INTEL471

THE 471 CYBER THREAT REPORT

2023-24

FROM THE CEO's DESK

I am pleased to share the annual Intel 471 Cyber Threat Report. Our intention is to assist cybersecurity practitioners across the globe by sharing trends observed and studied by our Research and Analysis Teams. The cyber underground insights in this report will guide cyber professionals in adjusting their strategic and tactical programs, as well as their investments in these challenging economic times. This report delves into key trends both increasing and decreasing in momentum; and, how these will influence the anatomy of the cyber underground and cybercrime over the year.

Readers can expect to gain data-driven insights that will help them shape their cybersecurity policies and initiatives to better protect and defend their organizations and assets. Some key takeaways include:

- The most frequent tactics, techniques and procedures (TTPs) observed in the underground are heavily weighted in the early stages of a typical attack chain.
- Ransomware persists as one of the primary threats to organizations worldwide. We reported almost 2,000 ransomware breach events in the first half of 2023, with LockBit 3.0 remaining the most impactful with more than 500 breaches.
- The popularity of access sales endured, as we observed and reported more than 2,000 claims from access vendors offering to sell compromised credentials and/or alleged unauthorized access to networks or systems in the first half of 2023.
- The malware landscape remained an ever-changing environment, with notable activity observed regarding two long-tenured botnets — Emotet and QBot.
- Threat actors continue to exploit a wide range of vulnerabilities. We documented about 260 vulnerabilities in our reports over the first half of 2023 — 28% were rated as high risk, 42% medium and 30% low; while 14% were productized, 52% were weaponized and 18% had only proof-of-concept (PoC) code available.

This report is but one way that Intel 471 demonstrates its commitment to our customers. We enable organizations to counter the threat of cybercrime by unlocking the power of cyber threat intelligence and support all aspects of the business and across the range of maturity levels.

Jason Passwaters
CEO & Co-Founder

TABLE OF CONTENTS

EDITOR'S NOTES

**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.*

The following table defines judgment terms used throughout this report and the associated probability range for each of these terms.

PROBABILITY YARDSTICK	
Probability Range	**Judgment Terms**
Less than 5%	Remote Chance
10% - 20%	Highly Unlikely
25% - 35%	Unlikely
40% - 50%	Realistic Possibility/Probability
55% - 75%	Likely or Probably
80% - 90%	Highly Probable or Highly Likely
More than 95%	Almost Certain

TOP TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

The most frequent TTPs observed in the underground are heavily weighted in the early stages of a typical attack chain. These TTPs are generally more visible because the acquisition and development of capabilities often requires threat actors to surface on underground marketplaces and forums, which can provide indicators and warnings of future attacks if monitored. The prevalence of access-related TTPs is indicative of the growth in the access market and the importance of access credential exploitation in many phases of an attack, including initial access, lateral movement and privilege escalation.

The following graphic depicts the top MITRE ATTACK TTPs observed in the cyber underground.

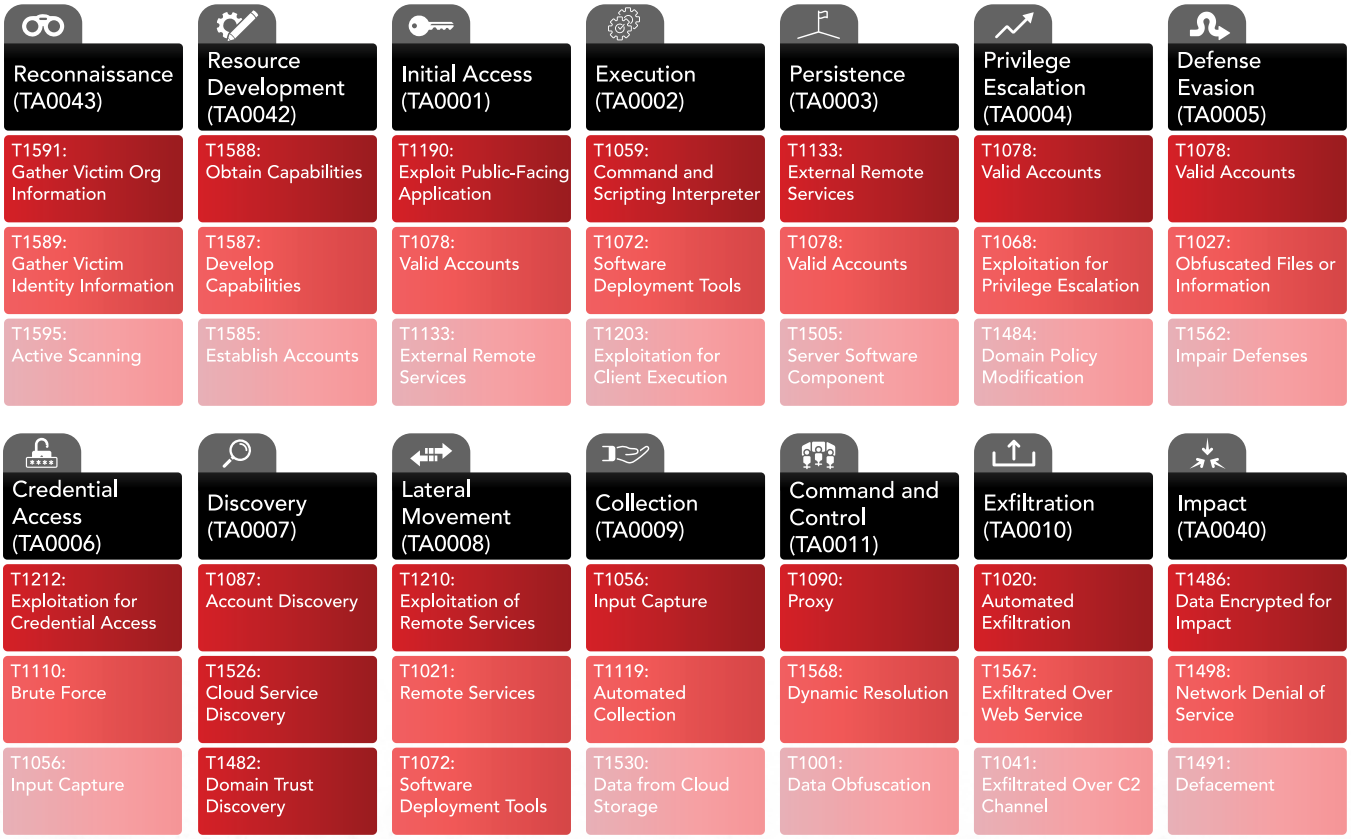


Figure 1: Top MITRE ATT&CK TTPs observed in the underground

PROMINENT CYBERCRIME TRENDS

Ransomware

We reported almost 2,000 ransomware breach events in the first half of 2023, an increase of more than 75% in comparison to the 1,102 from the first half of 2022*. The ransomware-as-a-service (RaaS) affiliate model, a business model in which affiliates pay to use the ransomware developed by its operators, continues to be popular. This is likely because this model lowers the entry barrier for attackers, by providing affordable means for affiliates who lack the ability or time to develop their own ransomware to launch an attack. The **LockBit 3.0** RaaS affiliate program continued to be the most impactful with more than 500 breaches — about 25% of the total amount. The next most-impactful ransomware in descending order were **ALPHV**, **CI0p**, **Royal** and **Play**. The U.S. was the most-impacted country with almost 46% of ransomware events, followed by the U.K. at 7% and Canada at just under 5%. The top three sectors most impacted by these offers in descending order were professional services and consulting, consumer and industrial products, and manufacturing.

