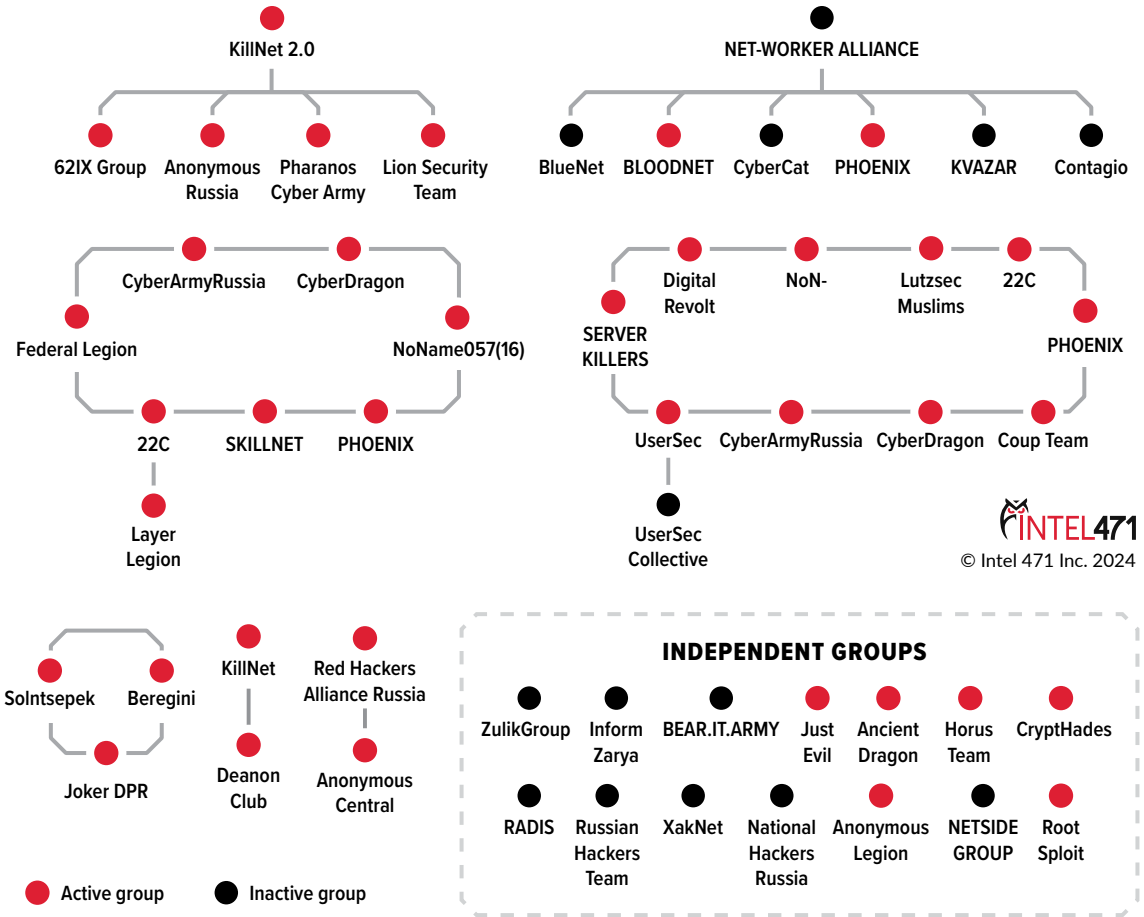


Figure 2: This image depicts the links between pro-Russian hacktivist groups as of March 2024.

By October 2023, the Israeli-Palestinian conflict also increased to new levels. Consequently, the situation in Ukraine took a back seat and the attention of pro-Russian hacktivists gravitated to the Levant. Many of the groups appeared to use the situation for opportunistic headline grabbing, while others, such as **Anonymous Sudan**, conducted protracted attacks against Israel-affiliated organizations. Initially, the conflict resulted in a reduced number of attacks associated with the Russia-Ukraine conflict. However, toward the end of 2023, we observed a spike in pro-Russian attacks once more. This rise was likely prompted by tactical victories for Russia in Ukraine, an increase in bellicose rhetoric from Russian President Vladimir Putin and high-profile cyberattacks sustained by both Russia and Ukraine.

Assessment

The pro-Russian hacktivist landscape has fluctuated over the conflict's two-year duration, yet the threat remains largely extant. The intensity of activity continues to be linked to international foreign policy pertaining to the conflict. As such, monitoring these events provides the clearest indicators and warnings for organizations located in the country of origin. As we move into the conflict's third year, the status quo is unlikely to shift dramatically. Groups will likely rise and fall as member support wanes or as more lucrative opportunities present themselves to what is likely a cadre of inexperienced cyber actors.

At the start of 2024, we observed a drop in the number of groups involved with pro-Russian hacktivism. However, the increasingly common trend of groups forging alliances is likely to result in the migration of members across collectives and is likely a net neutral in terms of overall participation. Furthermore, the increased number and size of alliances will likely result in more effective campaigns, counteracting a possible decline from ailing numbers.

We predict attacks will continue in a similar vein to what we have already observed, and it is highly likely DDoS attacks will remain the weapon of choice for pro-Russian hacktivists. This preference is likely due to the high impact and ease of use of such attacks, combined with the low barrier of entry they provide cybercriminals. Moreover, governments and critical national infrastructure (CNI) are highly likely to continue to be prime targets for pro-Russian hacktivists as we progress into 2024.

Israel, Palestine

On Oct. 7, 2023, members of the Palestinian militant movement Hamas launched a surprise attack from the Gaza Strip into southern Israel, plunging the region into conflict. Global condemnation and hacktivism swiftly followed the violence on the ground. While many sought to draw parallels with the Russian hacktivism scene —

and initial signs indicated that to be the case — pro-Israeli/Palestinian threat actors have not maintained the intensity and longevity of activity displayed by pro-Russian hacktivists.

Statistics

At the start of the conflict, open source trackers estimated the amount of hacktivist groups involved to be 118 to 137 pro-Palestinian and 19 pro-Israeli. This number has likely increased since, however, the intensity of related hacktivism has plateaued and possibly diminished as hacktivist groups that sought to leverage the conflict for publicity returned to their previous fields of interest. We monitor threats to Israel and Palestine using the 6.2.5.4 Israel and 6.2.5.9 Palestine General Intelligence Requirements (GIRs). Intel 471's reporting on the regions — including Breach Alerts and Information Reports — saw a rise in Q4 2023 in correlation with the conflict (See Figure 3). Toward the end of 2023 and start of 2024, most activity observed was low-level or, when investigated, was unfounded or appeared to relate to historical breaches.

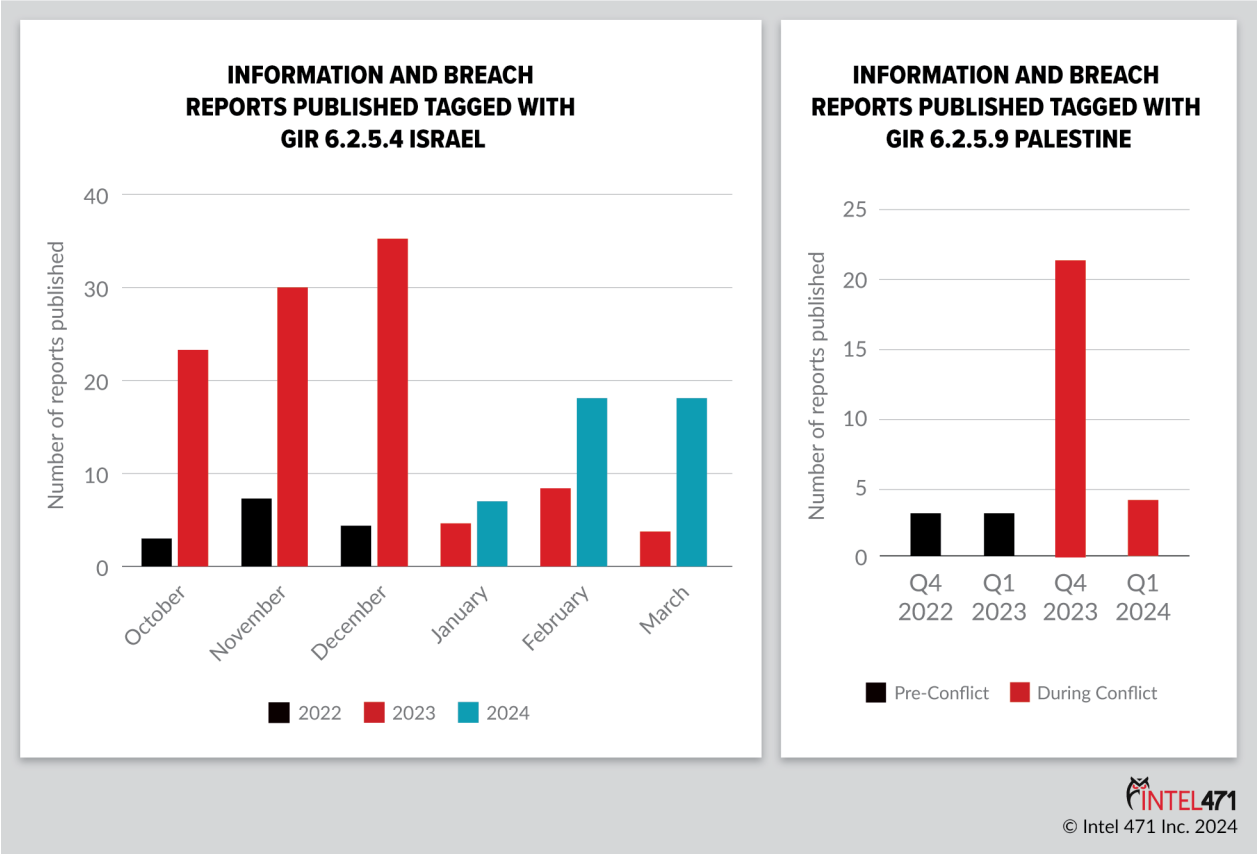


Figure 3: The graphs depict the number of Information and Breach Reports published that were tagged with the GIRs for Israel and Palestine.

Conflict Provides Opportunities for Iran and Associated Groups

The conflict is likely of great interest to the Iranian regime and reports of Iranian interference were prominent throughout the fourth quarter. On Dec. 24, 2023, the Israeli Cyber Directorate published a report that claimed 15 groups associated with Iran conducted cyberattacks against Israeli entities. Additionally, several hacktivist groups we reported were linked to the Iranian state. For example, the Iranian Ministry of Intelligence (MOIS)-linked **GURDIUM** group claimed responsibility for a spate of DDoS attacks on Israeli and Saudi entities. The Islamic Revolutionary Guards Corps (IRGC)-associated **Cyber Av3ngers** group impacted both Israel- and U.S.-based infrastructure through the compromise of Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). The latter captured many headlines and prompted three U.S. congressmen to write a letter to the U.S. Justice Department requesting them to investigate the attack.

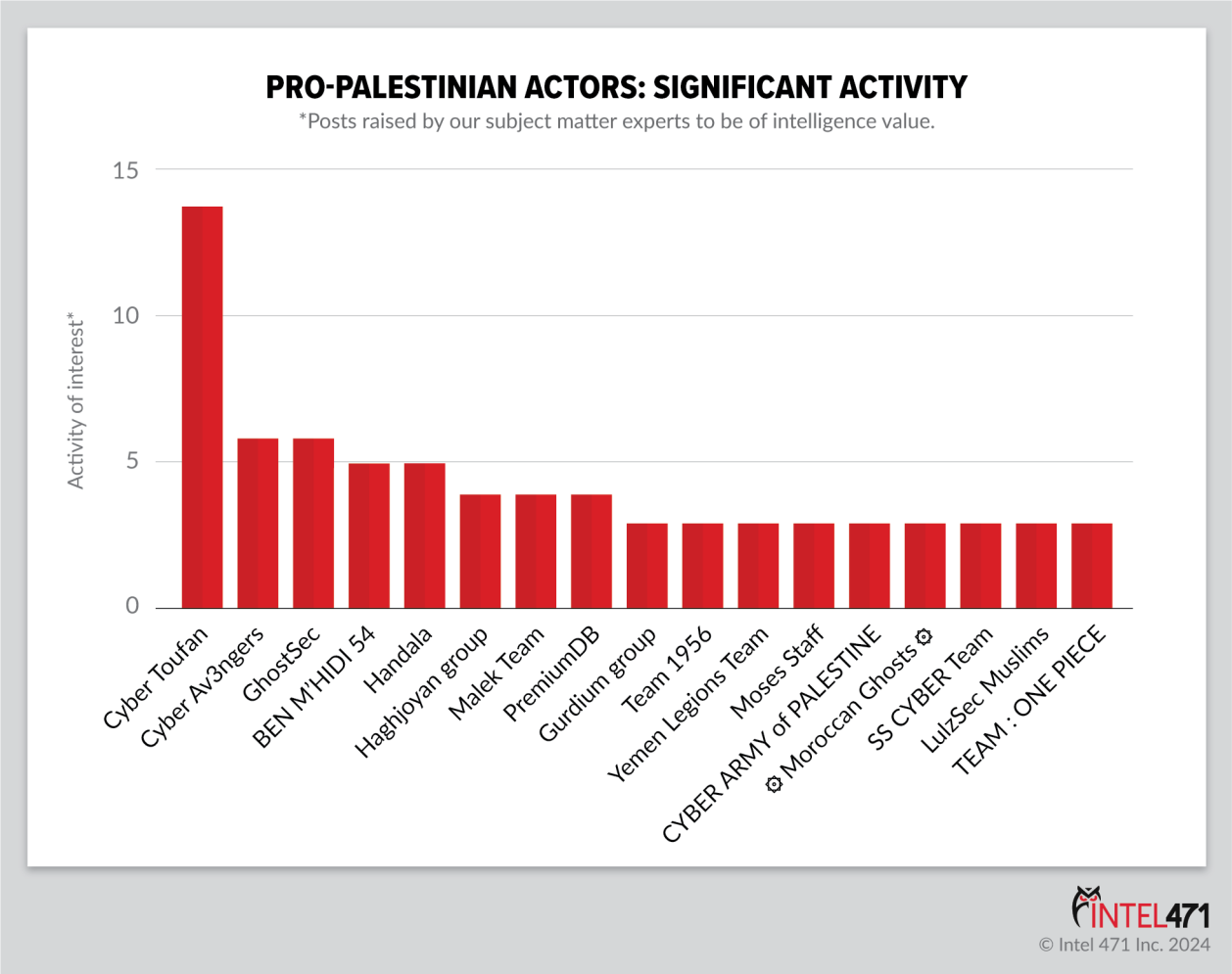


Figure 4: The graph depicts the most significant pro-Palestinian actors by number of posts from October 2023 to March 2024 with intelligence value according to SMEs.

