TLP:CLEAR

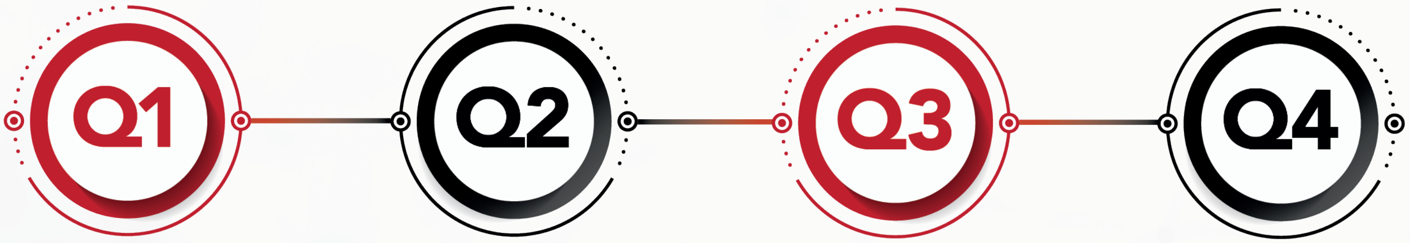
INTEL471

2022 - YEAR IN REVIEW

Introduction

The year of 2022 presented both new and evolving trends. We primarily recognized significant activity in five main areas – Russia's war in Ukraine and its underground implications, the continued popularity and evolution of ransomware, the rise and endurance of initial access brokers (IABs), developments in the malware threat landscape and consistency in the search for and use of vulnerabilities. Additionally, we observed a variety of trends through an analysis of our General Intelligence Requirements (GIRs) from 2021 to 2022. Our research and collection methods largely are driven by our GIRs, however, we continue to acknowledge that new trends in our reporting, recurring requests for information (RFIs) and other significant activity from or against underground threat actors and/or services are equally important to our research into trending topics.

***Actual threat actor names have been altered for operational security (OPSEC) reasons. All names have been altered to names of mountains, for example Etna, the mountain on the east coast of Sicily, Italy.**



- Conti leaks
- Raid Forums Outage
- Breached Forums announcement
- FSB announces house raids conducted against alleged members of REvil ransomware group
- Multiple Ukrainian state agencies hit with cyberattacks

- Raccoon Stealer resumes operations with version 2.0
- LockBit releases version 3.0
- Highest amount of initial access broker offerings
- Follina aka CVE-2022-30190 vulnerability discussed widely in underground
- Actor KillNet issues ultimatum to Lithuanian government, launches anti-NATO offensive operation days later

- LockBit 3.0 dominance
- Russian hacktivist attacks continue, multiple groups join in conducting DDoS attacks
- LockBit 3.0 suffers DDoS attack, leaked ransomware builder

- QBot distributors increase spamming volume during two-week period
- The most initial access broker handles offering victims
- Decline in activity from Epoch5, Emotet botnet, Epoch4 offline since early December

Figure 1: This image depicts a timeline of notable events from 2022.

Introduction

Key points:

- Russian hacktivists who engaged in cybercrime to support the Russian war effort will continue to diversify their capabilities to include targeted attacks leveraging malware. In 2023, pro-Russian hacktivist groups likely will seek to use ransomware they obtained or developed in recent months.

- LockBit 3.0 likely will remain the dominant ransomware variant in 2023 if the gang maintains its current operational strategies.

- The symbiotic relationship between ransomware groups and IABs will further develop and the provision of access likely will remain lucrative. We almost certainly will see the emergence of new IABs in 2023 as the bulk sale of access credentials remains a popular underground offering.

- QBot malware instances are highly unlikely to decline in 2023 and will remain a key indicator and/or warning for ransomware-related activity.

- Malware log services and post-exploitation frameworks likely will enable less sophisticated threat actors entry into cybercrime and additional illicit activity to be carried out.

- The number of new vulnerabilities being reported steadily increased over the past few years. Critical vulnerabilities continue to introduce significant risk and are a cause for concern for organizations committed to protecting their networks and data.

Russian war against Ukraine

On Feb. 24, 2022, Russian armed forces invaded Ukraine en masse in a major escalation of the conflict that started in 2014. This intensification had a significant impact on underground cybercriminal activity as many threat actors have ties to Russia. The Russian government and state-controlled media immediately sought to foment anti-Ukrainian and anti-Western sentiment among the Russian populace following the invasion. This rhetoric emboldened Russian threat actors and possible state-backed threat groups to intensify targeted cyberattacks on entities based in Ukraine and allied nations. This most notably came in the form of hacktivism. Secondary effects of the war, such as its impact on the world economy and Europe's energy security, continue to shape the cybercrime landscape. It almost is certain the conflict will continue in 2023 and will remain a major influence on the cyber underground.

Hacktivism:

A surge in hacktivism, both in support of and opposing Russia, has been the most significant underground response to Russia's war in Ukraine. Several pro-Russian civilian-led groups organized via Telegram launched hacktivist campaigns against private and public sector entities based in Ukraine and allied nations immediately prior to and following the invasion. Most of the hacktivist activity appeared to come in the form of distributed denial-of-service (DDoS) attacks. Early DDoS instances focused primarily on Ukrainian government services and organizations linked to Ukraine's critical national infrastructure. Much of the hacktivism seen since February 2022 followed a rotational basis, targeting countries based on real-time events in the war. For example, over the course of the year, we reported on how hacktivist groups targeted countries immediately following announcements that they intended to send aid to Ukraine or for imposing sanctions on Russian assets. Nevertheless, DDoS activity diminished in the final two months of 2022 and this likely will remain the case into 2023. However, any further escalation of the war highly likely would engender a significant increase in pro-Russian hacktivist activity since hacktivist groups remain highly reactive to current affairs.

Russian war against Ukraine

Ransomware

In more recent months, hacktivist groups that primarily focused on DDoS attacks also sought to introduce ransomware into their arsenals. As of November 2022, the **KillNet**, **PHANTOM DEV** and **Red Hackers Alliance Russia** hacktivist groups developed or obtained ransomware strains with the possible intent of using them against targets based in Ukraine and its allies. These groups have yet to employ ransomware in their operations, but it is possible the decrease in DDoS activity in late 2022 is preemptive of a change in tactics as hacktivists seek to leverage ransomware as a more impactful and potentially financially beneficial method of targeting their perceived enemies.

Conscription avoidance

On Sept. 21, 2022, Russia declared its intent to mobilize military reservists following strategic setbacks in Ukraine. The resulting conscription reportedly involved reservists with little military experience and conscripts outside the usual age range for service in armed conflict. The draft proved unpopular in Russia and protests took place across the country. The debate also took place on underground cybercrime forums and the mobilization gave rise to threat actors offering a variety of services to avoid conscription. Offers included forged documents for proof of disability, requirement for urgent medical treatment and HIV positive status, as well as military IDs with records claiming the bearer was not fit for military service. Due to the high number of Russia-based actors on cybercrime forums, it is likely Russia's war in Ukraine and how to avoid the economic and social impact of the conflict will remain an important topic of discussion going into 2023.

Russian war against Ukraine

Russian government support of cyberattacks

Pro-Russian hacktivists act with impunity and target entities that often align with the Kremlin's strategic aims in the war against Ukraine. It is possible more advanced groups such as **KillNet** and **XakNet** were influenced by the Russian state due to their highly targeted approach against specific government infrastructure. However, it remains unlikely pro-Russian hacktivist groups were directly tasked and funded by the Russian government. Should the Russian government's strategic aims change in 2023, pro-Russian hacktivist groups likely will attempt to align themselves with their government's objectives.

Assessment

Pro-Russian hacktivist activity became more sporadic in the final few months of 2022. Groups have shown a possible trend of diversifying their capabilities to include targeted attacks leveraging malware. In 2023, pro-Russian hacktivist groups likely will seek to leverage ransomware they obtained or developed in recent months. The use of ransomware in operations would be much more impactful than solely relying upon DDoS attacks that had limited impact or only resulted in short outages in many cases. Some hacktivist groups also sought to move into financially motivated cybercrime. This included **KillNet's** attempt to build an underground forum to discuss wider hacking and financial fraud topics. Additionally, hacktivist groups are home to thousands of individuals interested in learning about and engaging in cybercrime, and interest in Russia's war in Ukraine as well as the novelty of DDoS attacks could wane. As a result, it is highly likely some groups will pivot to financially motivated cybercrime.