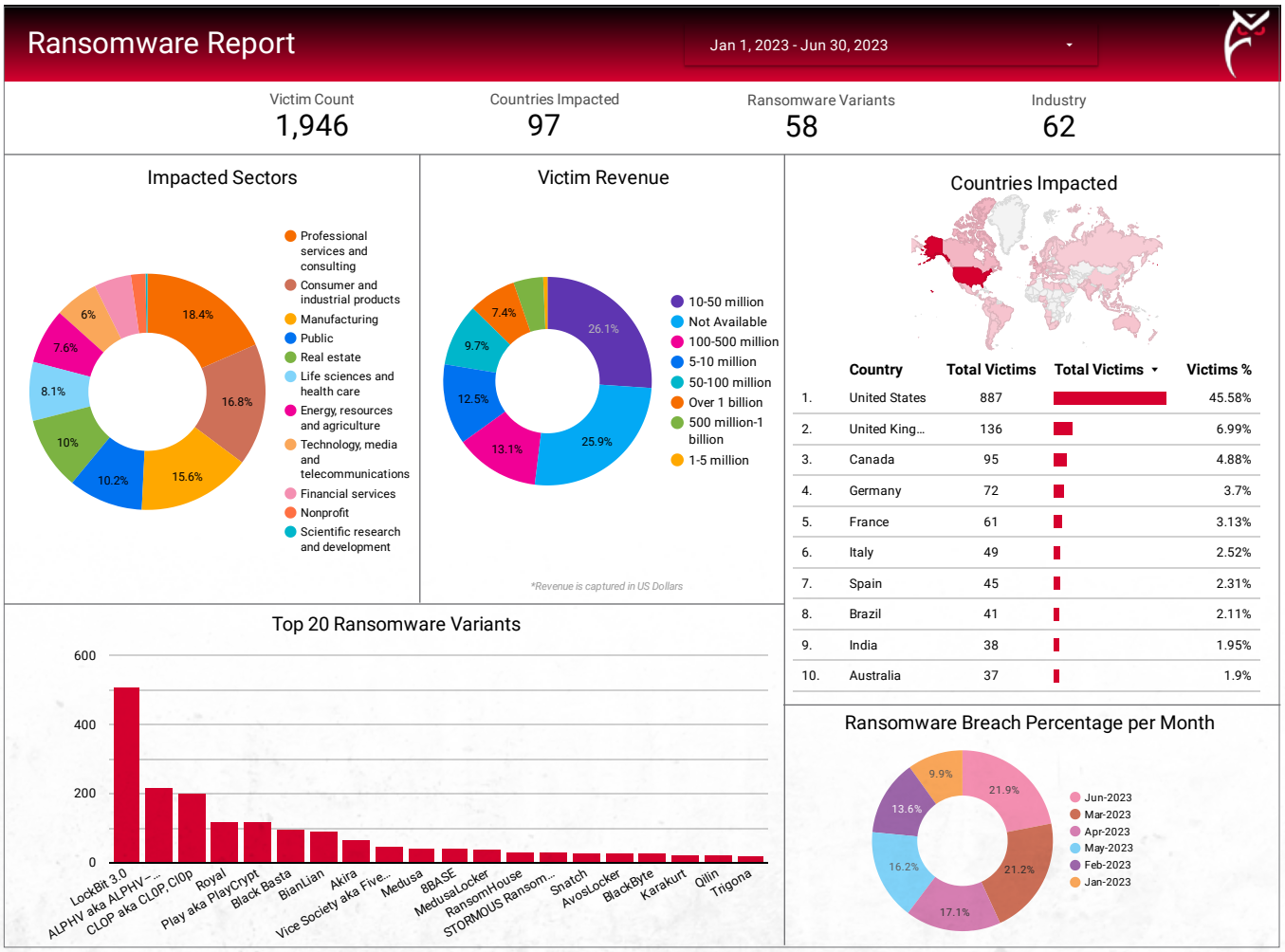
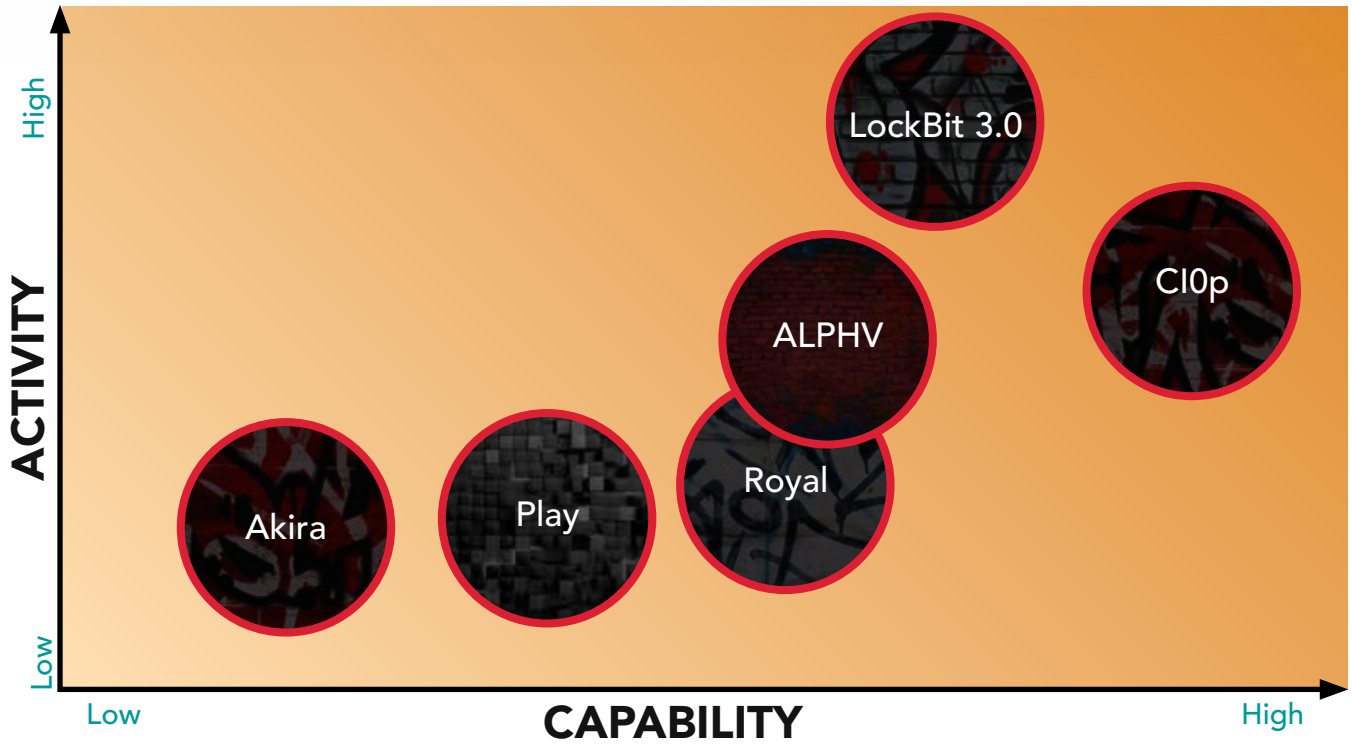


Figure 2: The image depicts a full breakdown of ransomware breach events across the first half of 2023.

In focus: Akira – 'New' variant



In the first half of 2023, operators of Akira allegedly impacted 65 victims, with the U.S., U.K., Canada, South Africa and Australia being the five most-impacted countries.

Although the major ransomware players largely dominated the first six months of 2023, we also observed the appearance of new variants. At the end of March 2023, the cyber threat landscape saw the emergence of ransomware dubbed **Akira**, though it reportedly did not become fully active until April 2023. Akira employs the usual double-extortion approach: encrypting data and threatening to release it on a victim shaming site hosted on the Tor network if the demanded ransom is not paid. The RaaS affiliate program was not openly advertised on cybercrime forums but actors tied to Akira engaged in recruiting additional personnel. Upon further examination, Akira appears to resemble parts of the Conti strain, implying developers of Akira might have used Conti ransomware files that were leaked in 2022.

In the first half of 2023, operators of Akira allegedly impacted 65 victims, with the U.S., U.K., Canada, South Africa and Australia being the five most-impacted countries. Akira affiliates seemed to focus predominantly on North American entities, accounting for nearly three quarters of all Akira victims. Moreover, the most-impacted sectors in descending order were professional services and consulting, manufacturing, public, real estate, and consumer and industrial products.

Assessment

In an ever-evolving cyber threat landscape, ransomware maintains its position as a leading concern for organizations globally — a scenario that is unlikely to change in the foreseeable future. As of the second quarter of 2023, this arena was dominated by the current "big three" players — LockBit 3.0, ALPHV and CI0p. These groups consistently adapt and evolve tactics to outpace their competitors and intended victims, highlighting the ransomware market's competitive nature and resilience.