Cyber Toufan Group

The **Cyber Toufan** group appeared as the most active pro-Palestinian group from October 2023 to March 2024 (see Figure 4). The group is part of the Anonymous #OpIsrael movement and was linked to the Iranian state by researchers. Much of its success can be attributed to its breach of the Israel-based data storage and software provider Signature-IT Ltd. which was allegedly carried out in November 2023. Following the attack, the group claimed to have impacted 150 entities, destroyed databases and servers, and extracted significant amounts of data. The group initially listed 38 alleged victims, many of which were in the national and regional government industries. We then issued 24 further Breach Alerts, demonstrating **Cyber Toufan** was highly impactful throughout the fourth quarter of 2023 (see Figure 3). Furthermore, open source reporting indicated the group had some success in destructive activity, such as wiping databases. In late December 2023, the group claimed not all of its leaks were a result of the Signature-IT breach, possibly indicating **Cyber Toufan** was not happy with the credit it received for its endeavors. At the start of the year, the group's impact diminished in line with the wider pro-Palestinian movement.

Assessment

Hacktivism associated with the Israeli-Palestinian conflict has cooled after the opening months, a trend likely to continue until a baseline is met. However, Israel has long been a target for several actors, and the conflict presents an opportunity to join forces with similar groups to enact real disruption. Equally, nation states have leveraged hacktivist groups to apply lateral, non-escalatory pressure in the past, and Iran will likely encourage the hacktivist groups it has influence over to disrupt Israeli infrastructure and provoke international condemnation of the Israeli government. Furthermore, the Iranian regime will be keen to leverage its cyber assets to monitor sentiment related to the conflict and look to use any insight gained to maneuver neighboring countries away from Israel and the West. However, these attacks will likely have limited impact and are unlikely to be coordinated enough to affect the situation on the ground.

Ransomware

Disclaimer: *The figures in this report refer only to the victims whose details were listed on data leak sites and reported by Intel 471. It is highly likely the actual number of victims is much greater since these sites typically do not disclose the identities of those who pay ransoms within a specified time period. Furthermore, we accept that not all groups who use data leak sites to extort their victims always use encryption through ransomware; however, due to the similarities in tactics, techniques and procedures (TTPs), we capture their activity in our ransomware coverage.*

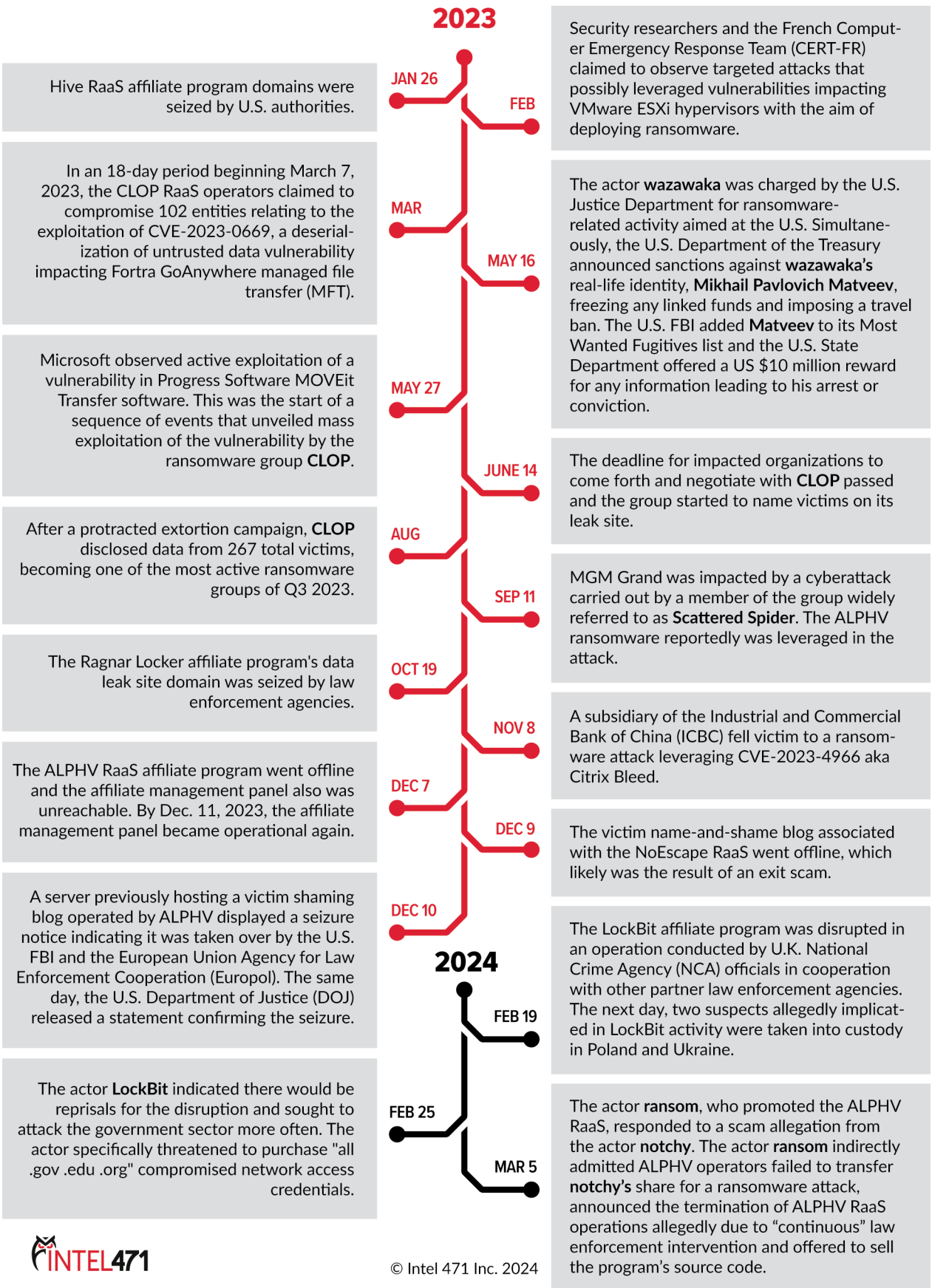


Figure 5: This timeline depicts key ransomware events in 2023 and early 2024.

Ransomware remained the principal threat in 2023 as attacks increased at an alarming rate marked by numerous high-profile incidents (see Figure 5). We observed more than 4,000 attacks in 2023, almost double the ransomware instances observed in 2022. As we progress through 2024, it is important to understand the evolving threat landscape and the impact ransomware attacks have on a range of entities.

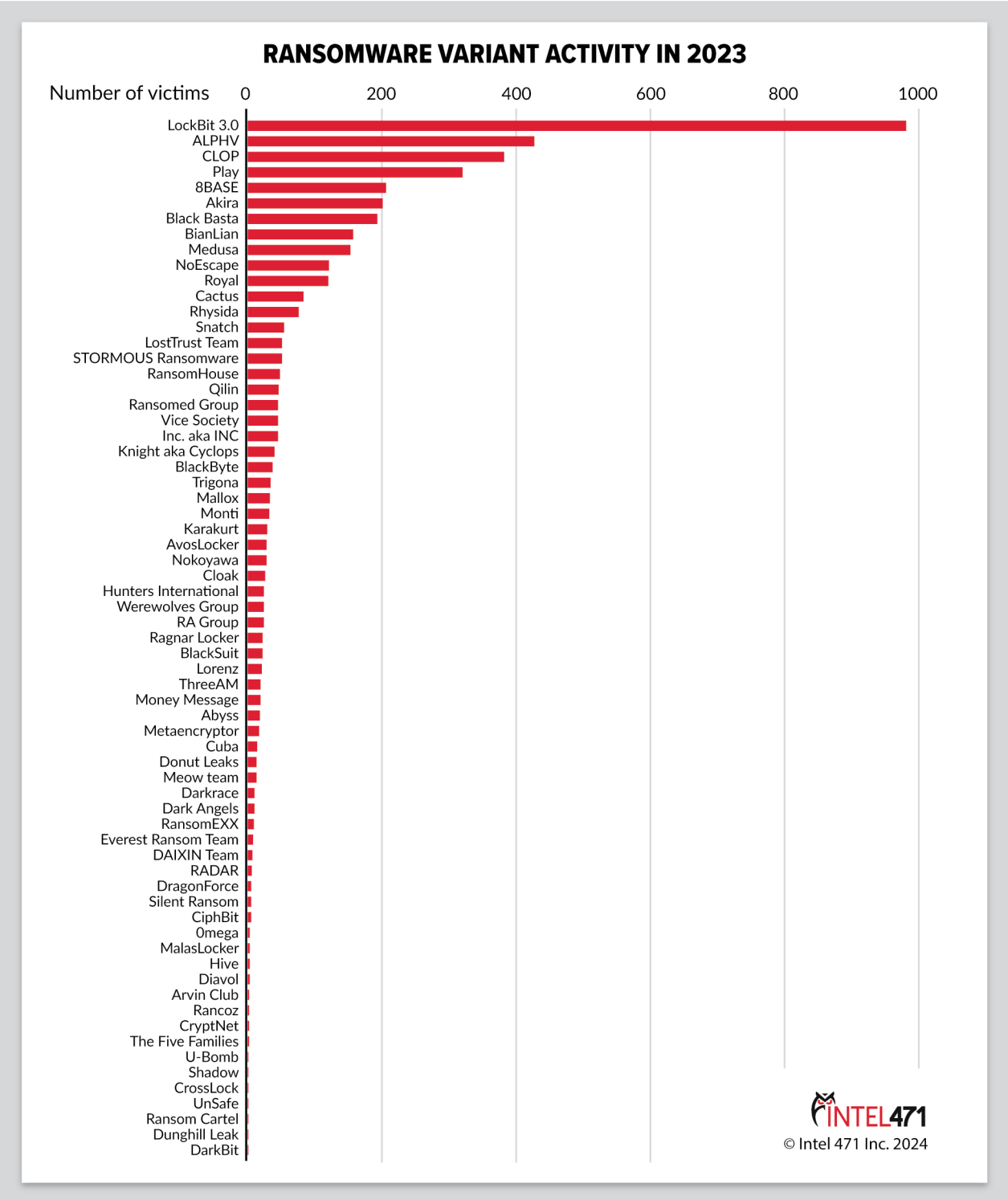


Figure 6: This graph depicts ransomware variant activity in 2023 reported by Intel 471.
**Note: Some variants were attributed to the parent strain.*

Ransomware Activity by Variant

In 2023, our reporting identified 68 ransomware variants, an increase of 19 variants compared to 2022. Once again, LockBit stood out as the most prevalent, impacting 981 victims. This was more than double the number impacted by the next variant, ALPHV, which impacted 427 victims. The remaining 67 variants each accounted for less than 9% of the total number of observed ransomware attacks (see Figure 6).

Ransomware Activity by Region

While ransomware can affect any organization, in any area of the world, some ransomware groups take aim at certain regions. North America was the most-targeted region overall in both 2022 and 2023. While all reported regions had an upsurge in attacks in 2023, North America had a notable 125.3% increase, followed by Europe with 67.7%, Asia with 46.8%, South America with 40.9%, Oceania with 55.9%, Africa with 87.2%, the Middle East with 63.5%, Central America with 61.9% and the Caribbean with 114.3% (see Figure 7).

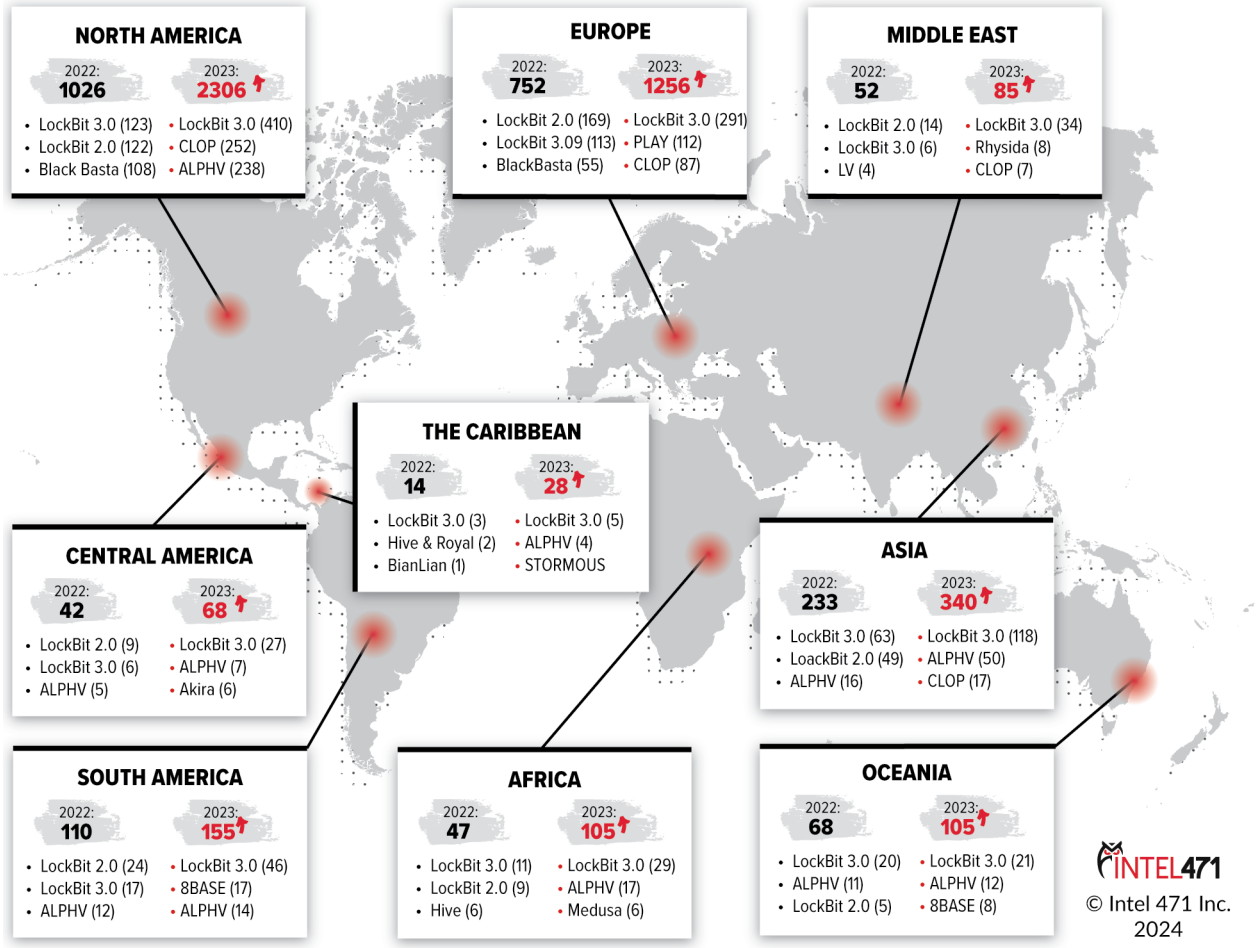


Figure 7: This map depicts ransomware attacks and the most prominent ransomware groups per region in 2022 and 2023.