Ransomware

We have covered ransomware as a key threat in our quarterly and yearly Threat Reports for two years straight at the time of this report. 2022 brought with it the rise and fall of notable ransomware variants and the evolution and development of their operational strategies, as we predicted in previous reporting. Data Intel 471 collected on the number of ransomware incidents from 2021 to 2022 might show a slight decrease, however, the threat ransomware presents remains the same.

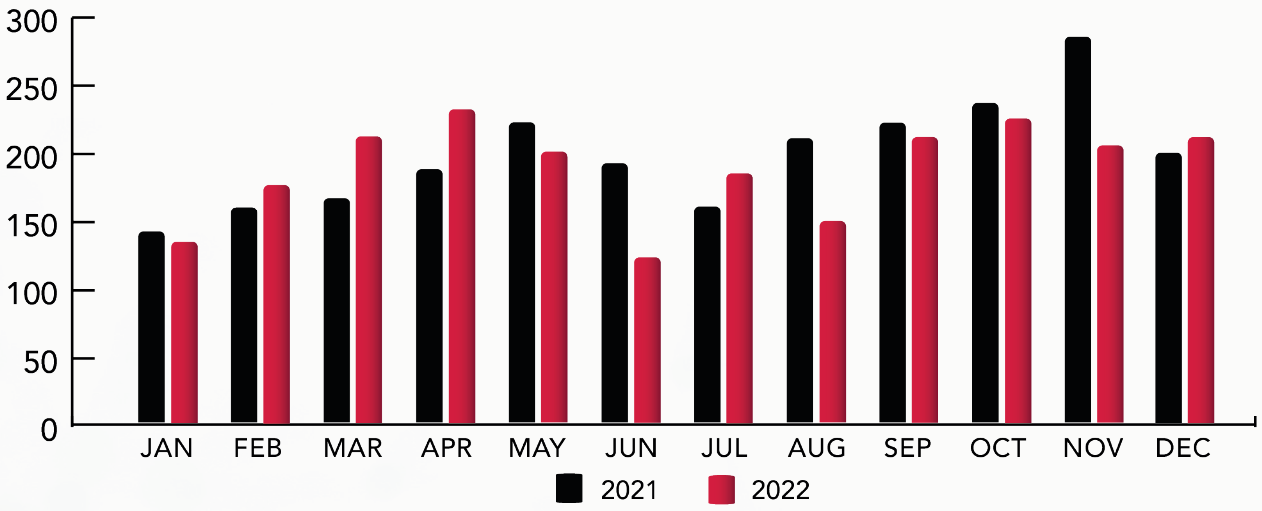


Figure 2: This graph compares the number of ransomware-related breach events Intel 471 observed in 2021 and 2022.

Statistics leveraged in this section were compiled using raw observables primarily reported in Intel 471 Breach Alerts and Spot Reports. The reported breach claims were not evaluated fully nor confirmed. Additionally, observations from this section should be seen as an overview of activity highlighted across individual breach events that were correlated to a specific ransomware strain. They are not categorized at the service operator or affiliate level, which would be difficult to ascertain based on information available in breach notifications.

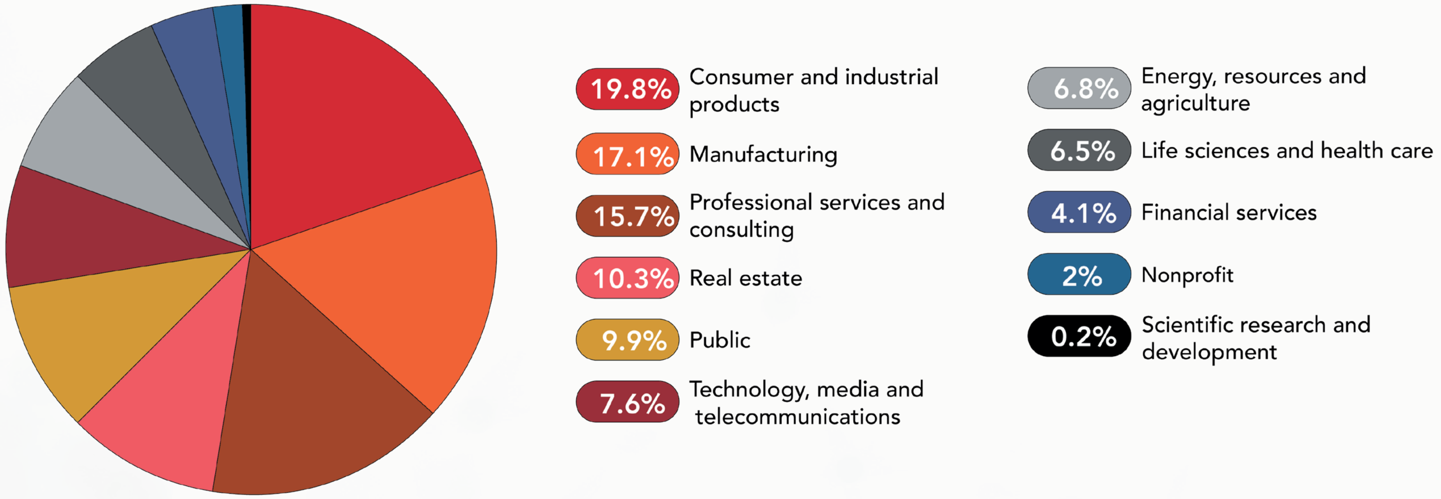
TLP:CLEAR

Ransomware

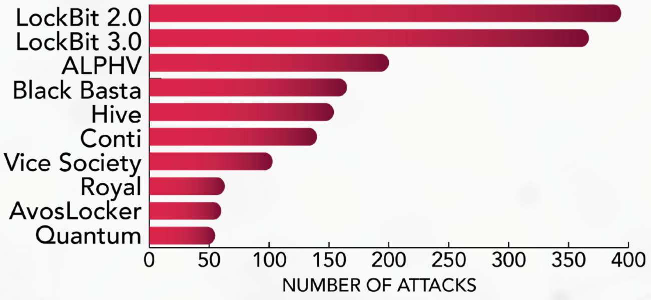
TOP 10 COUNTRIES MOST IMPACTED BY RANSOMWARE

US	UK	GERMANY	CANADA	ITALY	FRANCE	SPAIN	AUSTRALIA	BRAZIL	SWITZERLAND
39%	6%	6%	5%	4%	4%	3%	2%	2%	2%

SECTORS IMPACTED BY RANSOMWARE



MOST ACTIVE RANSOMWARE VARIANTS



RANSOMWARE ACTIVITY BY MONTH

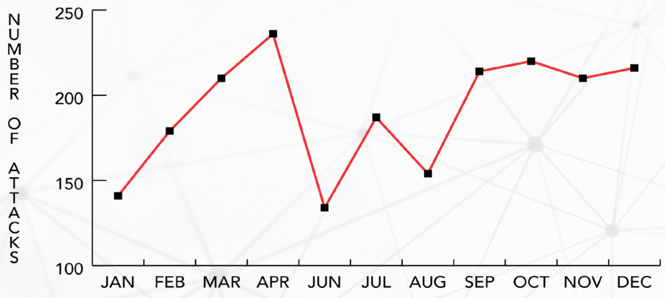


Figure 3: These graphs depict the breakdown of ransomware-related breach events we observed in 2022.

Ransomware

Top ransomware

LockBit

2022 started with the continued prominence of LockBit 2.0 maintaining its status as the most impactful ransomware variant from January through June. The actor **LockBitSupp** then announced the release of LockBit version 3.0, which included an updated data leak blog, a bug-bounty program and new functionality in the ransomware. From July onward, LockBit 3.0 held steady as the most impactful variant for the rest of the year. LockBit's success is not based on a single factor, but rather several decisions and strategies that allowed the group to remain ahead of competitors and elusive to victims. This included a strong focus on OPSEC, continuous development both technically and with regard to extortion methods and image, and effective extortion and negotiation techniques.

LockBit 2.0 was the most impactful ransomware variant of 2022 with 394 breaches, and LockBit 3.0 landed just behind at 367. The top three countries most impacted by LockBit 2.0 in descending order were the U.S., Italy and Germany, and for LockBit 3.0 were the U.S., France and Canada. The top three sectors most impacted by LockBit 2.0 in descending order were consumer and industrial products, professional services and consulting, and real estate, and for LockBit 3.0 were professional services and consulting, manufacturing, and consumer and industrial products.

Ransomware

ALPHV

ALPHV first was observed in December 2021 and several former DarkSide and REvil ransomware affiliates allegedly joined the ransomware-as-a-service (RaaS), likely contributing to the program's numerous impactful attacks. The ALPHV aka ALPHV-ng, BlackCat ransomware service held a place in the top four most impactful RaaS groups throughout each quarter of 2022.