The surge in ransomware threats over the years has evoked different responses from the cybercriminal underworld and cyber threat professionals. On one hand, underground threat actors recognize the lucrative prospects and are drawn to deploying ransomware or participating in a RaaS affiliate program — operations that have proven to yield substantial profit. On the other hand, successful ransomware variants often become targets of increased scrutiny from the media and law enforcement agencies. In response to this, the cybercrime landscape often witnesses the emergence of new or rebranded variants, to fill the void in the underground market. These successors often employ evolved TTPs aimed at averting the downfall experienced by their predecessors.

Ransomware maintains its position as a leading concern for organizations globally.

In the first half of 2023, new ransomware groups we observed included the rise of smaller factions that diverged from the affiliate business model, possibly to ensure better operational security (OPSEC) and foster internal collaboration. The emergence of these new groups testifies to the vibrant health of the ransomware scene, suggesting that, despite the dominance of established RaaS groups and variants, there is room for new players, like Akira, to carve out profitable niches.

While it is highly likely that the most prominent ransomware programs will retain their status quo in the upcoming months, the steady influx of newcomers to the market is a trend that calls for vigilant monitoring. As these groups strive to establish their foothold and refine their operations, their activities may significantly influence the dynamics of the global ransomware landscape.

ACCESS

In the first half of 2023, we observed and reported more than 2,000 claims from access vendors offering to sell compromised credentials and/or alleged unauthorized access to networks or systems. This is an increase of 23% in comparison to the 1,700 from the first half of 2022*. The U.S. was the most-impacted country at almost 16%, followed by Brazil at just over 7% and France at 5%. The top three sectors most impacted by these offers in descending order were public, consumer and industrial products, and professional services and consulting.

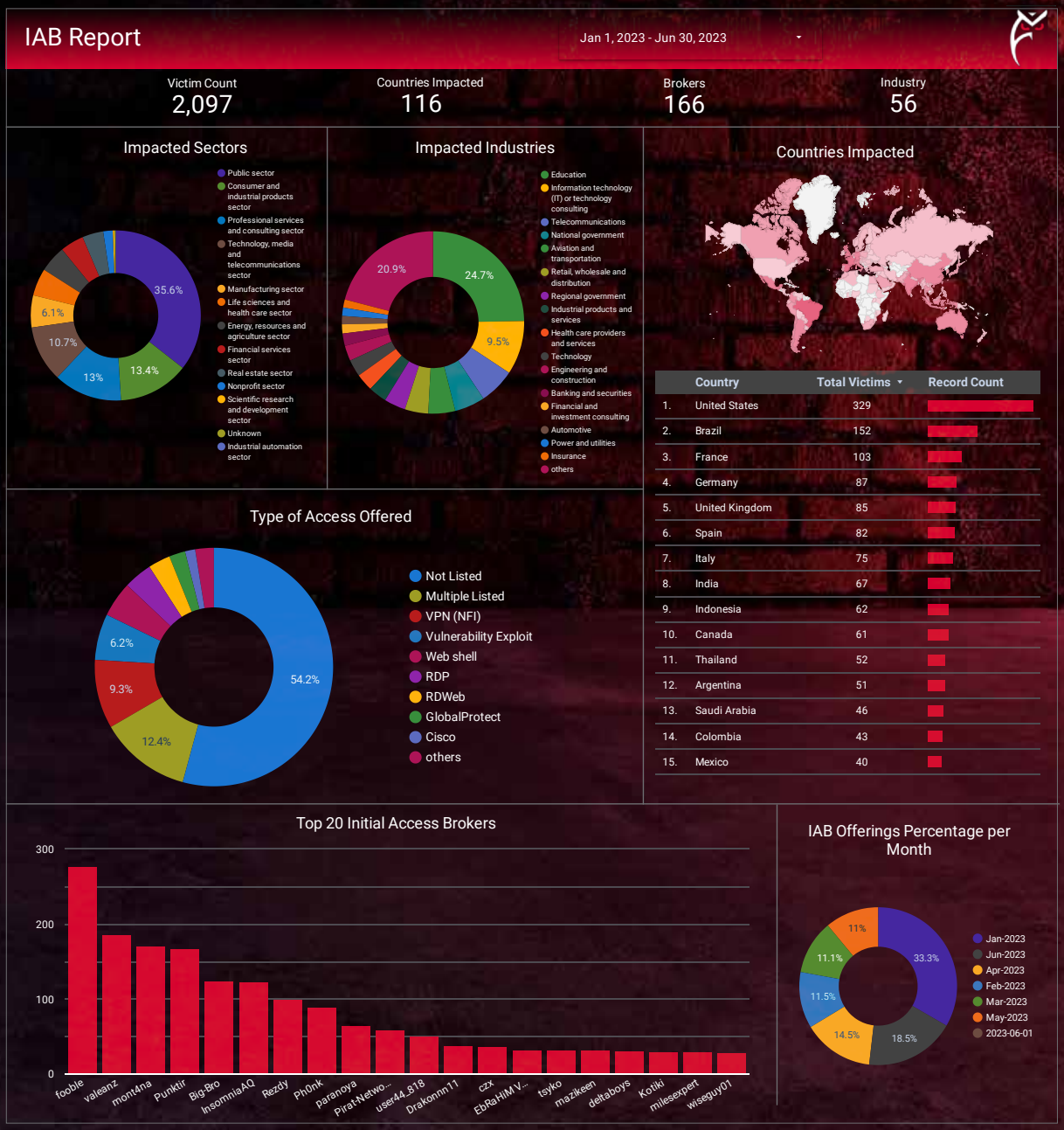


Figure 3: The image depicts a full breakdown of breach events reported by Intel 471 across the first half of 2023.

We split this data into two classifications to lower the noise floor.

- **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. Wholesale access is typically sold en masse where an actor sacrifices quality assurance for timely sales.

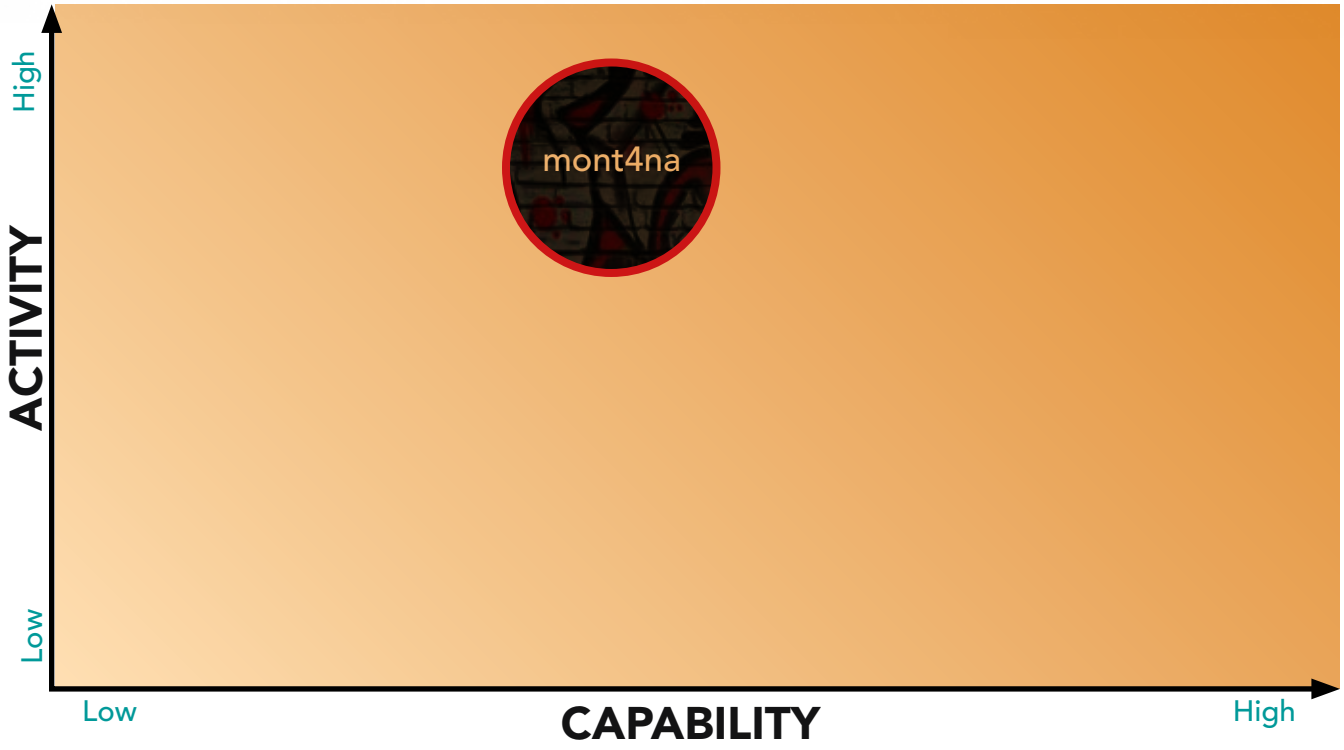
- **Specified access** is purported access to a network, resource or service by means of compromised access credentials, exploitation of a software vulnerability or misconfiguration or via similar means for which an indicator exists that a threat actor verified the validity of access as operational.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