Ransomware Groups Suffer Disruptions, Cease Operations

We observed a series of disruptions impacting operations of several ransomware groups during 2023.

- **Hive:** In late January 2023, we observed U.S. authorities allegedly seize Tor domain names associated with the Hive ransomware-as-a-service (RaaS) affiliate program after discovering its victim shaming blogs and victim communication website displayed a placeholder indicating the law enforcement action. Following these reports and rumors in the underground community, U.S. authorities confirmed a large-scale disruption operation against the RaaS. The U.S. FBI reported the domain names and a wider computer infrastructure were taken down, and decryption keys that allowed victims to access their encrypted data also were recovered.
- **Trigona:** In mid-October 2023, the **Trigona** ransomware group experienced an attack on its infrastructure. The **Ukrainian Cyber Alliance (UCA)** team allegedly exfiltrated and subsequently erased data from the ransomware gang's administrative panel, victim shaming and data leak blog, internal servers and backups.
- **Ragnar Locker:** In mid-October 2023, the European Union Agency for Law Enforcement Cooperation (Europol) carried out joint law enforcement action against the **Ragnar Locker** ransomware group. This action resulted in a takedown of the group's infrastructure and an arrest of the main developer of the ransomware.
- **NoEscape:** In December 2023, the **NoEscape** ransomware group's blog went offline for the second time in a few months. Several actors later accused the administrator of the RaaS of conducting an exit scam and allegedly stealing US $12 million.

ALPHV Disruption Leads to Exit Scam

In late December 2023, the U.S. Department of Justice (DOJ) released a statement that confirmed the seizure of the ALPHV aka ALPHV-ng, BlackCat, Noberus RaaS affiliate program. Despite the seizure, the group continued to post alleged victims to a new name-and-shame blog until March 3, 2024, when the blog and the group's affiliate management panel became unavailable. The same day, the actor **notchy** filed a complaint against an operator of ALPHV that accused the operator of a scam attempt. Specifically, **notchy** claimed that the ALPHV operator had appropriated a US $22 million ransom payment owed to them and their team after it breached a major U.S. health care organization. The actor also claimed that their RaaS account had been suspended shortly after the victim made the payment.

On March 4, 2024, an administrator, the actor **ALPHV**, claimed to be aware of the outage and stated that work to solve the issues was in progress. However, the message was later changed to indicate the source code was for sale for US $5 million. On March 5, 2024, the actor **ransom**, who promoted the ALPHV RaaS on the RAMP cybercrime forum, announced the alleged seizure of ALPHV RaaS operations. Subsequently, **ALPHV's** data leak site became available and displayed a similar seizure notice to the one observed in December 2023. The actor later indirectly admitted ALPHV operators failed to transfer the affiliate's share for the ransomware attack against the health care entity and blamed unspecified issues arising from law enforcement intervention. The actor **ransom** expressed the intent to sell the source code of the program and claimed negotiations already were in progress.

LockBit Appears to Weather Initial Disruption

The LockBit RaaS program also suffered disruption from law enforcement at the start of 2024. In late February, the U.K. National Crime Agency (NCA) conducted a disruption operation against the RaaS in cooperation with partner law enforcement agencies. The task force took control of **LockBit's** victim shaming data leak blog and control panel, and affiliates attempting to log in to the panel were presented with a message that indicated traces of their criminal activity were recorded by law enforcement agents. Officers allegedly obtained access to key infrastructure that belonged to the **LockBit** group and published screenshots of the compromised LockBit back-end infrastructure. They later released about 194 internally generated LockBit affiliate handles. The U.S. stated that sanctions would be imposed on those involved with the LockBit RaaS and two individuals reportedly were taken into custody in Poland and Ukraine. Simultaneously, officials at the U.S. Department of the Treasury announced the designation of two Russian individuals affiliated with **LockBit**, which included **Artur Sungatov** and **Ivan Gennadievich Kondratiev** aka **Bassterlord**, **FishEye** personas.

The leader of the LockBit RaaS, the actor **LockBit** aka **LockbitSupp**, eventually posted a lengthy statement on the RAMP underground forum that admitted the actor's own negligence with regard to network security. They claimed an improper restriction of operations within the bounds of a memory buffer vulnerability — CVE-2023-3824 — was exploited by the NCA to gain access to the group's infrastructure. Additionally, **LockbitSupp** stated the LockBit RaaS victim name-and-shame blog was available at several new Tor domains and listed multiple new victim organizations. The actor also indicated there would be reprisals for the disruption, stating an intent to attack the government sector more often and threatening to purchase compromised network access credentials related to government, educational and nonprofit organizations.

Assessment

The aforementioned activity related to ransomware group disruption in 2023 indicates law enforcement and intelligence agencies continue to improve anti-ransomware tactics dedicated to hampering and dismantling ransomware infrastructure. However, ransomware groups almost certainly will simultaneously continue to evolve their TTPs to at least maintain — if not improve upon — their profitable cybercriminal operations. Regardless, disruption operations against the top two RaaS programs of 2023 are noteworthy.

That said, the impact of these actions can take time to fully materialize. In the case of **ALPHV**, the group at first appeared to shake off the effects of the December 2023 disruption and continued operations for three additional months before folding. We assessed **ALPHV** almost certainly conducted an exit scam and used previous law enforcement action as cover for the dissolution. While it is likely **ALPHV** could have regained full operational effectiveness, the reputational damage sustained possibly resulted in mature affiliates moving away from the service. This was evidenced in the reduction of "high-value" victims added to its name-and-shame blog in January 2024 and February 2024; almost half of the alleged new victims on these blogs were small companies with lower revenues. This likely resulted in a drop in revenue and contributed to the operators' decision to conduct the exit scam.

In relation to the **LockBit** disruption, it is very rare that a ransomware group's collapse follows the same pattern as a previous example. However, the proximity in time to the collapse of **ALPHV** invites the drawing of parallels. To avoid a similar fate, we assess it is likely that **LockBit** initially sought to limit reputational damage by admitting fault for the security shortcomings and providing an assessment of how the network was penetrated. Additionally, the speed with which the **LockBit** group was able to reestablish the victim shaming blog and the addition of new victims likely reassured some affiliates. However, the victims posted were likely breached prior to the disruption and as such are an unreliable metric to assess the group's operational effectiveness post-disruption. It is almost certain affiliates will be anxious about reengaging with LockBit's infrastructure and will likely lay low before returning to their pre-disruption pattern of life.

Despite the takedown operations, ransomware remains a major threat to organizations worldwide and this is highly unlikely to change in 2024. We observed a significant global surge in ransomware attacks from 2022 to 2023, more than doubling the number of incidents and resulting in an increase observed across most regions. Despite indications that North America strengthened its security posture in recent years, it did not appear to deter cybercriminals from impacting the region.

There are several drivers for the continued focus on this region, for example, the prevalence of successful corporations based in the U.S. present lucrative outcomes for successful ransomware attacks. What is more, there is a prominence of Russian actors in the ransomware world who often prefer to target Western entities — the U.S. in particular — due to ideological and nationalist inclinations. As such, we assess North American organizations will likely remain at high risk of ransomware attacks as we continue through 2024.

Access

> ***Disclaimer:*** *This section includes data collected from Information Reports (IRs) and Breach Alerts and is not representative of all access possibly offered across the underground. Some of the access offers captured in our data points remain unverified at the time of this report and we included raw observables as part of the analysis of emerging threats and common TTPs. Additionally, we acknowledge not all access offers can be clearly or simply designated within one of our two categories. As a result, some analytical assessments are made on certain access offers to determine better categorization.*

Access Overview

The sale of access continued to grow in 2023 and remains one of the principal enablers for a multitude of cybercrime. We observed and reported 5,347 instances of access vendors offering to sell compromised credentials and/or alleged unauthorized access to networks or systems in 2023 (see Figure 8 on the next page).

Specified, Wholesale Access Offers

We previously introduced new terminology to better convey our thinking and differentiate the types of access seen in the underground into two categories: wholesale and specified.

Wholesale access is purported access to a network, resource or service by means of compromised access credentials, exploitation of a software vulnerability or misconfiguration or via similar means for which **no indicator exists that a threat actor verified the validity of access as operational.** It typically is sold en masse where an actor sacrifices quality assurance for timely sales.

- In 2023, we observed 4,272 wholesale access offers from access 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 countries most impacted

by these offers in descending order were the U.S., Brazil and Germany. The most impacted countries are likely reflective of opportunistic attacks rather than specific targeting.

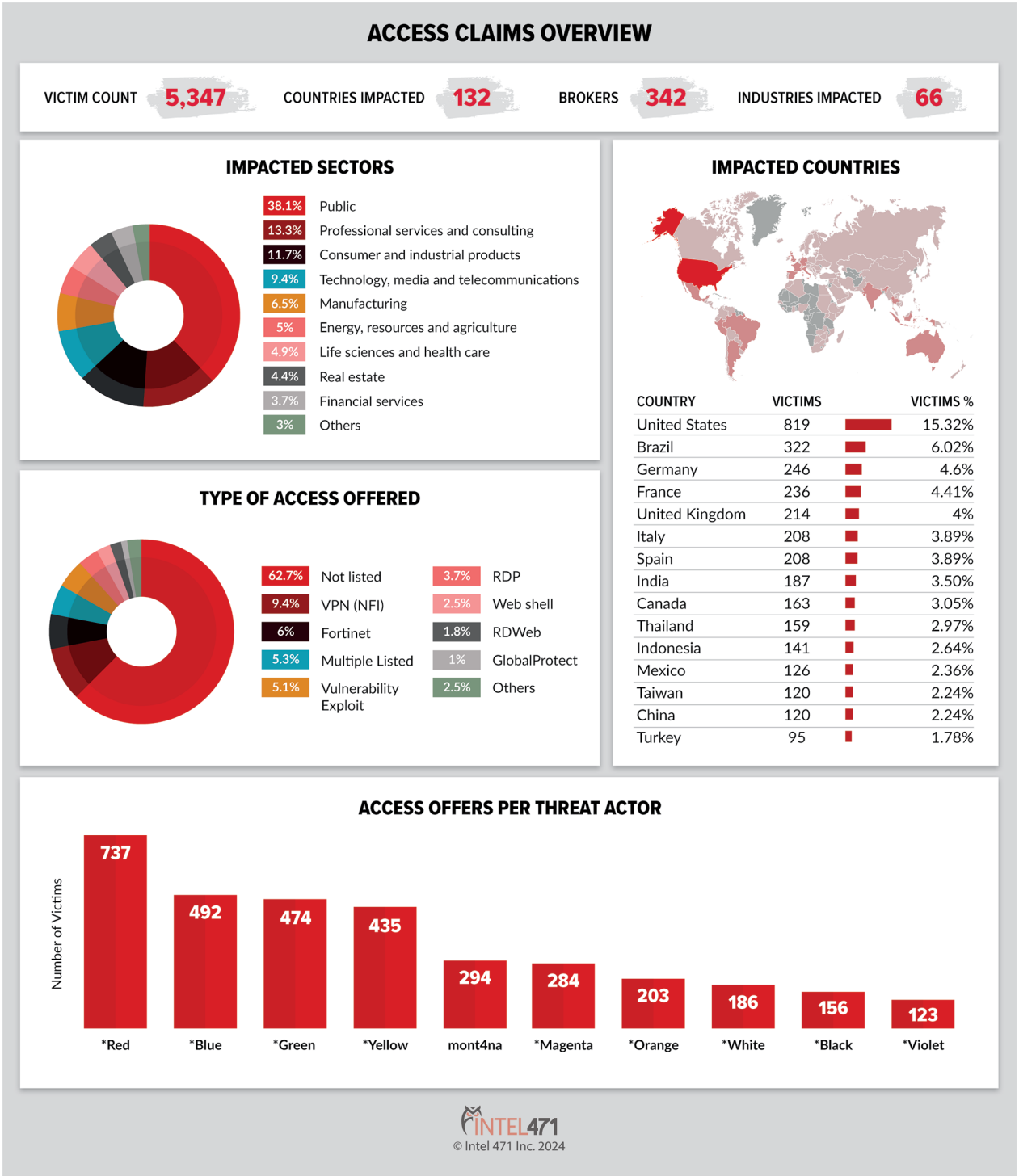


Figure 8: This image depicts the sectors and countries most impacted by both specified and wholesale access offers in 2023. The image also shows all access offers per threat actor.

Specified access is purported access to a network, resource or service by means of compromised access credentials, exploitation of a software vulnerability or misconfiguration or via similar means for which **an indicator does exist that a threat actor verified the validity of access as operational.** It typically is sold individually or in small batches with a level of quality assurance.

- In 2023, we observed and reported 1,076 offers of specified access listed for sale in the underground marketplace. The top three sectors most impacted by these offers in descending order were public; technology, media and telecommunications; and consumer and industrial products. The top three countries most impacted by these offers in descending order were the U.S., Brazil and Spain. Again, this is likely to be the result of opportunistic attacks.