ALPHV was the second most impactful ransomware variant of 2022 when considering the two LockBit versions as one strain and amounted to 199 total breach events for the year. The top three countries most impacted by ALPHV in descending order were the U.S., Germany and Canada. The top three sectors most impacted by ALPHV in descending order were professional services and consulting, consumer and industrial products, and manufacturing.

Ransomware

BlackBasta

The Black Basta ransomware variant first was spotted in April 2022 but likely was active as early as mid-February 2022. We observed several similarities between the Black Basta and Conti ransomware groups’ data leak blogs, payment sites, recovery portals and victim negotiation method, which led us to suspect a possible association between the two. The Black Basta RaaS quickly gained notoriety for high-profile attacks and was the third most impactful ransomware in the second quarter of 2022 and the second most impactful in the third quarter. Factors likely contributing to Black Basta’s success included practicing a selective recruitment strategy, sourcing capabilities from the underground, leveraging alleged insiders at strategic organizations and seeking to exploit vulnerabilities in victim networks.

Black Basta was the third most impactful ransomware variant of 2022 when considering the two LockBit versions as one strain and amounted to 165 total breach events for the year. The top three countries most impacted by Black Basta in descending order were the U.S., Germany and Canada. The top three sectors most impacted by Black Basta in descending order were consumer and industrial products, manufacturing and real estate.

Ransomware

New, emerging ransomware

BianLian

The BianLian RaaS reportedly was discovered in December 2021 and the service's name-and-shame blog first was observed July 21, 2022. The name BianLian likely was inspired by the ancient Chinese dramatic art Bian Lian, also known as "two-faced" or "face-changing." This inspiration and certain observed public discussions suggested the group could be of Chinese origin, however, this was not confirmed at the time of this report. The BianLian group appeared to cooperate with several well-known Russian access brokers, including **Etna**, **Glitter** and **Blanc***, indicating a possible strong link to the Russian underground. Such associations only further obscure the group's origin.

During the six months after the launch of the name-and-shame blog in July 2022, BianLian held a spot in the top 10 most impactful ransomware services for each month except September. BianLian was the second most impactful RaaS in August and the ninth most impactful ransomware variant of 2022 when considering the two LockBit versions as one strain. BianLian amounted to 55 total breach events for the year. The top three countries most impacted by BianLian in descending order were the U.S., U.K. and Canada. The top three sectors most impacted by BianLian in descending order were manufacturing, professional services and consulting, and real estate.

Ransomware

Royal

The Royal aka Roy, Zeon ransomware first appeared in January 2022 and we assessed the group likely originated from a Conti group hacking team who used the **Team One** aka **Team1** handle. Royal does not operate as a RaaS affiliate program and seemed to include only vetted former Conti members. The Royal group members initially used other ransomware strains for attacks until they developed their own strain dubbed Royal and started to use it in September 2022. By November, Royal tied with LockBit 3.0 as the most impactful ransomware strain that month.

Royal was the seventh most impactful ransomware variant of 2022 when considering the two LockBit versions as one strain and amounted to 63 total breach events for the year. The top three countries most impacted by Royal in descending order were the U.S., Canada and Germany. The top three sectors most impacted by Royal in descending order were consumer and industrial products, professional services and consulting, and manufacturing.

Ransomware

Evolution, peristance of ransomware

When a type of malware or service stays as popular as ransomware has over the past two years, there are bound to be evolutions and changes to TTPs to maintain status as a reputable, current and effective offering. We observed these changes in relation to ransomware in previous years when threat actors evolved from encryption-only attacks to encryption and extortion methods as a way of increasing the likelihood of a ransom payment. Alongside these changes, there also are tried-and-true methods threat actors maintain. Throughout 2022, we continued to see both adaptations and modifications to ransomware operations as well as the persistence of existing and effective tactics.

Cooperation with initial access brokers

The year of 2022 saw the increase of IABs, which is a trend itself that will be discussed in detail later in this report. Ransomware operators and affiliates likely took advantage of IABs by buying and leveraging access they offered in ransomware attacks. Purchasing access from IABs likely significantly reduced the amount of time it took ransomware operators to conduct an attack by enabling reconnaissance of systems and the identification of key data earlier and with greater ease. We identified at least 57 instances in 2022 where a victim organization was impacted by both an IAB and a ransomware incident. These observations should be understood as two separate instances about impacting the same victim organization. They are interpreted as a potential link but not a proven one at the time of this report.

For example, in November 2022, the operator or operators of the CLOP RaaS affiliate program claimed to compromise a U.S.-based full-stack development software provider that we previously reported the actors **Triglav** and **Tiede*** offered access to. The same month, we observed the operator or operators of the Hive RaaS claim to compromise the U.S.-based health care services provider that we previously reported the actor **Snowdon*** offered to sell compromised network access credentials to. Additionally, thorough analysis of access offers from the prolific IAB **Etna** revealed the actor likely provided access to the Conti, Hive, LockBit 2.0, LV, PYSA, RansomEXX and ViceSociety ransomware groups.

Operational security consideration

In several previous reports, we assessed multiple times that the illicit underground marketplace operates as a legal business ecosystem would. Likewise, we continue to observe successful and prominent ransomware groups consider, develop and encourage a variety of OPSEC measures to maintain business continuity.

Part of the LockBit group's dominance in the ransomware arena can be attributed to its awareness of OPSEC. The release of LockBit 3.0 in June 2022 featured a range of updates likely aimed at improving the group's internal security. This included upfront deposits from all new affiliates – likely to prevent competitors, cyber threat intelligence (CTI) researchers, law enforcement agents and journalists from infiltrating the group and leaking sensitive information – and a bug-bounty program that promised payouts of up to US $1 million for the discovery of vulnerabilities in the group's malware, victim shaming sites, Tor network and messaging service.

Ransomware

Connections, associations, rebrands

With the rise and fall of ransomware variants over the years, we continue to observe the complexity and interconnected nature of the ransomware operator, affiliate and variant environment. As we predicted last year, our understanding of the relationships between groups of individuals, partnerships or individual actors behind each ransomware service continues to build as we see additional changes in the management of existing programs and development or rebranding of "new" services.

Our view into the underground marketplace provides the ability to observe the interconnectedness of different ransomware groups, variants and affiliates over time. Although not always verified or fully corroborated at the time of this report, we have assessed the likelihood of several connections, associations and spinoffs. Another possible evolution and/or rebranding of a ransomware group can be seen with Ryuk, Conti and Black Basta. The Conti and Ryuk ransomware strains generally were attributed to the same hacking group and Ryuk likely was a predecessor to the Conti strain. One of our assessments was that Ryuk ransomware operators initially joined the Conti team as a stand-alone group to use the TrickBot trojan to distribute Ryuk ransomware. The two groups apparently merged at some point. We later reported on the possibility that the Black Basta group might be affiliated with the Conti ransomware gang. The attribution was based on some visual and structural similarities with the victim shaming blogs and recovery portals, and a similar way of communicating with victims. However, Conti group members publicly deny any connection with Black Basta.

Ransomware

Assessment

When it comes to the top ransomware groups, we assess LockBit 3.0 likely will preserve its prominence well into 2023 as long as the group maintains its current operational strategies. Black Basta ransomware appears to be the leading new variant of 2022 and while it may be much less impactful than LockBit, we likely still will see victims impacted by it in 2023. We also likely will see a continued emphasis on OPSEC within ransomware groups seeking to increase resilience and maintain successful business operations.

Additionally, initial access advertisements likely will continue to be increasingly common on underground forums and ransomware operators could look to recruit prominent and trustworthy actors to form partnerships with. At the same time, it is likely network access vendors will start to recognize they can save time and effort by making offers directly to highly active ransomware affiliate programs. Lastly, with the amount of new and rebranded ransomware strains that hit the underground market in 2022, it remains highly likely threat actors will persist in redesigning existing platforms, developing new and rebranded data leak blogs and ransomware variants, or joining multiple affiliate programs during the next year.

Initial access brokers

Intel 471 observed more than 3,400 listings of multiple access types from more than 190 IABs across the underground in 2022. IABs present a threat to every sector and industry, however, we observed the public sector was the most impacted when it came to the number of IAB offers. The most-impacted industries in 2022 were education, information technology (IT) consulting, health care providers and services, telecommunications, and banking and securities. The countries most impacted were the U.S., Germany, France, Brazil and the U.K.