This classification allows us to concentrate on more critical offers and claims of unauthorized access and ensure a more actionable view of access offers across the underground. We observed more than 600 instances of specified access, with the actor **mont4na** as the most impactful, and more than 1,400 offers of wholesale access, with the actor **fooble** as the most impactful.

We observed more than **600 instances of specified access** with **mont4na** as the most impactful.

...and more than **1,400 offers of wholesale access** with **fooble** as the most impactful.

In focus: Actor mont4na



While **mont4na** falls within both the markets of specified access claims and wholesale access offers, their offerings for specified access are far more substantial. Although the actor appeared to offer wholesale credentials, in the first half of 2023, mont4na offered just over 130 instances of specified access, making them the most impactful specified access broker at the time of this report. The variation in offers suggest an insight into mont4na's working practises. The actor is known for exploiting structured query language-injection (SQLi) vulnerabilities to gain specified access, and the amount of specified access offered indicates mont4na likely uses automated vulnerability scanning tools to provide starting points for further exploitation.

While the actor is very capable of finding SQLi vulnerabilities and exploring them, mont4na is likely not as capable of other, more advanced hacking such as expert pivoting, coding malware, exploits or other hacking tools which would provide more instances of wholesale access. It is possible that mont4na could triage the findings and seek to further exploit victims perceived to be more valuable, however, the offer of bulk credentials was slightly out of step with this methodology. Consequently, there is a possibility mont4na acquired credentials differently, potentially from marketplaces or through the use of malware.

Assessment

Access brokers remain key enablers of cybercrime by providing other threat actors with entry points into the underground cycle of fraud. These actors supply cybercriminals with a resource to carry out additional illicit activity within already compromised systems and networks. Moreover, as access offers remain popular, malware-as-service (MaaS) and other user-friendly tools will likely continue to lower the bar of entry, making it easier for threat actors with simple skill levels to participate in the booming market. This will likely ensure at least a continuation in the number of access offers, but also could result in a possible increase.

While wholesale access offers continually outnumber specified access, quantity does not necessarily equal quality or significance. Those who advertise wholesale access likely seek profit from a vast number of offers. They likely invest less time of their own to interrogate their inventory, which limits the information they can provide but also limits their exposure to further illegal activity. Conversely, those who offer specified access likely seek to increase profitability from their offers by investing time and skill to maximize the potential of access obtained.

Additionally, threat actors offering specified access appear to have the ability to carry out a variety of reconnaissance efforts; develop and obtain tools and malware; and occasionally maintain their foothold, move literally and/or exfiltrate an array of data from compromised networks. Actors who offer wholesale accesses likely source them from malware logs or purchase from others who likely are reselling captured data. Consequently, we continue to assess that vendors claiming to offer specified access, like mont4na, likely present a greater threat as they possess a higher level of sophistication compared to those who offer bulk wholesale access. Access offers as a whole continue to proliferate within the underground marketplace and this is unlikely to change in the next quarter.

Vulnerabilities

Threat actors persist in exploiting a broad spectrum of both recently discovered and long-standing vulnerabilities in their attempts to carry out a variety of cybercrime. As a result, keeping up with the latest vulnerability trends is of utmost importance. During the first half of 2023, the National Vulnerability Database (NVD) documented more than 12,100 newly identified vulnerabilities. This number indicates marginal growth compared to the same period of 2022, which saw the addition of just over 10,800 vulnerabilities. During the first six months of 2023, there also was a rise in the number of vulnerabilities classified as high or critical risk, reaching a total of almost 4,900. This figure indicates an increase compared to the previous year's tally of just over 4,600 vulnerabilities. The magnitude of reported vulnerabilities continues to make tracking, prioritization and patching efforts increasingly difficult. However, our Vulnerability Intelligence team strives to complement the effectiveness of the Common Vulnerability Scoring System (CVSS) mechanism by conducting supplementary analysis. This approach helps reduce unnecessary distractions and enables identification of more critical issues.

During the first half of 2023, the National Vulnerability Database (NVD) documented more than 12,100 newly identified vulnerabilities.

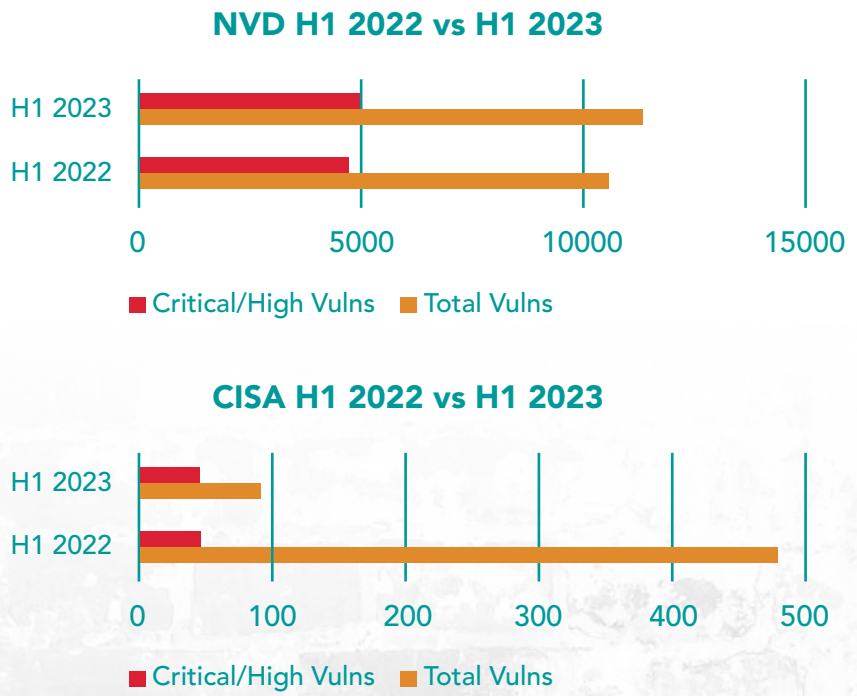


Figure 4: These bar charts depict the comparison of key vulnerability data from the first halves of 2022 and 2023.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) reported that about 42 vulnerabilities were identified as being exploited in the wild and were assigned the designation CVE-2023 during the first six months of 2023. This figure is one CVE shy of those exploited in the first half of 2022 (CVE-2022). CISA also maintains a living list of documented vulnerabilities that have been successfully exploited, known as the Known Exploited Vulnerabilities (KEV) Catalog. A total of 97 vulnerabilities were included in the KEV Catalog during the first six months of 2023. Interestingly, this figure is significantly lower than the 475 vulnerabilities added to the KEV Catalog during the first half of 2022. The disparity of successfully exploited vulnerabilities between the two dates, despite the similar number of newly exploited vulnerabilities identified, suggests a greater number of older vulnerabilities were included in the KEV Catalog during the first half of 2022 compared to the first half of 2023. This could indicate threat actors in 2023 are more focused on exploiting recently discovered vulnerabilities, often referred to as zero-day or one-day vulnerabilities, rather than targeting older ones.