Tactics, Techniques, Procedures Observed

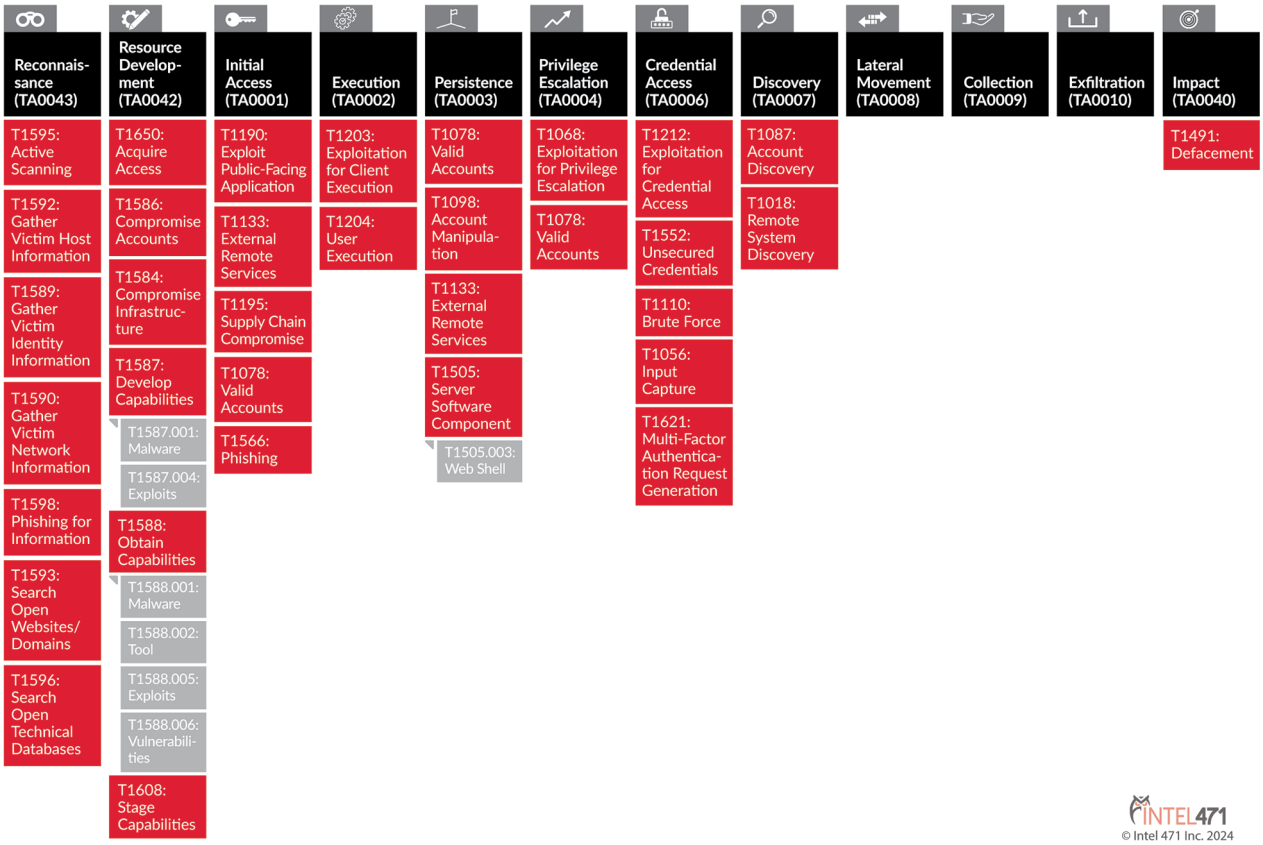


Figure 9: This image depicts the observed TTPs from threat actors offering compromised access in 2023.

We observed access brokers display several TTPs in 2023 (see Figure 9). This included different reconnaissance techniques such as identifying potential targets via Google dork complex advanced operator queries, the Advanced IP Scanner utility and the SoftPerfect Network Scanner tool, as well as seeking vulnerable and exposed assets

using search engines such as FOFA, Google, Shodan and ZoomEye. We also saw threat actors use reverse-proxy methods via secure shell (SSH) protocol-based tunnels to maintain persistence and commercially available and open source proxy client tools to redirect traffic to a victim's network.

Initial access brokers (IABs) allegedly leveraged Metasploit Meterpreter payloads, undisclosed socket secure internet protocol (SOCKS)-based tools and web shells to interact with compromised victim assets, as well as the Mimikatz pass-the-hash function to move laterally inside a victim's network and open remote desktop protocol (RDP) sessions. We also saw one threat actor employ the Hypertext Preprocessor (PHP)-based ALFA TEaM Shell web shell to maintain access and interact with compromised websites, and another use the Router Scan tool to gather information and exploit vulnerable hosts, brute-force weak access credentials and use public exploits. Other IABs also allegedly conducted brute-force, credential-stuffing and password-spraying attacks to gain access to accounts, with some likely using the NLBrute RDP brute-forcing tool. Additional tools used within the access market allegedly included the CrackMapExec, Impacket, Microsoft Windows PsExec, Rubeus and "vssadmin" utilities to facilitate authentication-based attacks.

Vulnerabilities and exploits also continue to play a large role in the process of obtaining unauthorized access. Threat actors allegedly leveraged the open source "ysoserial" tool to exploit unsafe Java object deserialization and exploited server misconfigurations as well as common vulnerabilities in exposed assets, such as a command-injection flaw that could lead to remote code execution (RCE) in certain conditions.

Assessment

The access market appeared to grow in popularity throughout 2023. The first half of the year saw averages of about 350 offers per month, which then surged to an average of 540 per month in the latter half. However, December 2023, January 2024 and February 2024 averaged about 192 offers per month. Consequently, there is a possibility that 2022's and 2023's IAB phenomena provided an opportunity for threat actors to advertise backlogs of access obtained over the course of their activity. Now that the "low-hanging fruit" has been sold and used, we could see a drop in the advertisement of unique, never-before-offered bulk credentials in 2024.

WE COULD SEE A DROP IN THE ADVERTISEMENT OF UNIQUE BULK CREDENTIALS IN 2024

Regardless, access vendors in 2023 remained key enablers of cybercrime by supplying initial access points into networks and systems for further fraudulent activity to occur and almost certainly will continue to do so in 2024. Moreover, as the market's traction continued to rise in 2023 and the number of access offers increased, we observed a similar increase in previously advertised access. As such, although wholesale access offers far exceeded specified access offers in 2023, we continue to assess the large volume of access offered by wholesalers does not always suggest or relate to the quality. Many wholesale access brokers likely seek a quick and easy profit by offering large data dumps likely derived from malware logs and/or reselling the findings of other actors rather than working to discover new access on their own.

Conversely, actors offering specified access appear to have the ability to carry out a variety of reconnaissance efforts, develop different resources to obtain initial access to systems and networks, occasionally maintain their foothold and exfiltrate an array of information. Therefore, vendors claiming to offer specified access continue to present a greater threat as they likely possess a higher level of sophistication compared to those offering wholesale access in bulk. Additionally, the collaborative relationship between ransomware groups and access brokers evolved throughout 2023 and likely will continue to develop into 2024. Access vendors persist as a crucial link in the ransomware threat chain and 2024 could see developments in the way ransomware groups interact with access brokers. As a result, we cannot rule out the possibility ransomware groups will seek to recruit skillful and successful IABs with exclusive agreements.

Vulnerabilities

Threat actors continued to exploit a variety of vulnerabilities in 2023 — both newly discovered weaknesses and unresolved issues — to carry out sophisticated attacks on global organizations. Maintaining awareness of key vulnerabilities, especially those that are actively exploited, and the array of threat actors involved can assist organizations that seek better vulnerability management.

UPTICK IN VULNERABILITIES DESIGNATED WITH CVE-2023 UNDERSCORES THREAT ACTORS' PREFERENCE FOR EXPLOITING NEW VULNERABILITIES OVER OLDER ONES

Statistics Overview

The NVD noted a significant rise in the total number of documented vulnerabilities from 2022 to 2023 — an increase from 25,081 to 28,831. The NVD

also observed a rise in critical and high-severity vulnerabilities from 14,326 in 2022 to 15,560 in 2023 (see Figure 10). This surge displays a notable increase in critical security threats presented by vulnerabilities, which pose continuous challenges in terms of tracking, prioritizing and patch implementation.

In 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) identified a total of 555 vulnerabilities that were actively exploited in real-world scenarios and therefore added to CISA's Known Exploited Vulnerabilities (KEV) catalog (see Figure 10). Among these, 91 were labeled with the CVE-2022 designator. CISA observed a decrease in the overall number of vulnerabilities added to the KEV in 2023, with the count falling to 187. However, there was a notable increase in the proportion of vulnerabilities assigned the CVE-2023 identifier, reaching 121. This uptick in vulnerabilities designated with CVE-2023, which were exploited in the year 2023, underscores threat actors' preference for exploiting new vulnerabilities over older ones, likely in an attempt to maximize their impact.

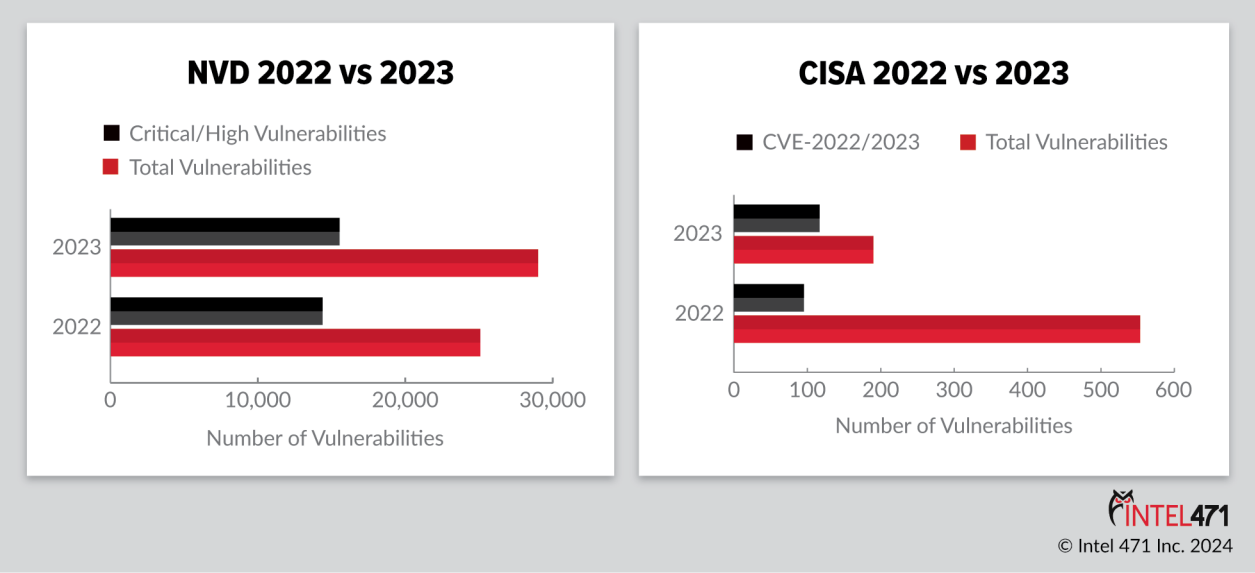


Figure 10: These charts depict the total number of vulnerabilities NVD reported as critical or high in 2022 and 2023 and the number of vulnerabilities with a designator of CVE-2022/2023 vs. all vulnerabilities CISA reported in 2022 and 2023.

Intel 471 reported an increased number of vulnerabilities in 2023 compared to 2022. In 2023, 28% of vulnerabilities were classified as high risk — up 1% from 2022, 47% as medium risk — up 4% and 25% as low risk — down 5%. Additionally, of the vulnerabilities from 2023, 10% were productized, 60% were weaponized and 16% had proof-of-concept (PoC) code available, whereas the statistics from 2022 consisted of 18% productized, 47% weaponized and 19% had PoC code available (see Figure 11).

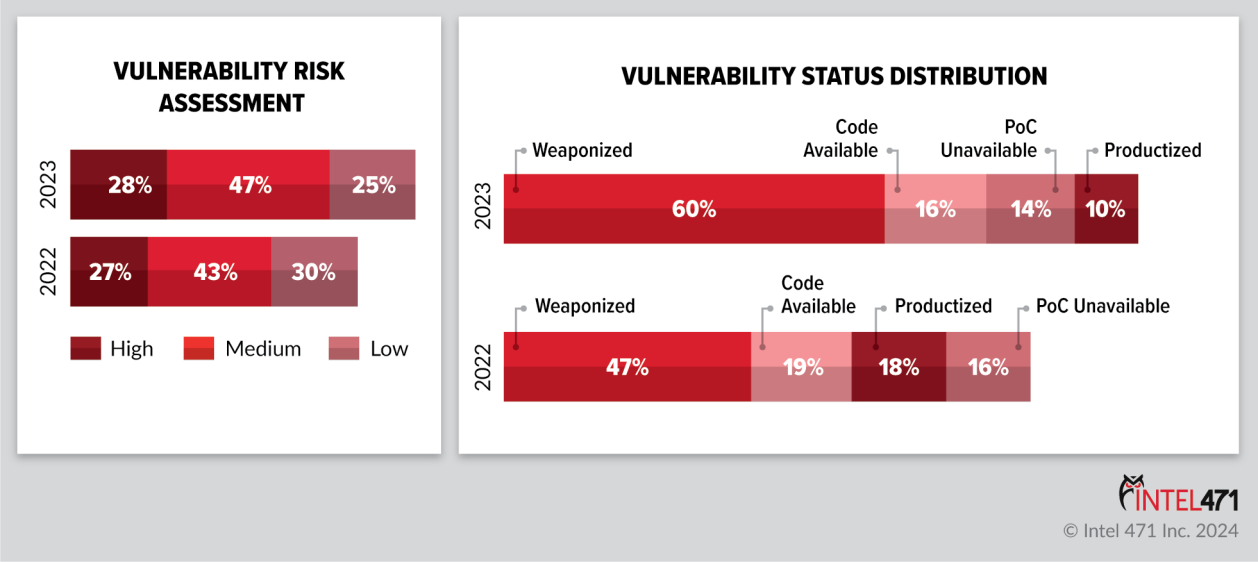


Figure 11: The image depicts the percentage of vulnerabilities we assigned a high, medium or low risk in 2022 and 2023 and the percentage of vulnerabilities we assigned a productized, weaponized, code available or PoC unavailable status in 2022 and 2023.