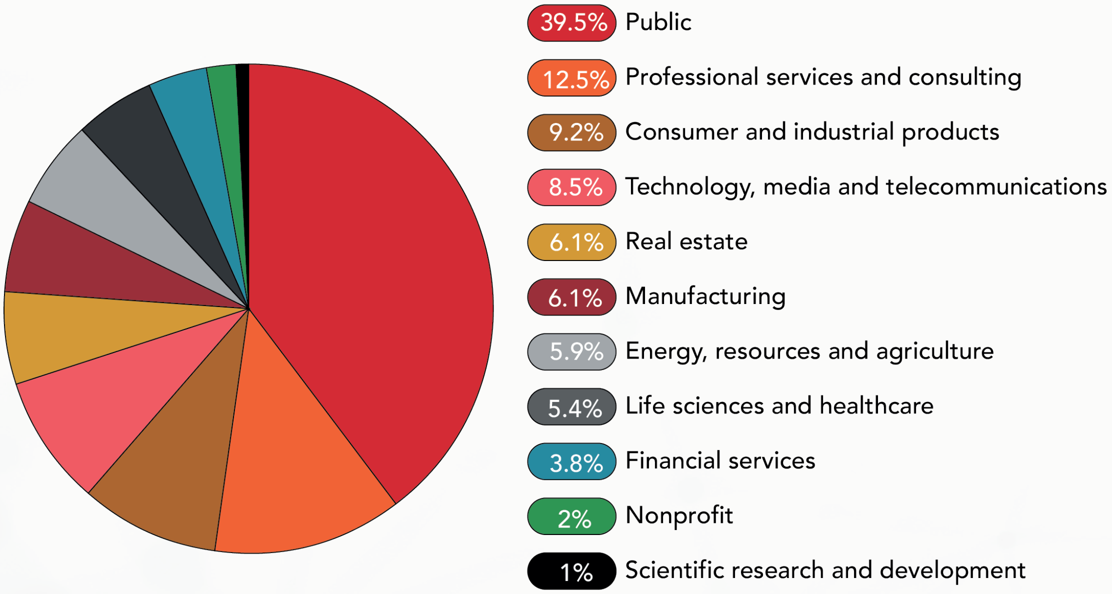


Figure 4: This pie chart depicts the sectors most impacted by IABs in 2022.

Inevitably, these statistics only paint a partial picture of underground IAB activity across 2022. IABs often do not confirm the validity of accesses and only reveal victims in private conversations. IABs usually post about having a large batch of access for sale and victim details ordinarily are not available until a potential buyer directly contacts the IAB. It also is important to note that the data and statistics in this section were compiled from Intel 471 Information Reports (IRs) and Breach Alerts published in our Titan platform from Jan. 1, 2022, to Dec. 31, 2022.

Initial access brokers

Top initial access brokers

The data we collected from IRs and Breach Alerts allowed us to determine the top two access brokers we observed in 2022 were **Cairngorm** and **Etna*.**

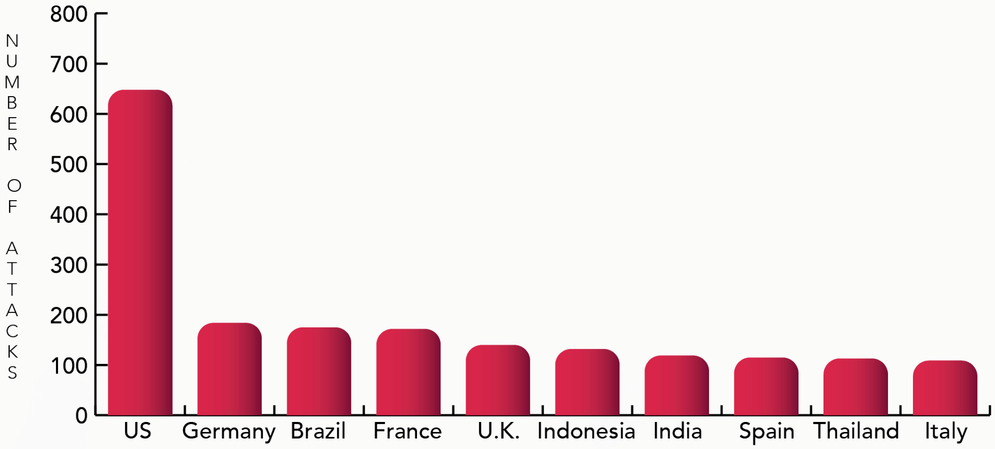


Figure 5: This chart shows the countries most impacted by IABs in 2022.

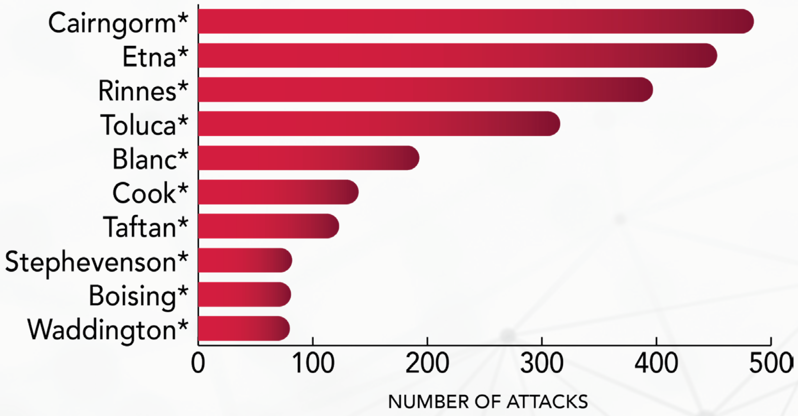


Figure 6: This chart depicts the top 10 IABs Intel 471 observed in 2022.

Initial access brokers

Actor Cairngorm

The actor **Cairngorm** sold access to at least 485 unique victims in 2022, making the actor the most impactful IAB of the year. The actor has been active on forums since 2010 and took on a new handle in May 2022. The actor regularly advertised access to organizations via compromised Citrix, Microsoft Remote Desktop Web (RDWeb) and Pulse Secure virtual private network (VPN) credentials on an underground forum. In 2022, **Cairngorm's** advertised access most impacted the U.S., France and the U.K. The actor primarily targeted educational institutions, which made up nearly half of **Cairngorm's** offers last year.

Actor Etna

The actor **Etna** was the second most prominent IAB in the first, second and third quarters of 2022. The actor sold access to at least 450 unique victims in 2022, making **Etna** the second most impactful IAB of the year. The actor has been selling access since June 2020 and compromised organizations worldwide affecting numerous industries. The actor appeared to focus on compromised Citrix, VMware Horizon and other VPNs. The countries most impacted by access **Etna** advertised included the U.S., Brazil and France. Similar to **Cairngorm**, **Etna** primarily targeted educational institutions, which also made up more than half of the actor's offers last year.

New, emerging initial access

The actors **Cairngorm** and **Etna** are well-established and reputable IABs in the underground, but 2022 also saw the rise of other IABs. The actor **Rinnes*** first was observed in the underground in early 2022 and now ranks third in the list of top IABs. Additionally, despite being first observed before 2022, the actors **Toluca*** and **Blanc** quickly rose from relative obscurity early in 2022 to ranked as the fourth and fifth most impactful IABs, respectively.

Initial access brokers

Actor Rinnes

The actor **Rinnes** was first observed in the underground in early 2022. The actor now ranks third in the list of top IABs in 2022 and was the most prominent IAB in the fourth quarter of the year.

Actor Toluca

The actor **Toluca** was the most active IAB of the third quarter of 2022 and one of the top most active IABs in the second quarter. While the actor first was observed in the underground in 2021, **Toluca** was inactive for almost a year before selling at least 315 unique accesses in the summer of 2022. The actor offered access to Citrix, FortiClient VPN, Global Protect, Pulse Secure and RDWeb login credentials to networks. The countries **Toluca** most impacted were Thailand, France and Indonesia. The industry **Toluca** impacted most was education, but to a lesser extent than the other top IABs of the year. The actor also targeted national government organizations and the IT consulting industry

Actor Blanc

The actor **Blanc** was one of the top 10 most active IABs in the second, third and fourth quarters of 2022, and sold access to at least 190 unique victims in 2022 to be ranked fifth for the year. The actor has been active since June 2021, but significantly expanded **Blanc's** presence on underground forums in March 2022 and quickly rose to become one of the most active IABs of the year. The range of victims **Blanc** offered access to is wider than typically observed from other IABs, suggesting the actor is highly opportunistic with little restriction regarding victim entities. The actor sold compromised Cisco AnyConnect, Citrix, RDP, RDWeb and VPN login credentials to organizations worldwide. The countries most impacted by access **Blanc** offered were the U.S., France and Turkey. Similar to the other top IABs, the most targeted industry was education but **Blanc** also targeted the IT consulting and power and utilities industries.