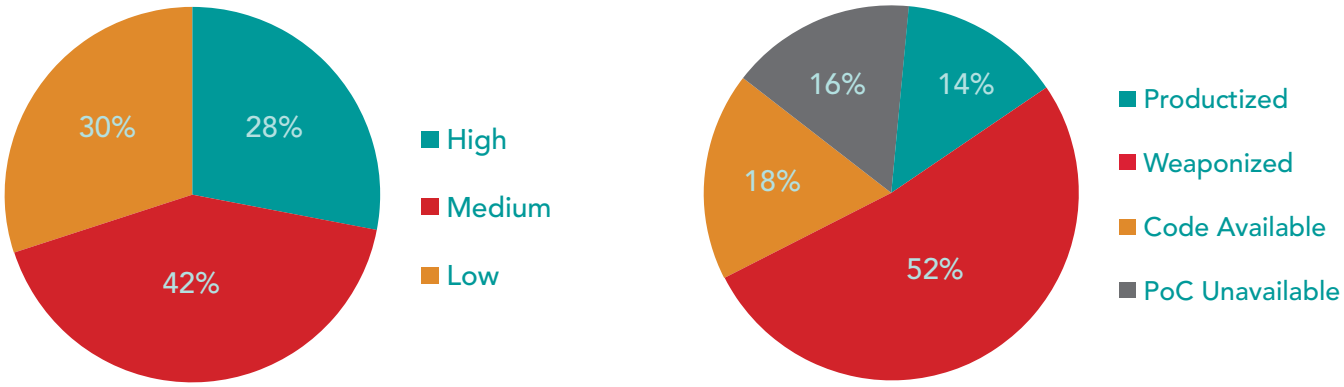


Figure 5: These pie charts depict the risk level (left) and exploit status (right) of CVEs Intel 471's Vulnerability Intelligence team reported and assessed in the first half of 2023.

Throughout the first half of 2023, we documented about 260 vulnerabilities in our reports*. Among these, 28% were rated as high risk, 42% medium and 30% low. Of the reported vulnerabilities, 14% were productized, meaning they were available for use in mass production by unsophisticated actors, such as incorporating exploits into Armitage, Cobalt Strike, Core Impact, Metasploit, Nexpose and more; 52% were weaponized, meaning they were integrated into malicious code for use by sophisticated actors, including exploit kits and malicious advertising (malvertising); and 18% had only PoC code available, meaning PoC code for those vulnerabilities was published and/or shared in the underground.

Separately, we continue to observe frequent exploitation of Internet-of-Things (IoT) devices across the underground. IoT devices are ubiquitous and often poorly protected and as such are leveraged by threat actors to build out powerful botnets.

In focus: GoAnywhere, MOVEit vulnerabilities allegedly leveraged by CI0p ransomware operators

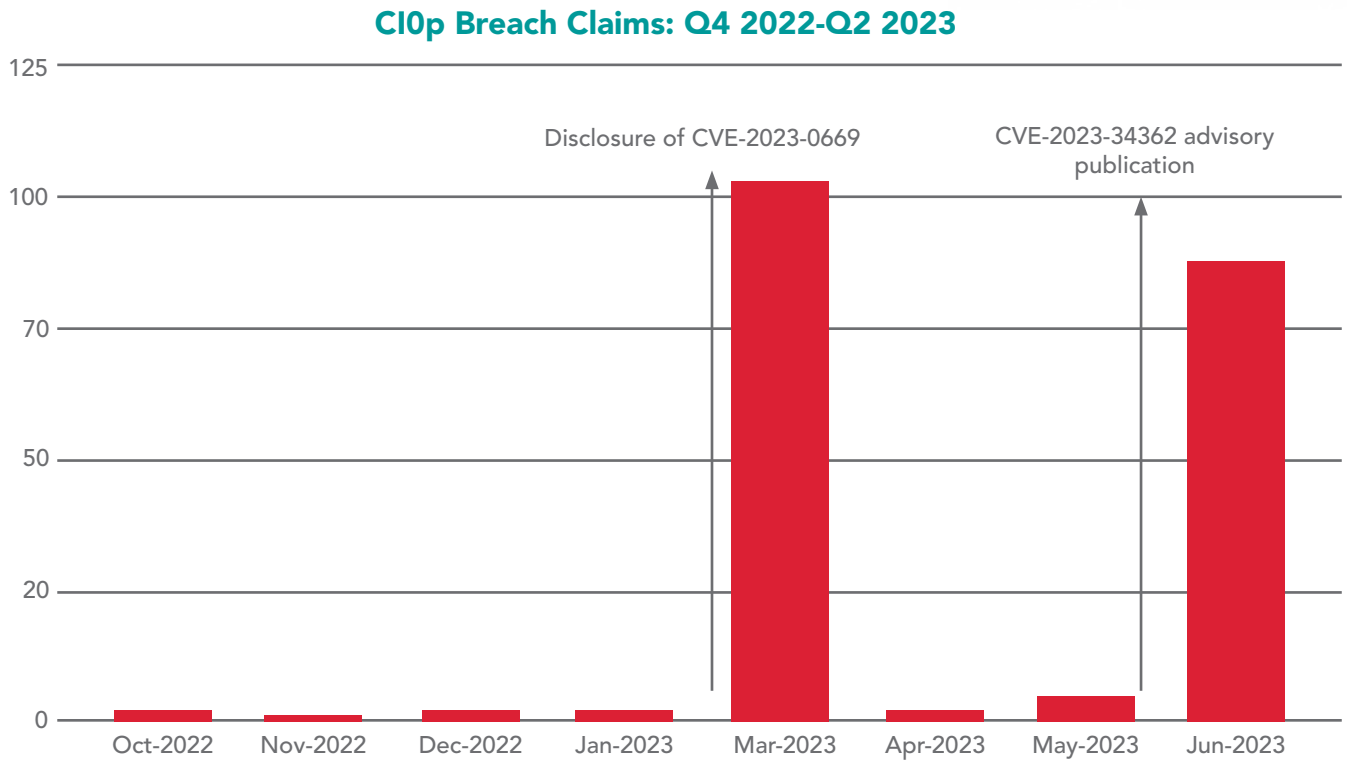


Figure 6: This chart shows CI0p breach claims from OCT '22 through JUN '23.

In February 2023, a deserialization of untrusted data vulnerability impacting Fortra GoAnywhere managed file transfer (MFT) was disclosed and designated CVE-2023-0669. Fortra and security researchers at CISA claimed the vulnerability was actively exploited in the wild and a Metasploit module was observed in open source. The CI0p ransomware gang also claimed via the Bleeping Computer cybersecurity website that it weaponized and leveraged the vulnerability for targeted attacks. We then observed new developments from the CI0p RaaS in the form of a significant increase in activity following a relatively quiet 2022. Within an 18-day period in March 2023, CI0p operators claimed to compromise more than 100 entities. This surge in activity likely was related to the exploitation of CVE-2023-0669.

Then in late May 2023 and into June, Progress Software published several advisories addressing three critical SQLi vulnerabilities impacting multiple versions of Progress MOVEit Transfer software tracked as CVE-2023-34362, CVE-2023-35036 and CVE-2023-35708. According to Progress Software and

security researchers at CISA, CVE-2023-34362 was exploited in the wild and security researchers at the Microsoft Threat Intelligence Center (MSTIC) claimed the CI0p ransomware group likely weaponized and leveraged the vulnerability for data theft and extortion attacks. This was corroborated by individuals claiming to be part of the CI0p group to reporters at Bleeping Computer. In the first week of June 2023, the operator or operators behind the CI0p ransomware blog claimed to have gained access to information of "hundreds" of companies using MOVEit software. The adversaries threatened impacted entities to contact the CI0p team before June 14, 2023 or they would publish the exfiltrated data. On the given deadline, CI0p compromised 12 entities via its name-and-shame blog and continued to list alleged victims throughout the month, totalling 88 entities in June 2023. The group have resorted to exfiltration only extortion, as opposed to exfiltration and encryption (double extortion). This TTP allowed CI0p to choose when to reveal victims and therefore control victim negotiations better. Extortion-only ransomware attacks are steadily on the increase amongst ransomware groups.