Vulnerabilities Exploited in Ransomware Campaigns

In 2022, vulnerabilities played a significant role in ransomware campaigns according to CISA data. Out of a total of 110 vulnerabilities used in ransomware attacks, 16 were linked to a vulnerability with a CVE-2022 designator. The remaining 94 vulnerabilities were identified with CVE designators from previous years, highlighting the diverse range of vulnerabilities leveraged. This trend continued in 2023, although

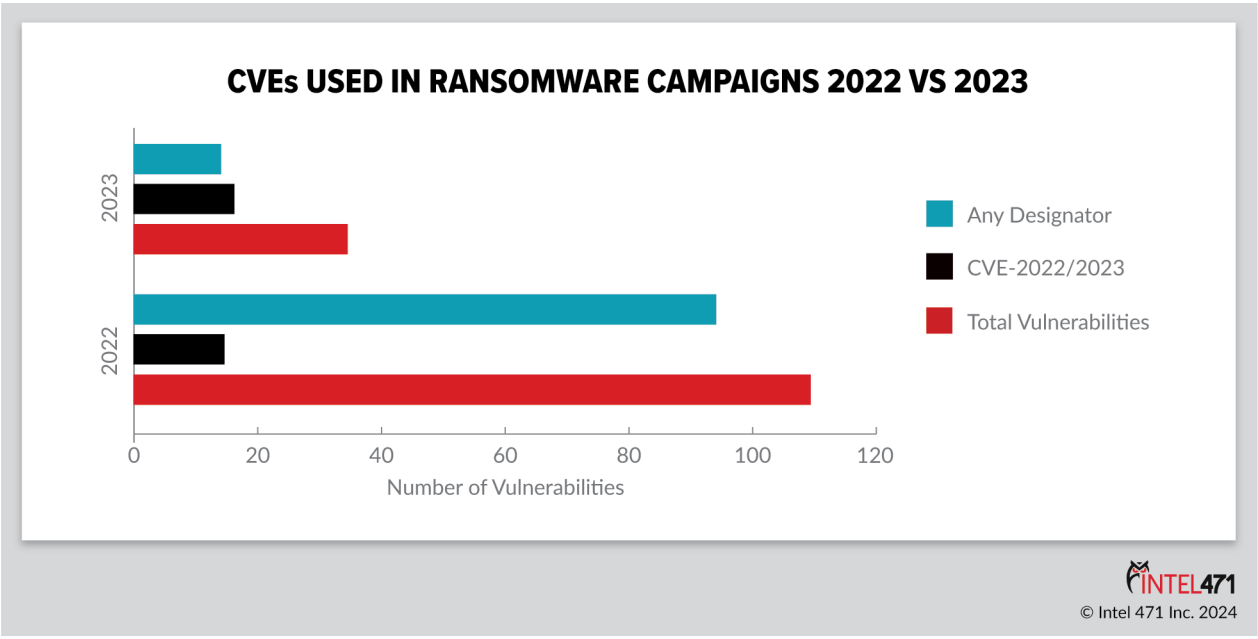


Figure 12: The image depicts the total vulnerabilities vs. CVEs with CVE-2022/2023 vs. CVEs with any designator used in ransomware campaigns in 2022 and 2023.

the overall number of vulnerabilities decreased to 34. However, there was a notable increase in the proportion of vulnerabilities used with the CVE-2023 designator, at 18. Consequently, more than 50% of vulnerabilities used in ransomware attacks in 2023 had a CVE-2023 designator according to CISA data. This suggests a more focused approach, indicating a possible shift toward exploiting recently identified vulnerabilities. Conversely, the number of vulnerabilities with CVE designators from previous years decreased to 16, implying a more selective yet potentially more impactful exploitation strategy.

Zero-day Vulnerabilities

A zero-day vulnerability represents a critical, undisclosed security flaw in software, hardware or firmware, which offers attackers a covert path to unauthorized network access, undetected movement and/or extraction of sensitive information. The term zero-day indicates the immediate risk these vulnerabilities pose, with no available patches or workarounds at the time of discovery, rendering them highly dangerous.

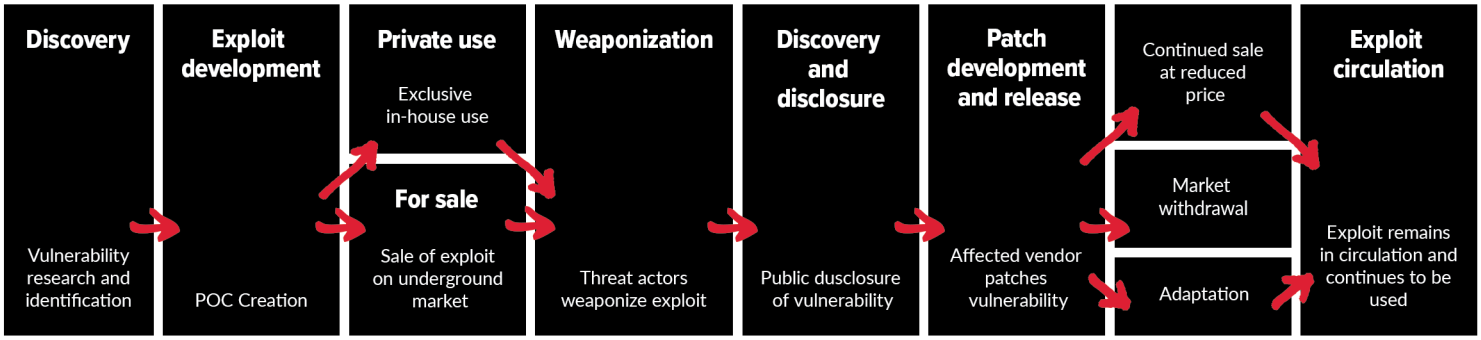


Figure 13: This image depicts an overview of the lifespan of zero-day exploits on the market.

In 2023, Intel 471's Vulnerability Intelligence team noted 88 zero-day vulnerabilities exploited by threat actors, a 43% increase from the 50 exploited in 2022. We identified 53 distinct actor handles that specialize in zero-day and N-day exploits. Among these, the actors **vulns_rock** aka **Vulns**, ***Grey** and **SebastianPereiro** emerged as the most prolific. Data from 2023 showed a 177.8% increase in the exploitation of software and web application vulnerabilities and a 41.86% increase in the exploitation of mobile operating system (OS) vulnerabilities from the previous year. Conversely, desktop and server OS vulnerability exploitations fell by 30.1%. The significant rise in the exploitation of software and web application vulnerabilities suggests threat actors are likely exploiting the broader attack surface created by the increasing reliance on digital platforms and services. Additionally, the noticeable

surge in exploited mobile OS vulnerabilities is highly indicative of their pervasive use, making these devices attractive targets for malicious actors.

Assessment

We observed a surge in vulnerabilities, rapid exploitation and evolving ransomware tactics in 2023. Threat actors were quick to capitalize on new vulnerabilities and leverage recent releases of publicly available vulnerability research and/or exploit code to target exposed instances. However, while a high number of vulnerabilities were released in the reporting period, only a handful were actually weaponized in attacks. Nevertheless, threat actors persisted in prioritizing vulnerabilities that enabled them to obtain an initial foothold within their target infrastructure and appeared to prefer recent vulnerabilities in public-facing applications to target instances that were not yet patched. As a result, ransomware operators were likely provided with increased opportunities to carry out illicit activity for financial gain. We observed this trend from ransomware actors when they actively exploited vulnerabilities in managed file transfer (MFT) software such as the one found in Progress Software's MOVEit. This exposed the reality of data exfiltration as an extortion tactic and also highlighted the growing focus on MFT software — a critical yet often overlooked attack surface.

ONLY A HANDFUL OF VULNERABILITIES WERE WEPONIZED IN ATTACKS

We also witnessed a significant rise in the exploitation of zero-day vulnerabilities throughout 2023. The 43% increase in zero-day exploitation from 2022 to 2023 provides much concern within the cybersecurity landscape and highlights an escalating threat. Moreover, the growing interest in zero-day vulnerabilities among financially motivated threat actors, particularly those involved in ransomware operations, suggests a strategic shift toward more covert and effective methods aimed at increasing success rates and thus financial gain. It is highly likely this trend will inspire a wider range of cybercriminal groups to pursue zero-day exploits, drawn by the lucrative opportunities and demonstrated return on investment from such attacks. Considering this, we

43% INCREASE IN ZERO-DAY EXPLOITATION HIGHLIGHTS AN ESCALATING THREAT

expect to see a continuous increase in the availability of exploits on designated marketplaces, indicating a sustained upward trend in this domain.

However, it also is important to note that while several threat actors remain interested in zero-days, not all of them possess the skill and sophistication to identify, develop and/or exploit them. Nevertheless, organizations are advised to enhance their detection and response capabilities with advanced threat intelligence and rapid incident response strategies, adopting a more proactive security posture. Furthermore, industry-wide collaboration and threat intelligence sharing are critical for anticipating and collectively improving defenses against zero-day exploits, ensuring a more robust cybersecurity framework in an era of escalating digital threats.

Malware

We observed several significant events within the malware threat landscape in 2023 (see Figure 14). This included the orchestration of several spam campaigns by the actor **TA577**, the resumption of activity from Bumblebee operators following a two-month hiatus and a noticeable increase in reports from cybersecurity researchers regarding spam campaigns specifically targeting the hospitality industry. Multiple malware updates also were observed throughout the year, such as the actor **raccoonstealer** announcing the release of the Raccoon Stealer information-stealing malware version 2.1, Privateloader malware bots downloading and executing a new variant of the RisePro information stealer, the actor **RastaFarEye** announcing a new version of the DarkGate malware loader and the actor **Loadbaks** revealing a major update to the actor's information-stealing malware dubbed Vidar.

There also were observed disruptions and takedowns impacting the malware threat landscape throughout the year. In March 2023, the U.S. DOJ announced a seizure order was executed against the domain name worldwiredlabs[.]com, which was used to advertise and sell the NetWire RAT. The same day, Swiss authorities seized a server that hosted the NetWire RAT infrastructure. Then in August 2023, the U.S. FBI announced a disruption operation of the QBot aka Qakbot botnet. The official statement indicated the FBI gained control of the QBot command and control (C2) and issued commands to bots to uninstall the malware. The FBI also claimed to have seized US $8.6 million of cryptocurrency assets from the cybercriminals. However, on December 16, 2023, Microsoft Threat Intelligence identified a spam campaign attributed to a new version of the QBot malware, marking the first notable QBot activity since its disruption. This comeback bears a striking resemblance to the revival of the Emotet trojan, which made a brief reappearance in late 2021 following its dismantlement by law enforcement authorities, only to fade away again after a few months.

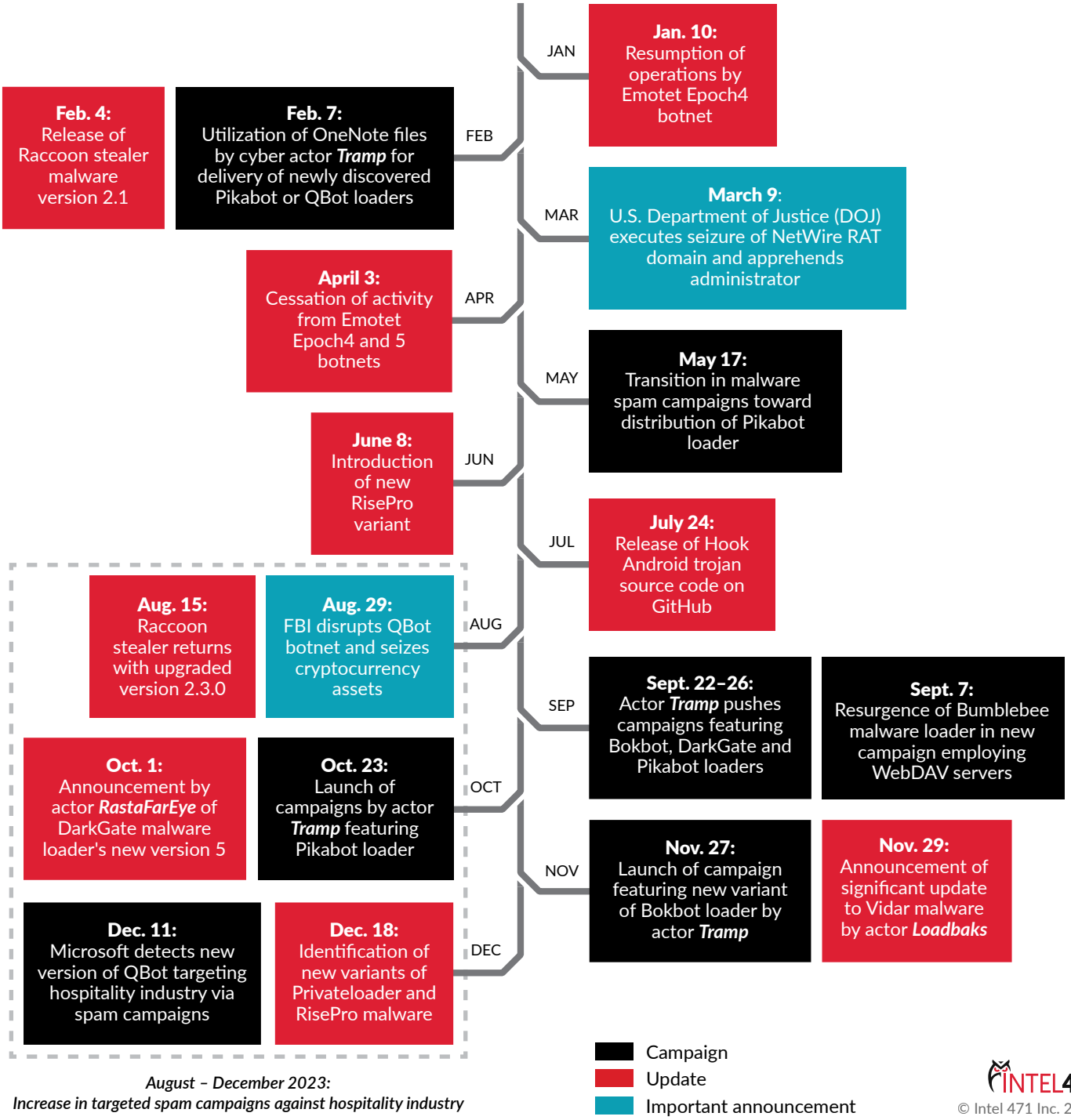


Figure 14: This graphic depicts a timeline of major malware-related events in 2023.