Initial access brokers

Actor Blanc

The actor **Blanc** was one of the top 10 most active IABs in the second, third and fourth quarters of 2022, and sold access to at least 190 unique victims in 2022 to be ranked fifth for the year. The actor has been active since June 2021, but significantly expanded **Blanc's** presence on underground forums in March 2022 and quickly rose to become one of the most active IABs of the year. The range of victims **Blanc** offered access to is wider than typically observed from other IABs, suggesting the actor is highly opportunistic with little restriction regarding victim entities. The actor sold compromised Cisco AnyConnect, Citrix, RDP, RDWeb and VPN login credentials to organizations worldwide. The countries most impacted by access **Blanc** offered were the U.S., France and Turkey. Similar to the other top IABs, the most targeted industry was education but **Blanc** also targeted the IT consulting and power and utilities industries.

Assessment

All the aforementioned IABs claimed to source access from malware logs. The actor **Blanc** previously was observed purchasing Raccoon Stealer malware logs from the actor using the **Ruiz*** handle. The actor **Etna** launched a Telegram-based store for malware logs in June 2022. Additionally, **Etna** previously sought to purchase private information-stealer malware with features similar to the Raccoon and RedLine stealers and purchased malware logs directly from a reputable seller of AZORult and RedBear logs, the actor using the **Rosa*** handle. Lastly, **Toluca** and **Cairngorm** also claimed to source access credentials from undisclosed malware logs.

Initial access brokers

The most prolific IABs of 2022 have similar TTPs and could source their access from the same location – whether a seller of logs, an underground shop or cloud storage. Intel 471 observed more than 500 occasions of IABs selling access to the same company in 2022. This is yet another piece of evidence that suggests identical sourcing methods. However, it also could indicate associates and/or alternative personas, or a victim company possibly had more than one account exposed. Overall, these observations highlight the importance of identifying and disrupting actors who operate underground shops for malware logs.

Looking ahead to 2023, it is highly likely bulk sales of access credentials will continue to increase and several new IABs almost certainly will emerge. Access likely will continue to be sourced from information-stealing malware, malware logs purchased from Telegram-based stores or other underground shops, or collected from free public cloud storage. Consequently, there likely will be increased potential for duplicate listings from multiple IABs. Nevertheless, these accesses almost certainly will remain lucrative, especially as instances of cooperation between RaaS operators and IABs persist.

Malware

Malware is a constant in the cybercriminal marketplace – year after year, a variety of malware is perpetually developed, created, bought, sold, leveraged and maintained. The vast array of malware offers in the underground present threat actors with significant choice when it comes to engaging in cybercrime. Throughout 2022, the notable activity we observed related to malware included QBot, SmokeLoader, malware log services and post-exploitation frameworks.

QBot

Last year, Microsoft changed the default behavior of Office applications to block macros in files from the internet. We expected to see a change from actors via different adaptations to overcome this obstacle, since the channel is a main delivery mechanism for malware through spam campaigns. As expected, we promptly observed QBot operators develop convoluted delivery chains that leverage multiple file formats in pursuit of leaving macros behind. For example, we published a report on actors leveraging CVE-2022-30190 aka the Follina vulnerability and released Malware Campaign Reports on optical disc image file (ISO)-based infection chains.

Assessment

QBot is one of the most significant threats emanating from the underground malware marketplace, considering several reports connect it with the exfiltration of information ending in massive deployments of ransomware. Actors operating QBot finished the year running aggressive spam campaigns for at least three botnets – azd, BB and obama – which showcases how they aimed to grow the botnets before the holiday break. As a result, we assess QBot likely will maintain its presence within the threat landscape well into 2023.

SmokeLoader

In May 2022, the long-standing actor **SmokeLdr**, whom we track as an author of the multifunctional SmokeLoader malware, announced a major update to the product. This included improvements to the malware engine, geolocation IP (GeoIP) database and communication between the control panel and database. Upgrades to the information-stealing module also improved the way the malware targets web browsers and the form-grabbing module received support for the Opera 64-bit version web browser. We soon began to see clients upgrading to the latest version, even though the previous release from 2020 still was leveraged widely by users reluctant to change or pay for a new tool set. Last year, we closely tracked four to eight botnets that rely on SmokeLoader to push additional malware payloads. We believe some of these botnets directly support pay-per-install services that bring to our collection a wealth of different malware samples, providing us with valuable insight into the malware underworld landscape.

Assessment

We assess the use of SmokeLoader is highly unlikely to decline in 2023 considering its long-standing tenure within the underground marketplace. Moreover, malware loaders continue to act as an enabler of additional cybercrime as they provide a wide range of threat actors the ability to gain initial access and deploy an equally large range of different malware samples. Follow-up payloads may leave no trace after execution, resulting in the need for severe cleaning measures should SmokeLoader, or any other loader such as Amadey or PrivateLoader, be detected running within the local network.

Malware

Malware log services

The perpetual collection of RedLine and Vidar samples from botnets we suspect fuel malware log services is among our most consistent observations last year. The Raccoon Stealer version 2 follows closely as another information stealer of choice in less quantity but not less important. Some of the more prolific botnets focused on pushing information-stealing malware include the aforementioned SmokeLoader as well as Amadey and PrivateLoader. Information-stealer logs is a niche market easily leveraged by actors focused on ransomware operations or selling access.

Assessment

Threat actors no longer need to develop elaborate plans to illicitly access internal networks or leverage more vetted marketplaces offering unknown zero-day vulnerabilities to obtain the proverbial "keys to the kingdom." Instead, they can obtain or purchase a set of working credentials through these services. Malware log services therefore act as a key enabler of at least two of the prominent threats discussed in this report – ransomware and IABs. As a result, we assess the popularity of both ransomware and access brokers will greatly assist in keeping malware log services in business well into 2023 and possibly beyond.

Malware

Post-exploitation frameworks

The threat landscape malware poses has shifted steadily from mainly fraud-based schemes perpetrated by banking trojan operators to massive ransomware deployments carried out by ransomware operators and/or affiliates. Several factors assisted this shift, including the use of post-exploitation frameworks. These frameworks are ready-to-use tools that enable actors to maintain illicit access to a system and provide capabilities for lateral movement and colonization of the internal network.

The most common post-exploitation framework tools threat actors currently abuse for malicious purposes based on our collection are Brute Ratel, Cobalt Strike, Metasploit and Sliver. Throughout 2022, we observed several instances of bots repeatedly getting commands to download and execute payloads of these frameworks. Operators of the Bumblebee loader were observed leveraging as many as three of them simultaneously, whereas most initial access bots would fetch just one follow-up payload. This specific Bumblebee operator used Cobalt Strike, Metasploit and Sliver at the same time in an increased effort to monetize their foothold.

Assessment

Threat actors have to perform lateral movement across a network from an initial infection point to critical machines of the infrastructure to take over an internal network, exfiltrate data and deploy ransomware to encrypt internal assets. However, they no longer need to come up with custom payloads or write any code to carry out such endeavors, since they can leverage existing frameworks for adversary emulation. These individuals now have access to powerful, ready-to-use tools that require less effort and skill to use than it would have taken to create the tools themselves. This significantly lowers the barrier of entry into this arena of cybercrime. We could see the use of post-exploitation frameworks persist as a common denominator of network and data breaches, as well as ransomware events, in 2023.

Vulnerabilties

The number of new vulnerabilities being reported has increased steadily over the past few years. Critical vulnerabilities continue to introduce significant risk and are a cause for concern for organizations committed to protecting their networks and data. The National Vulnerability Database (NVD) reported there were about 19,584 vulnerabilities disclosed in 2021 and about 19,856 in 2022. The sheer volume of reported vulnerabilities continues to make tracking, prioritization and patching efforts increasingly difficult. Zero-day and one-day vulnerabilities play an important role in successful network penetration, and once threat actors gain access to a network, lateral movement becomes synonymous.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) indicated there were about 172 vulnerabilities known to be exploited in the wild with a designator of common vulnerabilities and exploits CVE-2021 and 93 with a designator of CVE-2022. This may seem like a positive on the surface, but the number of vulnerabilities threat actors used in those years increased significantly. The number of vulnerabilities added to CISA's Known Exploited Vulnerabilities Catalog in 2021 was 311 and increased significantly to 557 in 2022.

Through our monitoring of the cybercrime underground, we also observed a notable increase in vulnerabilities, which were more complex and severe. We also saw a variation in the distribution of vulnerabilities by severity ranking over the last two years. While there was a significant increase in vulnerabilities during the first half of 2021, there appeared to be a minor decrease in the second half. Vulnerabilities reported in 2022 were fairly steady throughout the year, with a slight increase over the last three months.