The public manner in which CI0p navigated the MOVEit vulnerability likely was designed to create a sense of fear. The initial request for organizations to contact CI0p possibly was an attempt to illicit easy funds from unaffected parties. Once this tactic was exhausted, the group moved to the disclosure phase and sought to pressure alleged victims further. The group claimed it would erase data from government agencies, city services and police departments, however, this likely was an attempt to limit law enforcement attention and an excuse to focus efforts on more lucrative, high-earning businesses. It is highly likely that data stolen from the aforementioned groups has not been deleted and will be held for future use. Considering the highly publicized nature of CVE-2023-34362 and the release of a full remote code execution (RCE) exploit PoC in open sources, the vulnerability will likely be used in additional attacks by a variety of threat actors.

Assessment

There are several assessments to be made considering that vulnerabilities appear to be intertwined with many other key threats discussed in this report. On a basic level, threat actors almost certainly will continue to leverage new and existing vulnerabilities and target companies that fail to implement necessary patches or workarounds in a timely manner. Additionally, ransomware attacks have the capability to become more targeted and complex with threat actors exploiting known vulnerabilities to maximize financial gain.

IoT devices likely also will continue to be exploited for a variety of attacks, primarily DDoS, as the inherent risks associated with their widespread deployment combined with slow patch prioritization is often overlooked, making them easy targets for malicious actors seeking to disrupt networks and services. Lastly, the shrinking time between initial disclosure or discovery of a vulnerability and the publication or creation of PoC code will likely put certain infrastructure in danger if organizations lack a quick patching and vulnerability management strategy. We continue to recommend patch prioritization based on threat intelligence provided by our Vulnerability Intelligence Dashboard in our TITAN platform.

Malware

Underground trends

In addition to technical malware monitoring from our Malware Intelligence Team, we also monitor the underground threat landscape to track the frequency of malware offers for sale by threat actors. This provides insight into the appetite for certain types of malware and therefore the prevalence of a threat. In the first half of 2023, we observed actors offering a large volume of remote access trojans (RATs) as well as drainer, loader and stealer malware. Drainer malware will be discussed in greater detail in the upward trends section of the report.

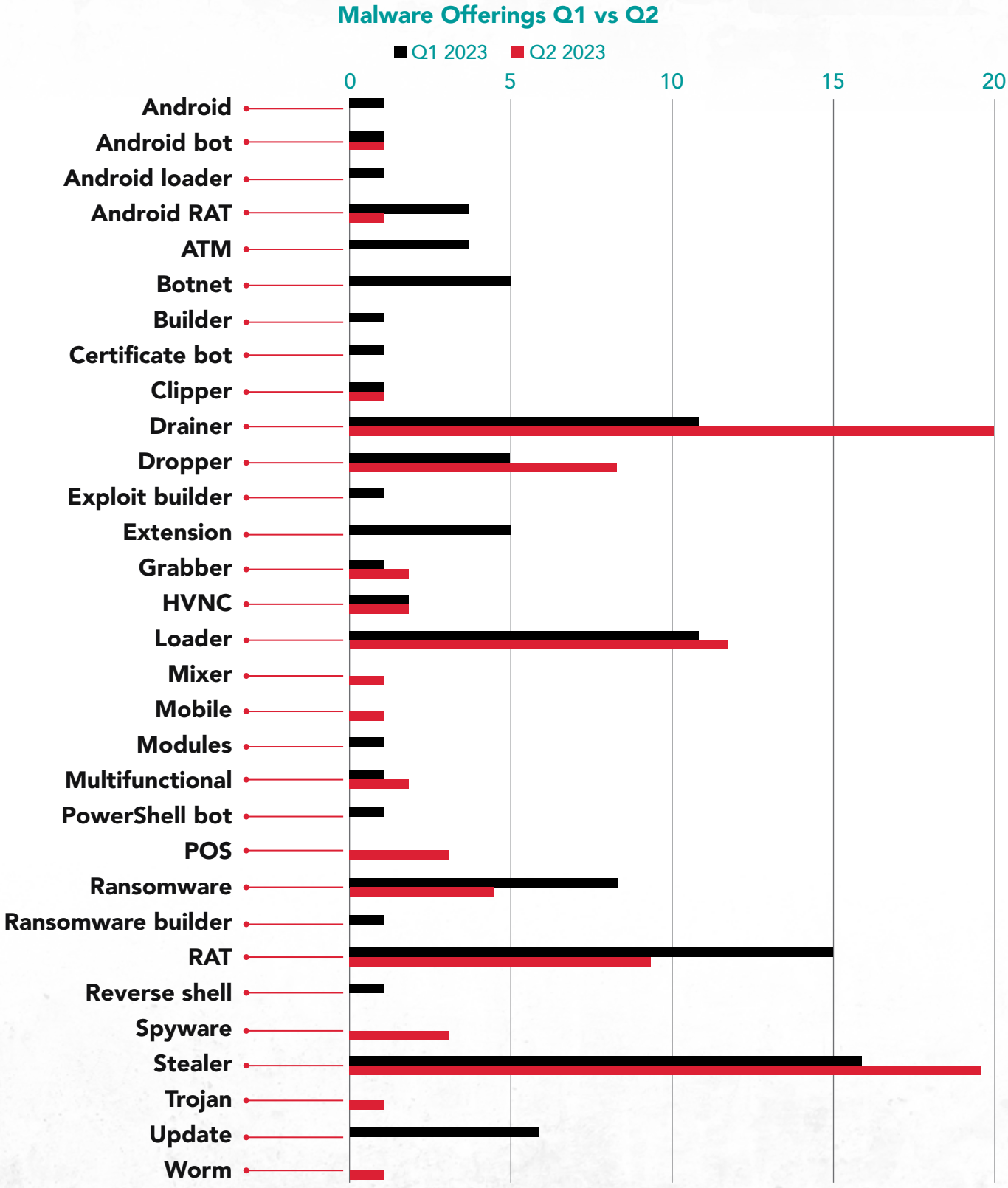


Figure 7: This image depicts the top malware types offered in the underground in Q1 2023 and Q2 2023.*

Separate to malware marketplace, we tracked the fluctuating activity of two tenured botnets: **Emotet** and **QBot**. Botnets typically do not feature as an abundantly offered asset in the underground because the infrastructure required to host them is difficult to establish and therefore likely not constructed quickly or with ease.

In focus: Decline of Emotet, rise of QBot

Our technical malware capabilities are acutely tuned to the monitoring of the botnet malware landscape. The landscape has largely been dominated by two infamous botnets — Emotet and QBot. Both groups initially emerged as banking trojans and have lengthy underground histories, with QBot surfacing in 2007 and Emotet in 2014. The latter eventually morphed into what once was considered the world's largest botnet before a collaborative effort in January 2021 coordinated by Eurojust and Europol succeeded in dismantling Emotet, albeit temporarily. During Emotet's inactivity, QBot developers continued to refine their infrastructure and bot and maintained their aggressive expansion of botnets. As a result, QBot emerged as one of the main threats that companies faced during 2022 and 2023.