Disclosure: *This graphic presents a curated list of significant events from our Spot, Malware Monthly and Malware Campaign Reports throughout 2023. One or two notable events from each month have been selected to provide a concise overview of the most compelling observations made throughout the year.*

Underground Trends

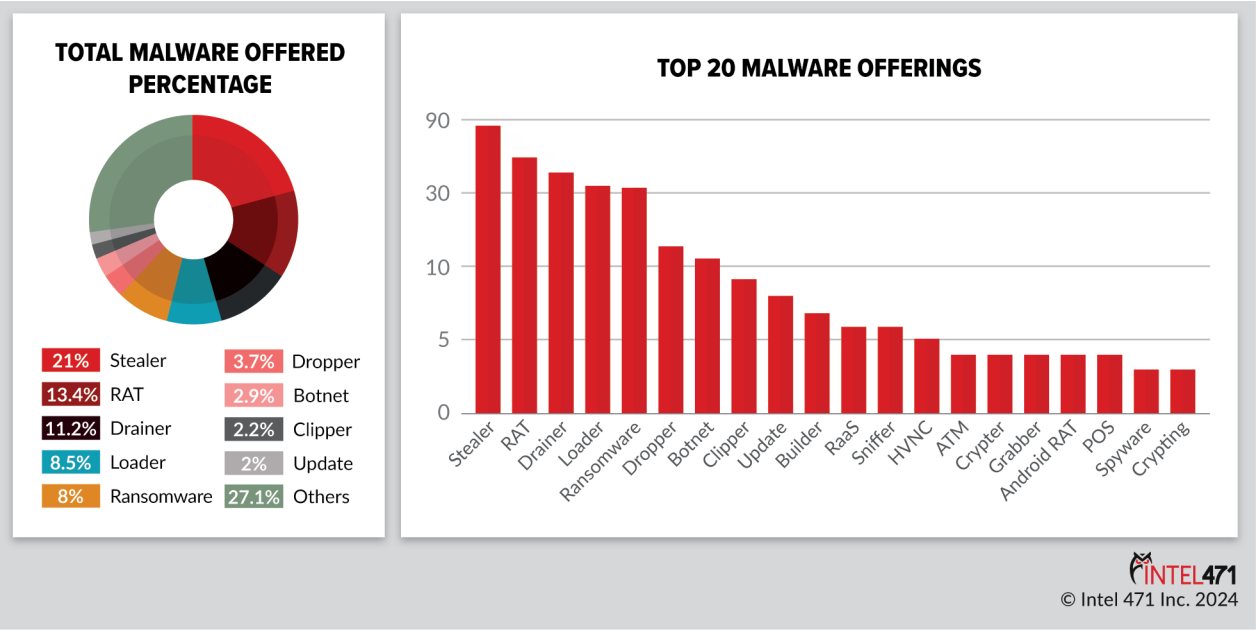


Figure 15: This graphic depicts the most popular malware offers in the underground market and their percentage of the total monitored.

In addition to technical monitoring of the malware environment, we also monitor the frequency with which threat actors offer to sell malware. This monitoring provides valuable insights into the demand for specific types of malware, serving as an indicator of the threat's prevalence. Throughout 2023, we observed a substantial volume of infostealers (aka stealers), RATs and drainers on the market (see Figure 15). Specifically, stealers accounted for 21% of all malware-related offerings, with RATs following at 13.4% and drainers at 11.2%.

Throughout the year, we also noted fluctuations in the market prevalence of different malware types (see Figure 16). In the first half of 2023, drainer malware was notably prominent, with 31 related offers recorded. This figure fell to 15 in the latter half of the year, marking a decline of more than 50%. Additionally, advertisements for loader malware saw a 60% decrease. There was also a marginal rise in the advertisement of stealer and ransomware types — though this increase was relatively minor.

Market dynamics, driven by demand and trends, dictate the prevalence of specific offers in any sector, including cybercrime. The notable decrease in drainer malware advertisements may suggest a shift in preference among cybercriminals toward the deployment of information stealers. These stealers are not only easy to use, but also tend to encompass capabilities akin to drainers, thereby offering a broader spectrum of functionalities and potentially higher rewards. Another potential reason for the decline in drainer-related advertisements could be increased competition within the

drainer market segment. Established drainer providers holding significant market share with their mature products pose a challenge for newcomers, thereby reducing the likelihood of success for newer offers in the drainer market.

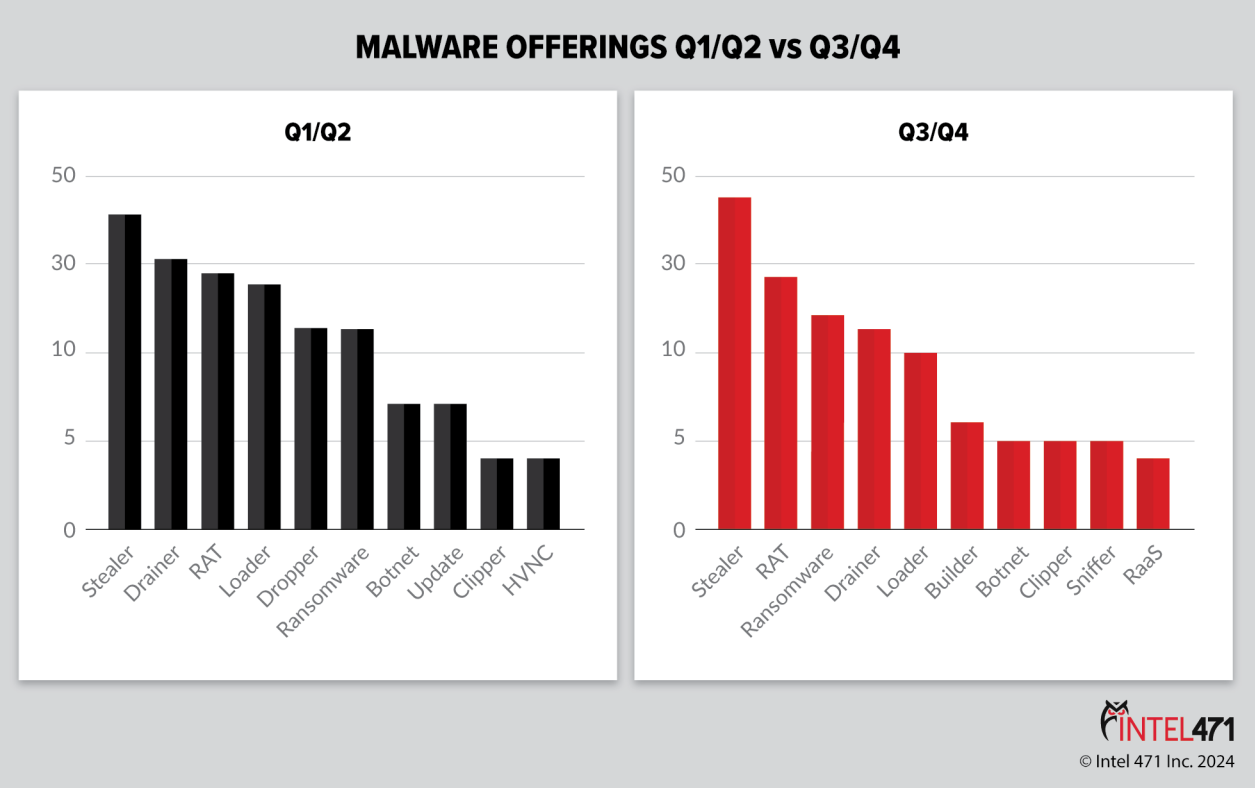


Figure 16: This graphic compares the most popular malware offers in the first and second halves of 2023.

The observed reduction in loader malware advertisements could be related to a growing inclination among users to utilize pay-per-install (PPI) services. Typically, when purchasing a loader sample, users must find a way to deploy the loader malware and subsequently use it to load the final payload. This can be complex and involve several additional steps. In contrast, install services use botnets of devices already infected with the initial loader malware. This approach allows users to directly install the malware through the service, making it significantly more convenient and cost-effective. Lastly, the uptick in ransomware advertisements correlates with the emergence of new ransomware groups within the cybercrime landscape. This trend indicates a diversification in the ransomware market and suggests a potential intensification of ransomware-related threats.

Assessment

The dominance of information-stealer malware in the cybercrime market is expected to persist in 2024. This malware type is favored for its efficiency in extracting

valuable data, profitability and the relatively low technical knowledge required to use it. We observed more than 90 advertisements promoting such malware in 2023. Newcomers such as Mystic, Lumma and Stealc managed to secure positions among the top 15 most-downloaded information stealers in 2023. Additionally, the heightened competition among malware-as-a-service (MaaS) providers will likely drive developers to stay current with ongoing trends in information stealer development. This trend signified a race among developers to enhance their product capabilities and make them more sophisticated. As a result, it is becoming increasingly challenging for newcomers to enter the market without offering a competitive product. Despite this, we do not anticipate a slowdown in the number of stealers advertised on the market — in fact, we expect an increase. Nevertheless, only a handful of new stealers will likely secure a market foothold and most may disappear shortly after their debut.

WE DO NOT ANTICIPATE A SLOWDOWN IN THE NUMBER OF STEALERS ADVERTISED ON THE MARKET — IN FACT, WE EXPECT AN INCREASE

In the case of QBot, the future remains uncertain regarding its ability to fully reclaim its former prominence. Considering QBot is an "elite product," it is unlikely the malware will become available to the wider masses. Instead, developers likely will continue to work on rebuilding the infrastructure while maintaining a low profile until the botnet becomes operational again. Additionally, given the prior maturity of QBot malware, which was in development for more than 17 years, original QBot clients will find it difficult to find a replacement. However, should a "newcomer" such as Pikabot successfully deliver a feature set robust enough to fulfill the demands of the elite clientele, it has the potential to emerge as a strong contender, possibly even surpassing QBot in certain aspects. While the complete resurgence of QBot to its previous dominance seems unlikely, the possibility of its gradual increase in the near future cannot be dismissed. Nevertheless, the true extent of this potential resurgence only can be realized with time.

With regard to the mobile malware threat landscape in 2024, we assess the evolution of Android banking trojans and advancement in social-engineering tactics are two trends to be aware of. Open source leaks of ERMAC and Hook malware source code in 2023 are expected to fuel the diversification and proliferation of Android banking trojans in 2024. The notable increase in the number of ERMAC and Hook samples serves as a clear indicator of the challenges posed by this trend. We also observed a shift away from traditional account takeover (ATO) methods toward the increasing adoption of keyloggers, as well as a rise in dropper malware on the

Google Play store. Additionally, we anticipate there will be enhancements to actors' social-engineering tactics through the use of tools such as ChatGPT. Threat actors also seamlessly have integrated technical expertise with psychological manipulation, resulting in highly effective schemes that have victimized thousands. As a result, we assess threat actors will likely develop even more sophisticated methods to lure victims into unwittingly installing malware on their systems in 2024.

Looming Cybercrime Trends

Artificial Intelligence

The release of OpenAI's ChatGPT chatbot interface for the company's large language model (LLM) generative pre-trained transformer (GPT) in late 2022 marked the first major effective AI capability to become accessible to the everyday user. This triggered somewhat of a modern-day space race, resulting in many organizations quickly working to implement AI in their own offerings. Similar to the legitimate business economy, underground cybercriminals also sought to leverage this newfound potential for their malicious products, goods and services. Throughout 2023, we observed threat actors' continued attempts to incorporate AI into their offerings via chatbot abuse, KYC verification bypass methods, social-engineering campaigns and deepfakes (see Figure 17).

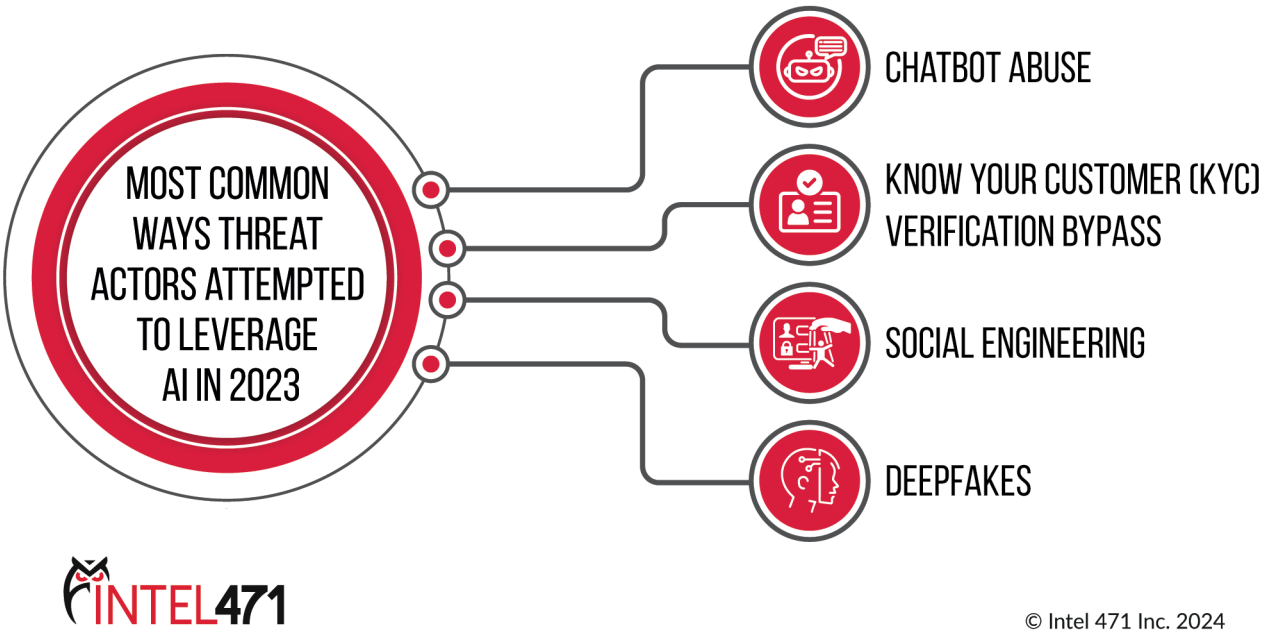


Figure 17: This graphic depicts the most common ways threat actors attempted to leverage AI in the underground marketplace in 2023.