Vulnerabilties

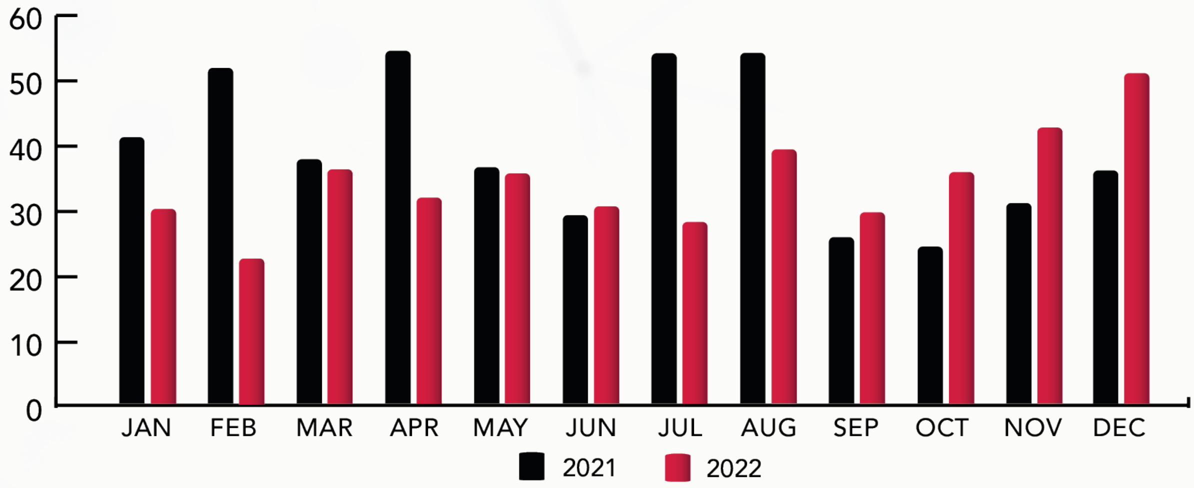


Figure 7: This graph displays a comparison of vulnerabilities Intel 471 reported in 2021 and 2022.

We reported 408 vulnerabilities in 2022, 31% of which were low risk. Twenty-five percent of CVEs were high risk, highlighting a significant threat to businesses if unpatched. We also reported vulnerabilities major hardware and software vendors disclosed in 2022 and ranked about 102 as high-risk issues.

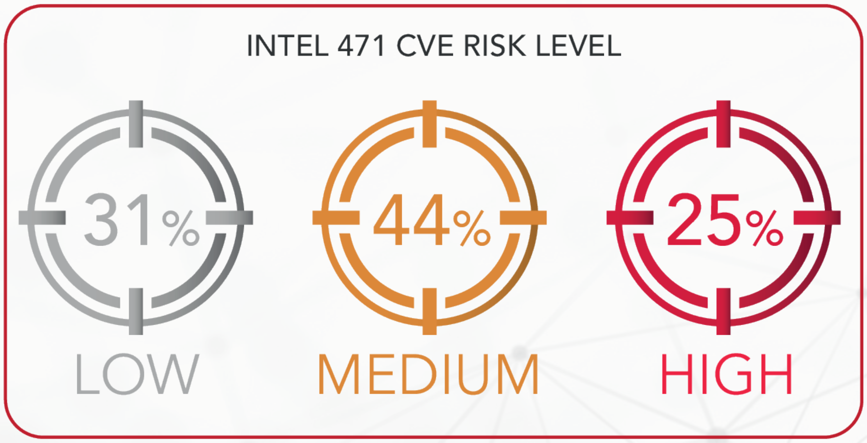


Figure 8: This image displays the risk level of CVEs Intel 471's Vulnerability Intelligence team reported and assessed.

Vulnerabilties

Of the 408 vulnerabilities we reported in 2022, 20% were productized, 55% were weaponized and 25% had code available. Productized indicates a vulnerability is available for use in mass production by unsophisticated actors, such as incorporating exploits into Armitage, Cobalt Strike, Core Impact, Metasploit, Nexpose and more. Weaponized indicates a vulnerability was integrated into malicious code for use by sophisticated actors, including exploit kits and malicious advertising (malvertising). Code available indicates proof-of-concept (PoC) code was published and/or shared in the underground.

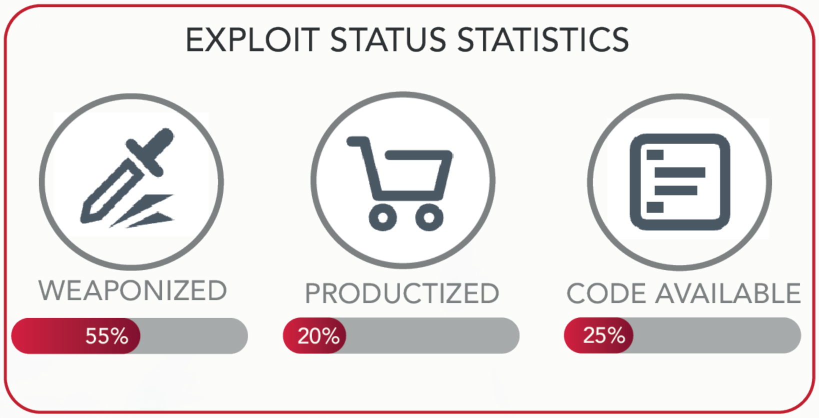


Figure 9: This image displays the percentage of vulnerabilities Intel 471 reported as weaponized, productized or had code avaliable.

Most discussed common vulnerabilities, exposures of 2022

Of the 102 high-risk issues reported, we pulled a sample of vulnerabilities for this report that posed a significant risk to organizations worldwide, including CVE-2022-41352, CVE-2022-26138, CVE-2022-29499 and CVE-2022-30525. In accordance with our critical risk score rating criteria, these vulnerabilities were weaponized, productized or used to support ransomware deployment operations.

Vulnerabilties

CVE-2022-41352

CVE-2022-41352 is an unrestricted file upload vulnerability impacting multiple versions of Zimbra Collaboration Suite (ZCS). A Metasploit module was observed in open source and subsequently shared in the underground. The vulnerability allows an unauthenticated attacker to remotely achieve arbitrary code execution by uploading a malicious file using a loophole in the file archiver utility cpio when exploited. The issue initially was reported by a user with the moniker yeak on Zimbra's official forums and has been tracked since September 2022. On Oct. 13, 2022, researchers at the Volexity security firm claimed to detect massive exploitation activity leveraging CVE-2022-41352. The attacks mostly were targeted against leading organizations affiliated with the government, IT and telecommunications sectors. The vulnerability remained unpatched for about a month, giving numerous threat actors an opportunity to exploit this issue.

CVE-2022-26138

CVE-2022-26138 is a use of hard-coded credentials vulnerability impacting multiple versions of the Atlassian Questions for Confluence application. When this application is enabled, it creates a Confluence user account named "disabledsystemuser" and the hard-coded password "disabled1system1user6708" to protect the account. Atlassian claimed Questions for Confluence had more than 8,000 installations at the time of disclosure. On July 21, 2022, exploitation of CVE-2022-26138 reportedly started after the hard-coded password was disclosed on Twitter by the user fluepke, who is a network engineer in Berlin, Germany, and maintains a GitHub repository using the same handle. Security researcher Kevin Beaumont claimed the issue was a critical zero-day vulnerability and recommended Confluence servers be placed behind a VPN or reverse proxy to add an extra layer of protection against the possibility of exploitation.

Vulnerabilties

CVE-2022-29499

CVE-2022-29499 is an improper input validation vulnerability within the service appliance component of multiple versions of Mitel MiVoice Connect. The issue allows an unauthenticated attacker to remotely execute arbitrary code on a target appliance when exploited. An attacker can exploit this vulnerability by populating the get_url parameter with a malicious URL, which would request a local file on the system. The system then would generate a second HTTP GET request by itself to a server the attacker controls. This would allow the attacker to execute any arbitrary commands stored on the attacker's server at the requested URL. A PoC was observed in open source and security researchers at CISA claimed the vulnerability was actively exploited in the wild. Additionally, open source reports claimed the vulnerability allegedly was used in suspected ransomware deployment operations.