Campaigns propagated by Emotet and QBot operators

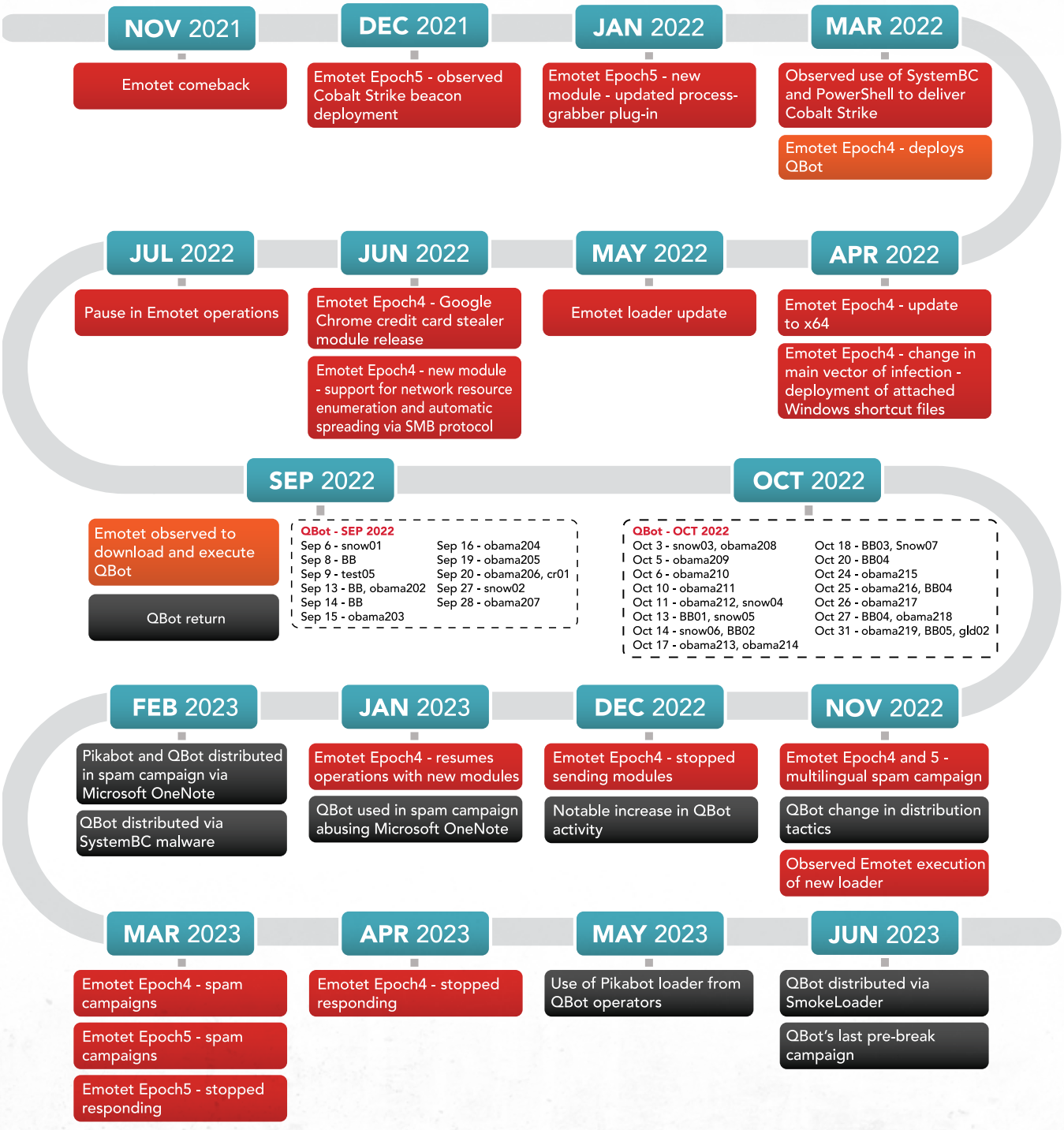


Figure 8: This image depicts the timeline of the campaigns propagated by Emotet and QBot operators in 2022 and 2023.

The legal victory against Emotet proved only to be temporary when it reemerged in November 2021. Upon its return, it launched a series of spam campaigns. The operators initially adopted a strategy that exploited stolen email reply chains to distribute malicious Microsoft Word or Excel documents with embedded Visual Basic for Application (VBA) macros. However, in April 2022, Emotet altered its tactics and started to use attached Windows shortcut files (LNK) as the primary vector for infections in malicious spam emails. The adjustment likely aligns with Microsoft's February 2022 decision to disable VBA macros in all downloaded documents, ultimately enforced in July of that year. After a hiatus over the summer of 2022, both QBot and Emotet resurfaced in September. QBot reappeared first with updates and the new botnet ID "snow01." Emotet was then seen by our systems downloading and executing an instance of QBot bearing a different botnet ID "azd." This sequence marked a significant development for actors involved with Emotet, who previously were quiet on the spam and distribution front. It suggests the potential for a botnet transfer, implying the actor operating Emotet may continue operations under the banner of QBot.

Assessment

Emotet and QBot have had a long tenure in the underground malware domain and have built reputations to establish themselves as among the most formidable cyber threats in history. In times of significant change, adaptability becomes a crucial determinant of survival. The ability to evolve and navigate new challenges dictates which products, goods and services remain key players in the underground and which ones fall into decay. Since its emergence in September 2021, Emotet went through multiple transformations and was leveraged in diverse campaigns. Nevertheless, the extended periods of inactivity could suggest Emotet operators faced technical difficulties maintaining their botnets online. This fact ultimately led to difficulties in leveraging the bots for further monetization, including ransomware operations. The demise of Emotet does not mean actors involved quit all criminal endeavors, but rather that they likely migrated their bot base to another botnet and continued operations from there. From 2022 through 2023, QBot operators demonstrated great adaptability by devising new delivery chains and unleashing aggressive spam campaigns. Despite a pause in QBot activity at the end of June 2023, presumably for a summer break, we anticipate it will remain a prominent player in the cyber threat landscape in 2023 and likely increase its activity throughout the rest of the year.

In times of significant change, adaptability becomes a crucial determinant of survival.

Pro-Russian Hacktivism

The first half of 2023 saw Russia's full-scale invasion of Ukraine enter its second year and we continued to observe threat actors leverage the situation for both financial gain and to further their political cause. As a result, pro-Russian hacktivism remains the most significant byproduct from the war in the cybercriminal underground. This included loosely organized and associated groups of pro-Russian cybercriminals who conducted attacks against entities in countries perceived as enemies of Russia's ongoing war in Ukraine. These attacks were largely carried out via distributed denial-of-service (DDoS) attacks, though website defacement and network intrusions also were observed. Generally speaking, the impact of these groups' campaigns was limited and members likely had rudimentary technical skills at best. Nevertheless, the potential reputational impact of an attack was, and still is, substantial.