Chatbot Abuse

Chatbot abuse was a primary use case we observed threat actors discussing in 2023. Compromised ChatGPT login credentials began to circulate on underground forums while multiple ChatGPT "jailbreaks" and malicious chatbots were advertised. Popular versions we reported included BlackHatGPT, DarkBARD, DarkBERT, Evil-GPT, FraudGPT, WormGPT and XXXGPT. Notably, interest in these chatbots appeared to dwindle toward the end of 2023, possibly due to cybercriminals learning how to manipulate ChatGPT prompts to obtain the desired results themselves. The primary outcomes that threat actors sought to achieve with chatbot abuse included the development of exploits, malware, text for business email compromise (BEC) attacks and phishing pages.

Social-engineering Campaigns, Deepfakes

ChatGPT became a popular topic of conversation in underground forums almost instantly upon its release, and social engineering was one of the main focuses. This remained constant throughout 2023 as more AI offers were made available and threat actors found ways to leverage them to conduct automatic translation, construct phishing pages, generate text for BEC attacks and create scripts for call service operators. As the sophistication of the technology evolved, so too has AI-generated spam, making it harder to differentiate real from fake.

The technology appeared to improve further with the advent of deepfakes, and the use of AI took on a new meaning for fraud-focused threat actors. The concept of deepfakes was known long before the recent spike in AI advancements, however, cybercriminals struggled to find a cost-efficient way to effectively create deepfake content. The available technology also required a creator to obtain an extensive amount of audio, photographic or video material to create anything even remotely resembling the intended victim. This resulted in the majority of content impersonating celebrities due to the vast representation of them on the internet. However, cybercriminals now are learning to develop AI-generated content they can leverage to impact common individuals and corporations more frequently.

Consequently, while celebrity-centric deepfakes might not fully be in the past, it is more likely a threat actor would be able to develop AI-generated content for phishing or extortion of your average person today compared to years ago. However, phishing and extortion are just the tip of the iceberg for what AI-produced content could influence. Years ago, there were reports of disinformation

PHISHING AND EXTORTION ARE JUST THE TIP OF THE ICEBERG

campaigns featuring deepfakes of well-recognized politicians, and recently more research showed the ease of developing disinformation content for social media posts — an application of AI we will likely see leveraged during the 2024 U.S. presidential campaign. Likewise, the increasing number of hacktivists could harness similar applications of AI and deepfake technology.

Know-your-customer Bypass

Traditional KYC verification bypass methods remain prominent in the underground despite the widely publicized AI enhancements. However, we observed actors claim to use AI in some capacity to provide better KYC bypass services. The actor John Wick allegedly operated a service called OnlyFake and used "neural networks" to generate realistic looking photos of identification cards. An author from the 404 Media technology publication claimed to have obtained an image of a U.S. driver's license from OnlyFake that allowed them to bypass KYC requirements on the OKX cryptocurrency exchange, although it remained uncertain whether the claims of the service using AI tools were true.

We also observed the actor *Maroon advertise KYC verification bypass services and claim to be able to unlock all accounts that require face verification, including ones that necessitate the user to upload a video or photo or provide them in real time via the user's phone camera. Users allegedly needed to provide several photos of the impersonated person along with login credentials to the account in question. It stands to reason that advancements in deepfake technology will likely allow services such as the ones detailed above to provide KYC bypass capabilities quicker and more effectively than before.

Assessment

The conversation related to AI and more specifically generative AI is far from over. The use of this technology in business processes, as well as its availability to the masses, raises questions about the changing cyber threat landscape, specifically whether there has been a sea change here due to the advent of AI capabilities. We maintain minimal change has occurred but, as with most threats, there is refinement to TTPs that make a threat more sophisticated, less detectable and overall more convincing over time. Consequently, rather than supporting the development of new attack types or strategies, AI has played a supportive role in making it easier to do the things threat actors already have been doing.

Nevertheless, considering we observed cybercriminals find ways to abuse mainstream AI technology in its early stages, this will only likely increase as AI products become more advanced. Threat actors will likely continue to conduct prompt injection

attacks to bypass chatbot restrictions, allowing them to leverage chatbots for malicious activities. Those involved in fraud will likely continue to seek ways to use AI tools to create media that will increase the effectiveness of offerings, such as KYC verification bypass attempts; and future advancements in deepfake technology could result in a significant increase in the success rate of ATO attacks. Additionally, the previous U.S. presidential election was marred with reports of disinformation campaigns featuring deepfakes of well-recognized politicians, and it is almost certain AI applications will be leveraged for similar activity during the 2024 election process.

'TheCom'

Overview

One of the more notorious threats of the past few years emanated from a broad online ecosystem known as "The Com" aka "TheCom," "Com," short for "The Community." TheCom is composed of a geographically diverse and independent group of individuals with a significant number of youths operating mostly from

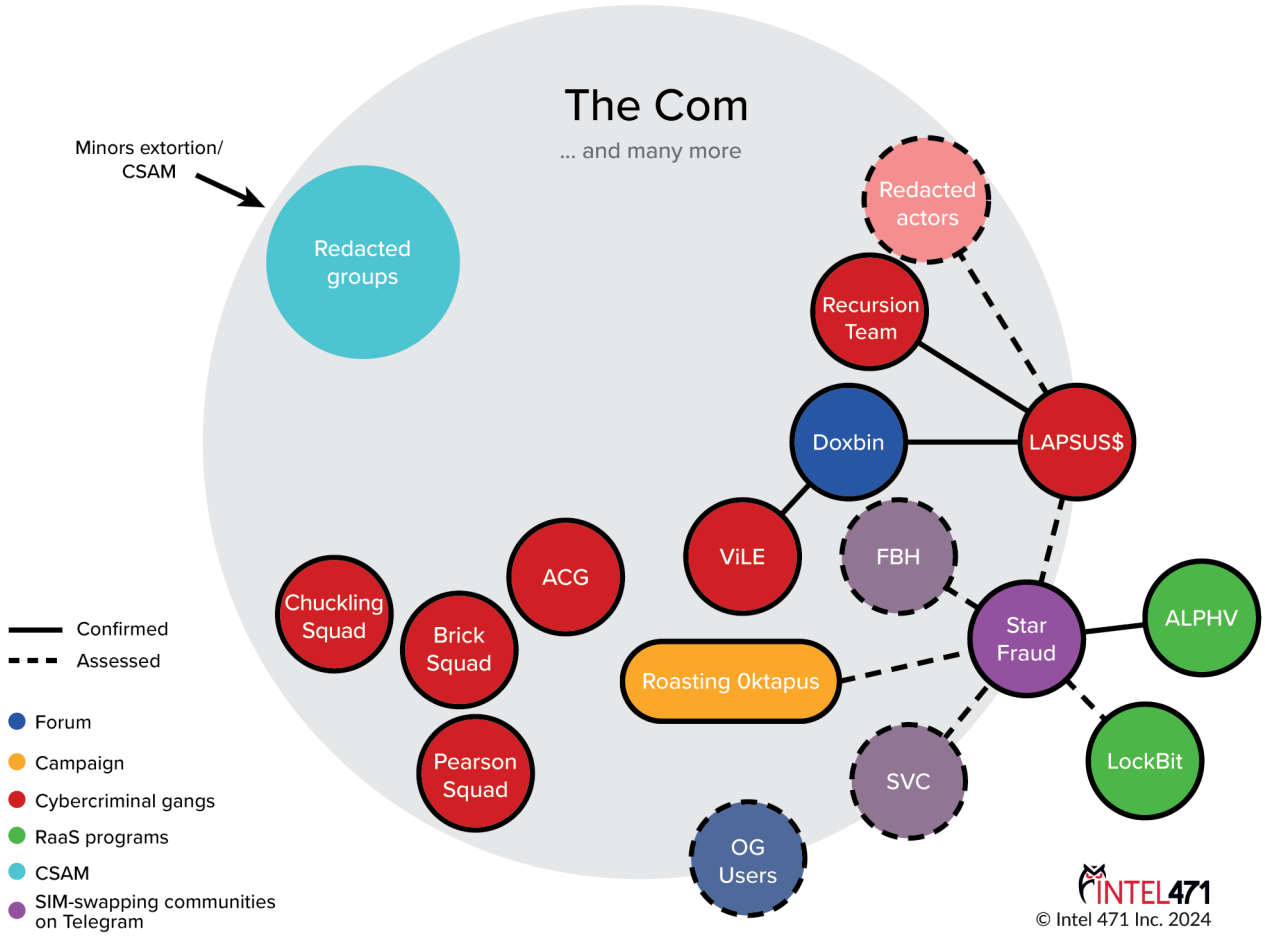


Figure 18: This graphic depicts some of the threat groups and communities assessed as part of The Com.

Canada, the U.S. and the U.K. Only a small portion of individuals operating within this ecosystem are engaged in cybercriminal activities for financial gain, such as subscriber identity module (SIM) swapping, cryptocurrency theft, online harassment, swatting, bricking and corporate intrusions. These individuals meet experienced threat actors online, form small subgroups and mix their techniques to elevate their capabilities of breaching corporations (see Figure 18).

This online community was linked as the source of a variety of high-profile compromises that occurred over the last few years and is the origin of well-known threat groups such as **LAPSUS$, Chuckling Squad** and **Pearson Squad**. The **Scattered Spider, UNC3944, Octo Tempest** and **Muddled Libra** intrusion clusters; and the Roasting 0ktapus and Scatter Swine phishing campaigns, also were linked to operators within TheCom. These groups leverage effective social-engineering techniques and tools such as adversary-in-the-middle (AITM) toolkits, conduct massive short message service (SMS) phishing campaigns to harvest login credentials of employees with access to corporate systems, lure information technology (IT) help desks into reassigning multi-factor authentication (MFA) tokens to new devices, perform SIM card-swapping attacks enabling access to victims' online accounts and conduct other notables techniques during the attack chain to gain access to core corporate systems and steal sensitive data from high-profile companies (see Figure 19). One group assessed as the source of many of these breaches was composed of more experienced ransomware operators and members from the Star Fraud aka Star Sanctuary SIM-swapping community. The group elevated their attacks in 2023 by aligning with the **ALPHV** RaaS group to conduct attacks against MGM Resorts International and Caesars Entertainment. Over the last year, we also tracked a smaller group of actors who replicated similar TTPs, revealed their intentions to affiliate with RaaS programs and disclosed a possible link with the now-defunct **LAPSUS$** group.

During the entirety of 2023, we observed waves of phishing campaigns delivered via SMS that leveraged human resources (HR), single sign-on (SSO) and other corporate themes to lure target employees across a range of organizations with the aim of harvesting login credentials and MFA codes. The phishing sites closely resemble the Okta authentication pages of the respectively targeted organizations. Operators within groups of TheCom were likely behind this wave of campaigns, having targeted more than 100 companies with a focus on the telecommunications, technology and BPO industries. Most of the targeted companies were also based in the U.S.

OPERATORS WITHIN GROUPS OF THECOM WERE LIKELY BEHIND THIS WAVE OF CAMPAIGNS

DIVERSE METHODOLOGIES AND THREAT GROUPS

The Community aka The Comm, The Com, TheCom

TheCom is a broad online ecosystem composed of a geographically diverse and independent group of individuals with an expressive number of youths operating mostly from Canada, the U.S. and the U.K. that engaged in cybercriminal activities such as SIM swapping, cryptocurrency theft, online harassment, swatting, bricking and corporate intrusions. The term originates as part of the cultural norms of tens of thousands of people, all of whom coordinate through online communication platforms such as Discord and Telegram, where only a small proportion engage in cybercrime. These individuals meet experienced threat actors, form small subgroups and mix their techniques to elevate their capabilities of breaching corporations. Several threat groups originated from TheCom such as LAPSUS$, Chuckling Squad and Pearson Squad.

Scattered Spider, UNC3944, Octo Tempest and Muddled Libra

These are intrusion clusters informing adversarial tradecraft identified from different intrusions occurring since 2022 and don't provide insights on actors or specific entities in the underground. Internally, other inputs and data sources may collaborate to bring additional context of specific actors involved with the intrusions.

Scatter Swine

Is both an intrusion analysis and phishing campaign research informing details of a large-scale phishing operation overlapping with the Roasting 0ktapus research. The report included details of findings identified during incident response engagements and correlating network infrastructure used to host the phishing pages.

Roasting 0ktapus

Is both a threat actor and campaign attribution research informing details of a large-scale phishing operation designed to steal login credentials from Okta customers and was observed about August 2022. The report included redacted details of actors operating in the underground that had high-confidence overlaps with research we conducted during the same period.

Redacted actors

We conducted threat actor attribution research on specific actors operating in the underground which revealed the use of techniques overlapping with the Scattered Spider, Octo Tempest and UNC3944 intrusion clusters to breach and steal sensitive data from high-profile companies. A smaller group possibly originating from TheCom and responsible for the compromise of high-profile companies sought access to ransomware operators to elevate their profits. Although overlaps were identified, this research leveraged different methodologies and data sources from those originating the intrusion clusters.

Figure 19: The image depicts the different research methodologies and threat groups Intel 471 observed.

Assessment

The attribution of groups adopting TTPs synonymous with TheCom will likely continue to cause broad industry confusion. The term **Scattered Spider** became a catch-all for the aforementioned groups and its use misses the mark when discussing the cybercriminals behind these attacks. For example, following the September 2023 MGM Resorts International breach, open sources referred to **Scattered Spider** as a single individual entity affiliated with the ALPHV RaaS program. It did not clarify that it actually consists of a set of observed behaviors from multiple intrusions collected over different time periods, very likely conducted by dozens of different actors. All of this exemplifies the importance of understanding and discerning research methodologies and data sources that cybersecurity firms leverage during their research. Consequently, the aim of our continued research is to provide insights about specific adversaries, groups or entities involved in these breaches.