CVE-2022-30525

CVE-2022-30525 is an operating system (OS) command injection vulnerability impacting multiple versions of Zyxel USG FLEX 100(W), USG FLEX 200, USG FLEX 500, USG FLEX 700, USG FLEX 50(W), USG20(W)-VPN, advanced threat protection (ATP) series and VPN series firmware. The issue initially was discovered by Rapid7's lead security researcher Jake Baines. The vulnerability reportedly allows an unauthenticated and remote attacker to achieve arbitrary code execution as the "nobody" user on the impacted device. A Metasploit module capable of achieving remote code execution by sending a malicious setWanPortSt command containing an mtu field with a crafted OS command to the /ztp/cgi-bin/handler page is publicly available. In September 2022, the security researcher Germán Fernández claimed to have detected mass exploitation activity leveraging CVE-2022-30525 to deploy Mirai botnet malware.

Vulnerabilties

Vulnerabilites with notable underground activity 2022

We continue to monitor underground threat actor activity related to discussions of vulnerabilities to assist in assessing risk level. This includes threat actor interest in disclosed vulnerabilities, which is determined by observations of cybercriminals sharing links to news articles, exploit codes or publicly released and free PoC code. While this can show signs of trending vulnerabilities, we also look for more substantial activity to assign a higher risk assessment, such as individual threat actors seeking to leverage certain vulnerabilities for attacks. Below is a roundup of vulnerabilities allegedly exploited last year that garnered a high volume of underground activity.

CVE-2022-30190 aka Follina

In May 2022, we reported CVE-2022-30190 aka Follina as an arbitrary code execution vulnerability impacting multiple products and versions of Microsoft Windows. On May 27, 2022, the security research team nao_sec tweeted about a malicious Microsoft Word document in the wild that was uploaded from an IP address in Belarus. The security researcher Kevin Beaumont identified it as a zero-day vulnerability and dubbed it Follina. The issue was discussed widely in the underground since its discovery, including the actor **Rainier*** advertisement of a payload-embedded Word document on an underground forum in June 2022. Additionally, the actor **Helka*** sought an exploit kit for CVE-2022-30190 and the actor **Helicon*** posted a link to an exploit generator tool pertaining to Follina. We also observed the actor **Dachstein*** share a demonstration video and offer to sell an exploit builder on an underground forum for tens of thousands of US Dollars. The actor made similar claims on an underground forum using the alternate handle **Olympus*** as did the actor using the **Trivor*** handle.

Vulnerabilties

CVE-2022-26134

In June 2022, we reported CVE-2022-26134 as an object graph navigation language (OGNL) injection vulnerability impacting multiple versions of Atlassian Confluence Server and Atlassian Confluence Data Center. Several actors posted a link to an exploit for CVE-2022-26134 from open source and an undisclosed actor on the Iranian مرکز تحقیقاتی APT IRAN (Eng. APT IRAN- Research Center) Telegram channel allegedly exposed several Iran-based entities impacted by CVE-2022-26134. The actor **Meru*** advertised an exploitation toolkit that leveraged CVE-2022-26134 on an underground forum, while the actor **Cook*** sought help with CVE-2022-26134 on an underground forum. Additionally, the actor **Botev*** claimed to have leveraged CVE-2022-26134 to obtain access to systems and the actor **Cradle*** sought help with exploiting CVE-2022-26134 on the vulnerable Windows systems.

CVE-2022-41040, CVE-2022-41082 aka ProxyNotShell

In September 2022, we reported two unpatched vulnerabilities impacting Microsoft Exchange Server. The research team at the Vietnamese GTSC security firm identified the vulnerabilities and the security researcher Kevin Beaumont dubbed them ProxyNotShell. He also claimed the vulnerabilities might have existed because of an incomplete fix for ProxyShell vulnerabilities from early 2021. ProxyNotShell is a server-side request forgery (SSRF) and remote code execution (RCE) vulnerability impacting multiple versions of Microsoft Exchange Server. The vulnerabilities have been discussed widely in the underground since their disclosure. Examples include the actor **Ararat***, who advertised an exploit for Microsoft Exchange Server, and several other actors who shared information from open sources reporting on multiple forums. Additionally, the actor **Suthep*** shared a detailed write-up on and received appreciation from several actors. We also observed the actor **Revolution*** seek PoC information for ProxyNotShell vulnerabilities.

Vulnerabilties

CVE-2022-40684

In October 2022, we reported CVE-2022-40684 as an authentication bypass vulnerability impacting multiple versions of Fortinet FortiOS, FortiSwitch Manager and FortiProxy. Several threat actors were observed discussing, seeking and offering information about the exploitation of this vulnerability since its disclosure. As a result, the vulnerability was weaponized and productized in the underground. The actors **Elbrus*** and **Apo*** posted a link to a Metasploit module from open sources and several threat actors discussed exploitation of the vulnerability. The actor **Tahan*** claimed to have leveraged CVE-2022-40684 using an undisclosed method. The actor **Bia*** shared an article on how to exploit CVE-2022-40684 and received positive comments from multiple users. The actor **Koussi*** sought to collaborate with actors who could obtain access to corporate networks in Canada and the U.S. using the Fortinet vulnerability, and several actors inquired about a ready-to-use exploit that leverages CVE-2022-40684. Additionally, the actors **Meru*** and **Sabinio*** advertised an exploit for CVE-2022-40684 and expressed readiness to work through an escrow service.

Assessments, reccomendations

As underground threat actors continue to discover new and creative ways to compromise networks and systems, it is important to apply security updates to impacted systems as soon as they become available. Most of the impacted software mentioned in this section is being used by a large number of users and most is subjected to code execution issues. Additionally, these vulnerabilities can be leveraged in conjunction with other issues to increase the potential impact of exploitation, which only emphasizes the importance of patch prioritization. While patching every disclosed vulnerability may not be feasible and could involve technical complications, we recommend prioritization based on the threat intelligence provided by our Vulnerability Intelligence Dashboard in our Titan platform.

INTEL471

General Intelligence Requirement trends

With our access and purview into the cybercrime underground, we continue to grow our capability of observing a variety of developments over long periods of time. Our research and collection methods largely are driven by our GIR framework, which we use to tag and monitor our reporting output. The following section details the starkest changes in the use of certain GIRs when comparing our report production from 2021 to 2022.

Trending upward

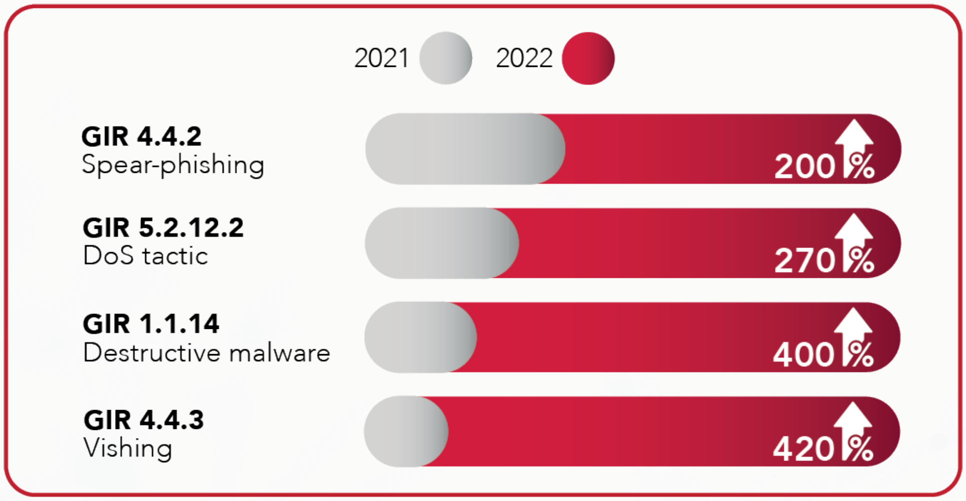


Figure 10: This image displays the GIRs with the highest percent increase in reporting from 2021 to 2022.

General Intelligence Requirement trends

Phishing: Spear-phishing – 4.4.2, vishing – 4.4.3

There was a spike in phishing in all its various guises in 2022 when compared to the previous year. We observed a steep rise in telephone-oriented attack delivery (TOAD) methods, where threat actors leveraged callback phishing services to engage victims. We noted phishing emails were tailored to the target organization to appear legitimate and include information regarding invoices, receipts or subscription confirmations. The voice phishing (vishing) attempts that follow the email lure are conducted by threat actors with professional and trustworthy voices and follow a scripted prompt that has proven to be effective against previous targets.

Assessment

Cybercrime continues to be simplified through the provision of as-a-service business models, which enable a low barrier of entry for a novice threat actor. The concepts related to phishing also are unsophisticated and cater to a large user base. The increased implementation of multi-factor authentication (MFA), which often requires a form of short message service (SMS) phishing (smishing) to circumvent such security measures, likely led to an increase in this tactic. The stark rise in spear-phishing likely is connected to a growth in business email compromise (BEC). The targeting of organizations' senior leadership often is the first step in a successful BEC campaign and likely accounts for some of the increase in numbers. Preying on the human element of the security chain remains an effective tactic for threat actors and one that increasingly is important when contending with authentication. Therefore, we likely will see this threat continue its upward trend into 2023.

General Intelligence Requirement trends

Destructive malware – 1.1.14, denial of service tactic – 5.2.12.2

The Russian invasion of Ukraine and the consequential conflict resulted in a dramatic spike in Russian-aligned hacktivism and to a lesser extent Ukraine-aligned hacktivism. We observed DoS attacks and the implementation of destructive malware were the primary vectors hacktivists leveraged to wage their war. As DDoS attacks grew in popularity and availability in the underground, the range of tools and services available expanded to meet the demand. We also observed RaaS groups build upon previous double extortion models to incorporate DDoS attacks into their arsenal as part of a "triple extortion" methodology. Similarly linked to the Russian invasion, we observed an uptick in destructive malware early in the year. This appeared in the form of wiperware, where threat actors would alter traditional ransomware builds so they would destroy all data holdings as opposed to encrypting them.

Assessment

The growing use of DDoS attacks in both hacktivism and RaaS operations attests to more sophisticated threat actors and groups incorporating this method into their arsenal. We assess DDoS attack tools are becoming more widely available due to the low barrier of entry and likely will remain an active threat into the new year. Destructive malware predominantly was active in the early months of the Ukrainian invasion and decreased as the year went on. This likely is a result of hacktivist groups professionalizing and becoming more financially motivated. There is a roughly even chance wiperware usage will begin to plateau as groups opt for lucrative ransomware attacks to monetize their activity and sustain growth.

INTEL471

General Intelligence Requirement trends

Trending downward

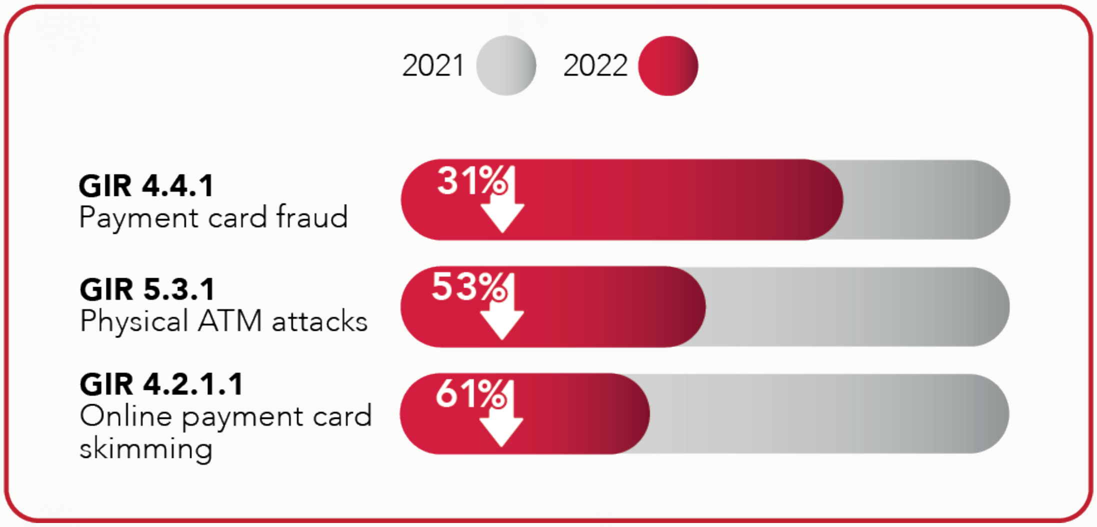


Figure 11: This figure depicts GIRs with the highest percent decrease in reporting from 2021 to 2022.

Outlook

Payment card fraud – 4.2.1, online payment skimming – 4.2.1.1, physical ATM attacks – 5.3.1

We issued 227 reports related to payment card fraud in 2021, compared to 156 in 2022. While this shows a dramatic decline, it also demonstrates that payment card fraud continues to be a key component of the underground. The carding market is far more disparate than in previous years – the era of one-stop dump shops such as Joker's Stash appears to have ended. We now tend to see more of an ebb and flow of new shops coming and going, with few able to dominate the market. We also observed a stark decline in reports on payment skimming, which possibly was connected to the overall card-related fraud reduction. Additionally, we observed a more than 50% decrease in reports on physical ATM attacks. The broader decline in ATM usage prompted by the COVID-19 pandemic possibly was related to this trend, which could have led underground actors to move away from physical ATM attacks due to a reduction in targets for physical card skimming.

Assessment

The observed fall in payment card fraud likely was driven by multiple factors. Content management systems (CMSs) have hardened over time, likely making online skimming more difficult; customers are more attuned to the perils of fraud and phishing due to repeated messaging from banks; and the introduction of regular 2FA checks undoubtedly raised the general complexity of payment card fraud. Furthermore, when comparing this form of fraud to the relative simplicity of access or data brokerage, the cost benefit is far less alluring. The decline in some card harvesting mechanisms such as online and physical skimming likely also contributed to a holistic downward trend.

Outlook

There are several possible developments that could play out in the cybercriminal underground moving forward. We assess the selection of drivers seen in the image below likely will be integral to the development of the cyber threat environment in 2023. We then made informed assumptions on the trajectory of these drivers, which led us to our outlook for the new year.

Driver	Assumption
Russia-Ukraine conflict	The conflict almost certainly will continue well into the new year as Russia seeks to compound Ukrainian energy issues during the winter months. Pro-Russian hacktivist groups likely will continue to support the state but pivot financially rewarding activity. This could lead to a rise in ransomware attacks, predominantly "big game hunting" of organizations in countries aligned to Ukraine.
Economic instability	Economic instability is forecast to last into at least the third quarter of 2023. Similar to the 2008 financial crisis, we likely will see an uptick in cybercrime as actors look to bolster legitimate earnings with illicit activity. It is possible we could see actors look to leverage the downturn by preying on the desperate with get-rich phishing schemes. Large-scale technology industry layoffs could lead to an increase in developers turning to the underground to ply their trade.
Blue team optimization	Businesses and vendors continue to implement more effective mitigation measures. Actors follow the path of least resistance, resulting in a continual decline in the carding markets and an uptick in access selling. Efforts taken in 2022 to minimize the effects of macros will continue into 2023 and suppliers of spam will seek novel methods to circumvent these measures.
Vulnerability complexity	Vulnerabilities become less frequent but more severe. Actors will begin to chain vulnerabilities to overcome increasingly robust security measures, increasing the technical skills required by these individuals. The increase in cloud infrastructure and API usage will likely result in vulnerabilities being sought in these mechanisms and they likely will be easier to identify due to these platforms being relatively new.
Increased accessibility	Many actors who provide key enabling services have adopted the as-a-service business model. This allows them to generate consistent revenue but also lowers the bar to entry for actors who possess limited skill. This trend will continue as different markets adopt similar practices. This could result in an increase of actors active in the underground and force criminal vendors to innovate to maintain market share.

Outlook

In 2023, the Russia-Ukraine conflict likely will become less of an initiator for new activity as actors who gained prominence in 2022 move toward personal financial enrichment. The decrease in global law enforcement cooperation as a result of the war likely will embolden actors to partake in ransomware activity. The coincidence with an upward trend in access brokerage realistically will see ransomware attacks outstrip figures from 2022.

It is unlikely an ailing economy alone would be a significant driver for underground activity, however, when combined with the increasing accessibility of many aspects of cybercrime, we likely will observe an uptick in novice actors seeking to bolster their finances. The increase in novice actors potentially will result in further adoption of the as-a-service model across more facets of the underground.

INTEL471

GIRs

1.1.1	Ransomware malware
1.1.4	Banking trojan malware
1.1.5	Information-stealer malware
1.1.6	Loader malware
1.1.7	Botnet malware
1.1.10	ATM malware
1.1.12	Denial of service (DoS) malware
1.1.14	Destructive Malware
1.2	Malware-as-a-service (MaaS)
1.3.2	Malvertising
2.1	Vulnerabilities
4.1.9	Business Email Compromise
4.1.10	Document fraud
4.2	Compromised data or access
4.4.2	Vishing
4.4.3	Spear Phishing
5.2.1	Initial access tactic
5.2.8	Lateral movement tactic
5.2.12	Impact tactic
5.3.1	Physical ATM attacks
5.5.3	Information or data breach
5.5.4	Blackmail
6.1	All sectors and industries
6.2	All geographic regions

INTEL471

www.intel471.com | sales@intel471.com | (800)833-1471