Social engineering has proved to be an effective technique for members of TheCom carrying out waves of phishing campaigns to gain initial access to organizations. Their most recent decision to employ an HR theme likely stems from the understanding that many companies conduct employee performance reviews toward the year's end. Therefore, employees might be more inclined to perceive requests to access the HR portal as legitimate during this period. With the continued success of these campaigns and the limited resources required to conduct them, it is almost certain these threat actors will continue to conduct similar campaigns and will likely inspire other threat actors to adopt the same methods.

Threat Outlook

2023 proved to be a significant year for cybersecurity teams. Natural selection shaped the threat landscape, with actors adapting to maintain operations and their relevance against competition and disruption. Ransomware was a primary threat, with the wider landscape shifting to support the ransomware machine, resulting in a near doubling of victims. Furthermore, our data shows the first two months of 2024 consisted of 45% more ransomware attacks than the same time period in 2023. This growth was not without complications. The top two most impactful RaaS groups were hit with law enforcement action, resulting in a shaken **LockBit** and the eventual capitulation of **ALPHV**. This could precipitate a drop in victims in the coming months compared to the previous year. Nevertheless — as is often the case with ransomware groups — where one falls, two will likely rise to replace it, ensuring the pervasive threat of ransomware is here to stay in 2024.

For the last two years, we also observed the access market grow to service the expanding ransomware market, yet the number of access offers appeared to dwindle in the final month of 2023 and into the first two months of 2024. While this is not a definitive indicator for how the market will fare in 2024, it does raise questions regarding the popularity of broader access methods. With the increasing popularity of information-stealer malware and phishing-as-a-service (PhaaS) offerings, we cannot rule out the possibility that threat actors are cutting out the middleman — namely IABs — and obtaining access credentials on their own. There would therefore be less need to purchase and/or openly advertise bulk offerings of initial access. However, it is more likely that low-quality, bulk access offerings are less attractive to threat actors. So, while 2023 might have been the year to sell the "low-hanging fruit" that is wholesale credentials, which have a relatively high rate of duplication, 2024 could be the year of more unique and specified access offerings which provide threats actors more value.

2024 COULD BE THE YEAR OF MORE UNIQUE AND SPECIFIED ACCESS OFFERINGS

Simultaneously, the malware landscape rapidly is evolving, with a significant focus on the aforementioned information-stealer malware expected to dominate in 2024. The competitive environment of the MaaS market is poised to fuel further innovation and enhance the sophistication of these malicious tools. We also expect the introduction of new attack vectors by threat actors for malware deployment. This will likely include an increased reliance on both zero-day and known vulnerabilities, as well as the broader exploitation of widely used web protocols such as Web Distributed Authoring and Versioning (WebDAV). Additionally, the development of more complex social-engineering tactics is anticipated, posing substantial challenges for organizations trying to distinguish between legitimate interactions and malicious phishing efforts. With the latest advancements in mobile malware, there also is an increased potential for more campaigns targeting Android users, potentially introducing new mobile malware families to the market.

As we can now see, vulnerabilities continue to be intrinsically tied to ransomware, initial access and a variety of malware campaigns. CISA reportedly added slightly fewer vulnerabilities with 2024 designators to the KEV over the first few months of 2024 compared to the same time period of 2023, regarding 2023-designated vulnerabilities. While a drop in such reports is a positive start to 2024, threat actors remain quick to take advantage of new vulnerabilities and leverage recent releases of publicly available vulnerability research and/or exploit code to target exposed instances — of which ransomware operators almost certainly capitalized on.

AI is guaranteed to capture the imaginations of the cybersecurity fraternity while its development continues at such a notable pace. We assess the most pressing threat stemming from the underground use of AI at present is the enhancement of social-engineering techniques such as AI-generated voices for call services as well as text for phishing campaigns and BEC attempts. For now, malware development and coding via AI remains inadequate and legitimate AI tools continue to implement measures to stop threat actors from abusing them in this way. Nevertheless, while legitimate business operations seek to enhance their own offerings with AI, so too will cybercriminals. We therefore almost certainly will continue to see the commercial and cybercrime usage of AI play out throughout 2024 and beyond as the technology becomes more advanced and easier to work with.

We also continue to monitor activity related to TheCom. We assess more subgroups will likely arise in 2024, making it more difficult to differentiate between groups within the community. Additionally, there is the possibility that as more threat actors join these groups, there could be a greater likelihood of increased sophistication through collaboration. However, at the same time, we also cannot rule out the possibility that more members could result in a reduction to TheCom's overall skill level and even impact the group's operational security since a larger number of individuals is likely harder to monitor and/or keep in check. Regardless, we aim to keep our finger on the pulse for any noteworthy subgroups that crop up as we continue through 2024.

Overall, the core cyber threats facing organizations worldwide remain familiar. However, activity observed within each realm continues to fluctuate and awareness of such variations only can benefit you and your organization.

How Intel 471 Can Help

Intel 471 arms enterprises and government agencies to fight the cybersecurity war using real-time insights from the cyber underground. We are a trusted advisor to security teams, assisting organizations in their efforts to safeguard sensitive data and critical access by uncovering threats and highlighting indicators and warnings before an incident occurs.

Organizations leverage our cyber intelligence platform to gain real-time monitoring of threats to protect their organization from costly, debilitating security breaches and cyber incidents. Our intelligence domains enable security and intelligence professionals to solve cyber use cases, including attack surface protection, third-party risk management, security operations, brand protection and fraud.

With structured data, less noise, and high-fidelity results, you can focus your team on the threats that matter most. Help protect your organization from costly debilitating security breaches and other incidents, while delivering more value to the business. Let us join your fight against cybercrime.

Learn more at **www.intel471.com.**

Intelligence Domains

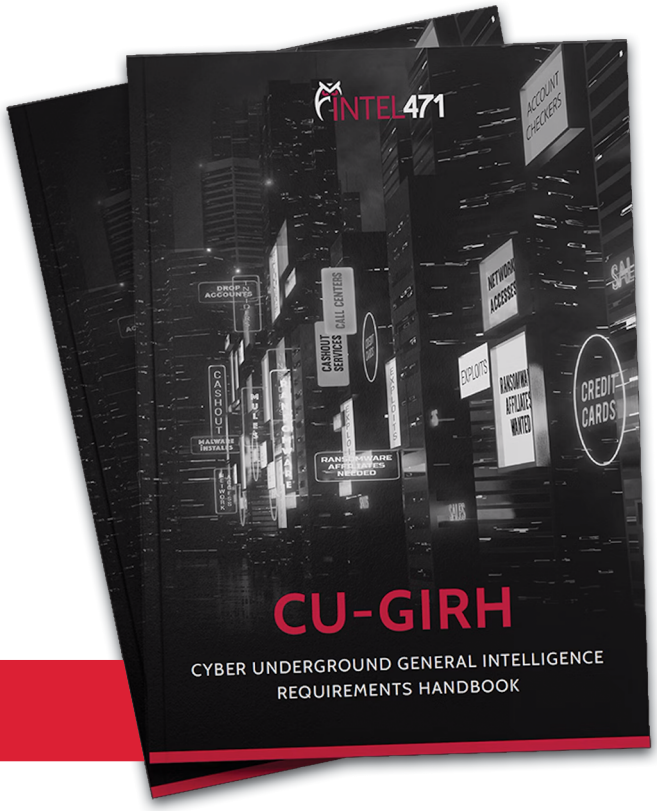
- **Adversary Intelligence:** Ground-breaking insights into the who, what, where and why of cyber adversaries and their methodologies via automated collections and human intelligence (HUMINT) infiltrating where they operate: the cyber underground.
- **Credential Intelligence:** Continuous monitoring and analysis of compromised credentials found across the cyber underground related to your employees, VIPs, third-parties and more.
- **Malware Intelligence:** Track threats through real-time monitoring of malware activity at the command and control level with our patented Malware Emulation and Tracking System (METS), human analysis, high-fidelity stream of technical indicators and reporting to harden your defenses.
- **Vulnerability Intelligence:** Analyst-driven assessment of vulnerabilities and their life cycles, including weaponized and productionized threats, to enable patch prioritization and vulnerability management.
- **Marketplace Intelligence:** Insight into the most prolific and active underground marketplaces and where illicit goods, such as stolen credit card details and compromised credentials, are bought and sold.

Cybercrime Underground General Intelligence Requirements Handbook

To assist cybersecurity teams in defining relevance, synchronizing the intelligence effort, and routing information to the right stakeholders or systems, Intel 471 developed a proprietary framework: the Cyber Underground General Intelligence Requirements (CU-GIR). Our intelligence domains: Adversary, Credential, Malware, Vulnerability and Marketplace Intelligence are mapped to this framework and are driven by your Prioritized Intelligence Requirements (PIRs).

Our Cybercrime Underground General Intelligence Requirements Handbook (CU-GIRH) can be used as a baseline tool to assist security professionals and teams in organizing, prioritizing and producing cyber underground intelligence. Central to this handbook are General Intelligence Requirements (GIRs) — a compilation of frequently asked intelligence requirements applicable to the cybercrime underground such as forums, marketplaces, products, services and threat actors. Our handbook also contains a list of common intelligence stakeholders and use cases, along with a comprehensive cybersecurity glossary.

The Intel 471 Intelligence Team has been using this framework for years. It underpins the research and collection methods used to provide the clear and concise reporting for you in this report. We want to share it with the community. Access to the CU-GIRH includes Intel 471's Intelligence Planning Workbook — a collection of templates and samples used by intelligence planners to operationalize the GIR framework, gather requirements from stakeholders and measure success. Download a copy of the GIR Handbook on our website.

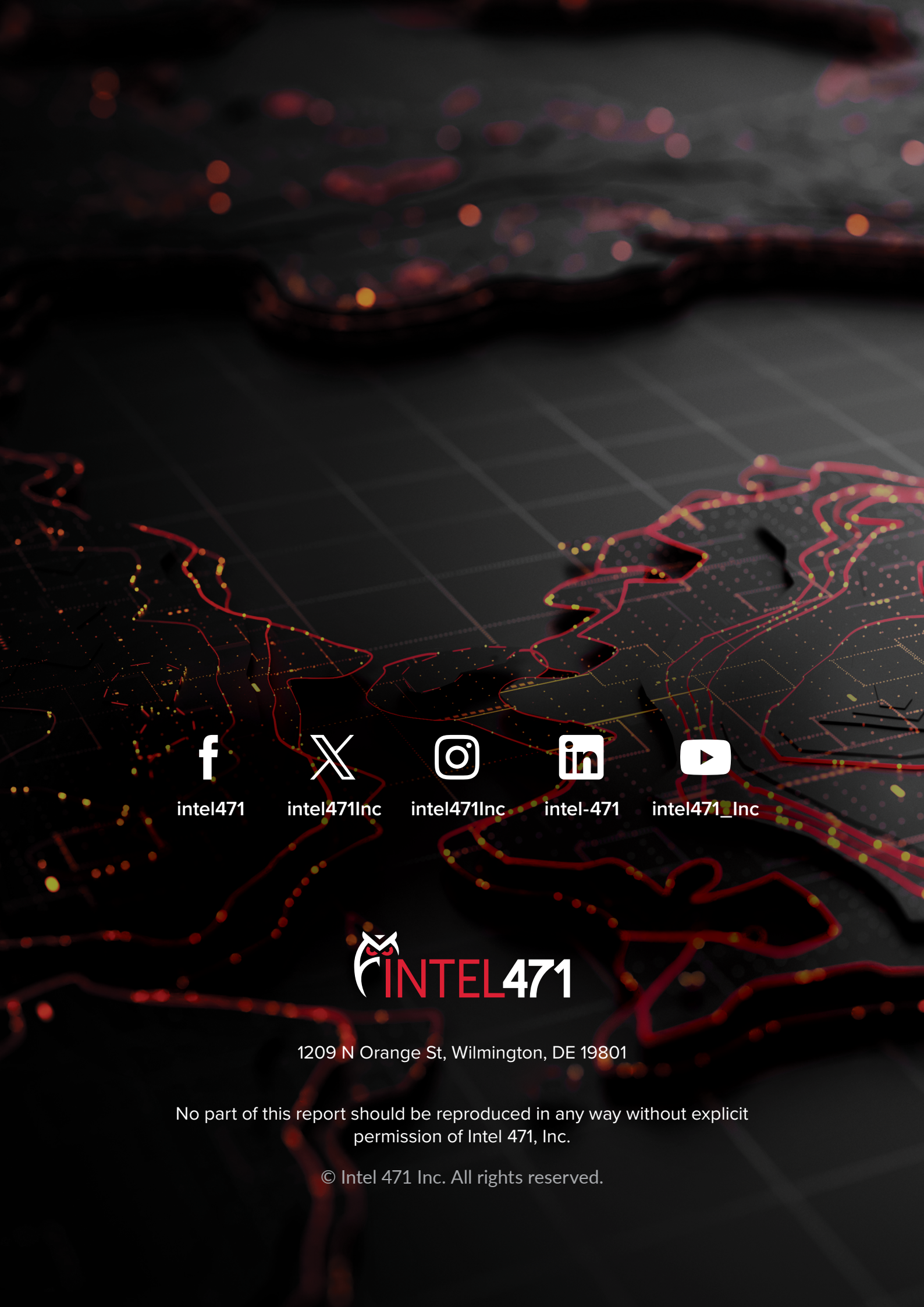


Download CU-GIRH handbook

A Note on Report Data

The reporting metrics for this report were sourced from Intel 471 reports and data. Therefore, they are not representative of all instances related to the aforementioned threats possibly claimed across the underground. Ransomware groups typically do not broadcast ransomware breaches when the victim pays the desired ransom, and some hacktivist claims and access offers captured in our data points remain unverified at the time of this report. It is important to highlight that our analysis is based on events specifically observed and recorded by Intel 471. Additionally, we included raw observables as part of the analysis of emerging variants and common TTPs.

Notes



intel471 intel471Inc intel471Inc intel-471 intel471_Inc

INTEL471

1209 N Orange St, Wilmington, DE 19801