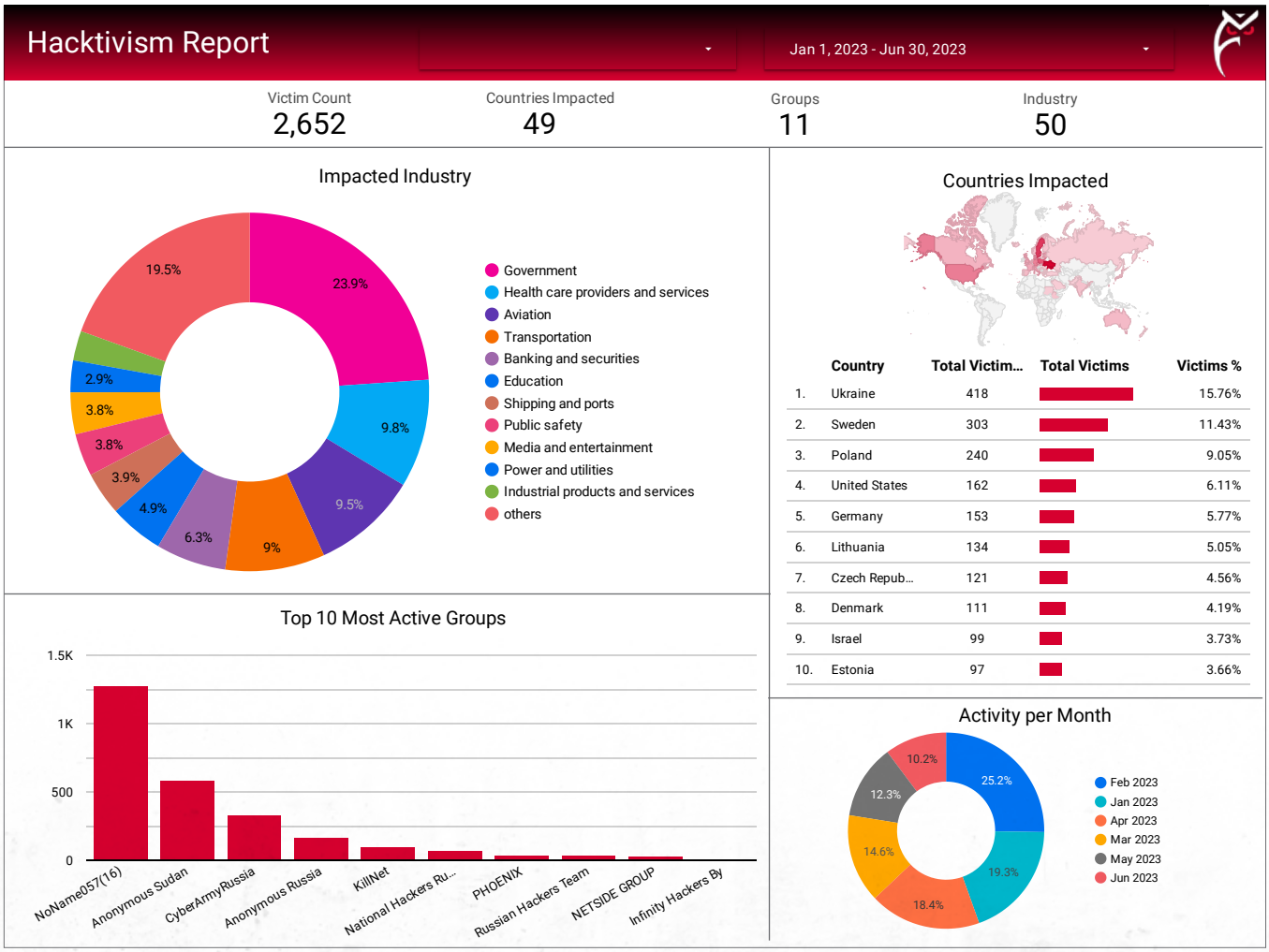
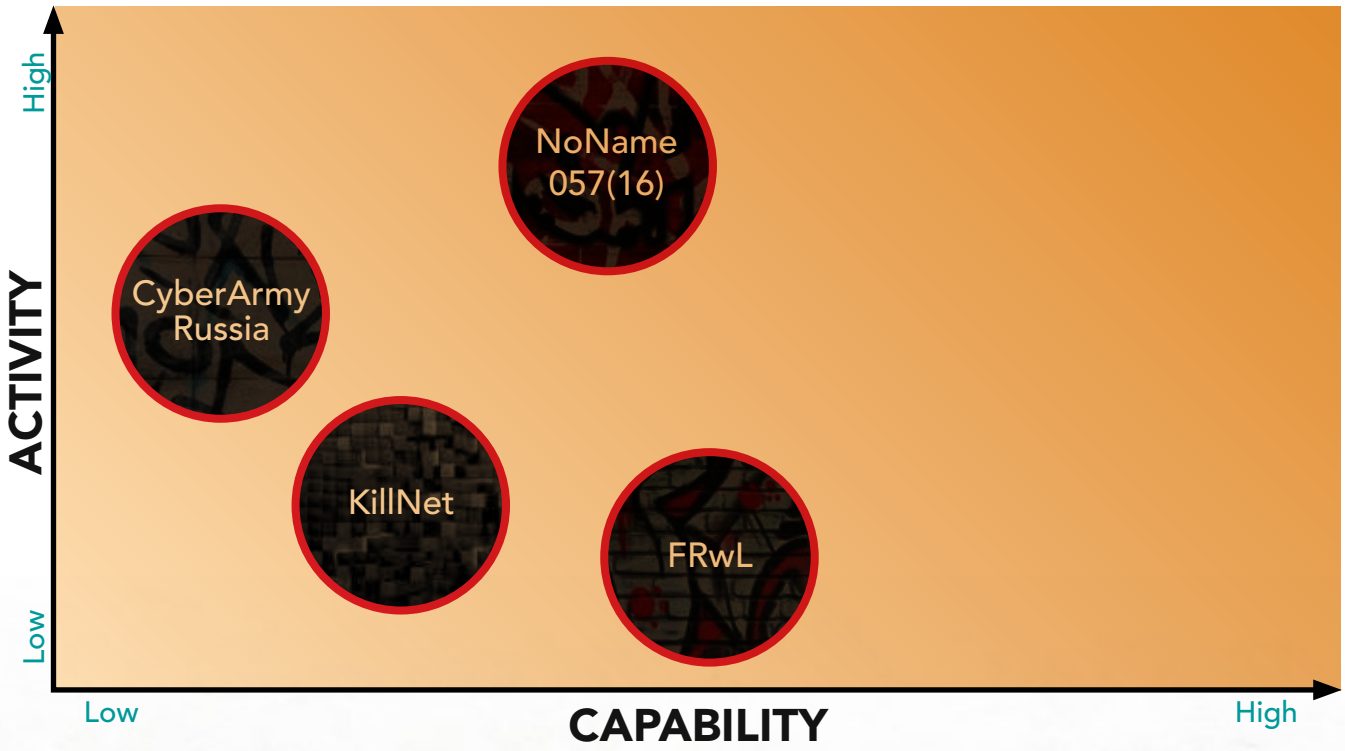


Figure 9: This chart depicts a full breakdown of hacktivist activity across the first half of 2023. This data includes the non-Russia-aligned group Anonymous Sudan, which accounted for almost 400 breaches and 200 breaches in the first two quarters of 2023.*

Pro-Russian hacktivists were highly reactive to on-the-ground events since the beginning of operations in February 2022. In the first half of 2023, we recorded 2,652 entities impacted by alleged hacktivist DDoS attacks*. The five most-impacted industries were government, health care providers and services, aviation, transportation, and banking and securities. The first quarter of the year saw a slight reinvigoration of efforts from pro-Russian hacktivist groups after a slight decline toward the end of 2022. This small revival was likely in response to increased NATO provisions sent to Ukraine as well as the Kremlin's move to a protracted war in Ukraine based on the revitalization of Russia's defense industrial base (DIB).

By the second quarter of 2023, we observed another significant downturn. We largely attributed this to a declining appetite for hacktivism in pro-Russian cybercrime circles. The general landscape of pro-Russian hacktivism is likely fractured — groups conducted widespread internal restructuring, objectives constantly fluctuated without logic and group leadership and alliances remained unsettled.

In focus: Move to financially motivated cybercrime



The first half of 2023 was marked by many pro-Russian hacktivist groups changing their tactics. Several groups moved into more financially motivated cybercrime and alleged network intrusions. This included the hacktivist group **FRwL Team** aka **From Russia with Love** who claimed to deploy its own ransomware variant dubbed Somnia against a U.S.-based energy company, though it was likely a third-party supplier instead. Additionally, members of **KillNet** — likely the highest profile pro-Russian group — launched its own cybercrime forum at the start of 2023 known as INFINITY. This foray into financially motivated cybercrime was short-lived; however, as an actor connected to the project listed it for sale only three months later. This temporary move was likely executed in an attempt to raise funds, as we also observed the groups post pleas for donations from supporters during this time. The decision to abandon the ideals of hacktivism by engaging in such activity also likely contributed to the disillusion of some members.

Assessment

Pro-Russian hacktivism appeared to have a difficult start to 2023. Waning interest among cybercriminals reflects Russia's faltering hopes of what it would deem a positive outcome in the war against Ukraine. The first half of 2023 also was marked by outlandish claims, such as a collaborative attack by **Anonymous Sudan**, KillNet and the **REvil** ransomware gang on European banking and payment systems. These dubious declarations amounted to very little in reality and likely are highly indicative of the current desperation of pro-Russian groups to remain relevant in the public eye. Pro-Russian hacktivist attacks will likely continue to have limited, short-term impact and as a result similarly extreme claims will likely be made in the near future in an attempt to maintain media interest and/or garner much-needed donations from followers or supporters.

These dubious declarations amounted to very little in reality and likely are highly indicative of the current desperation of pro-Russian groups to remain relevant in the public eye.

OTHER CYBERCRIME TRENDS

Upward trends

Artificial intelligence gains interest among cybercriminals

At the start of the year, we reported that AI had become a popular topic of conversation on underground forums. Since then, most observed activity has consisted of general discussions regarding public news of AI developments or legitimate money-making concepts, such as using ChatGPT to generate content to complete services advertised on freelance websites including Fiverr or Upwork. Threat actors debated whether AI is good overall, speculated on the future with AI and promoted ways to allegedly make money using current AI tools. We also observed threat actors claim to use ChatGPT to develop cheats for video games and create viewbots for SoundCloud and YouTube. Few threat actors allegedly used the chatbot for truly malicious purposes; however, numerous forum threads were created to discuss the possibility of leveraging ChatGPT in social-engineering attacks, as well as the collection of personal information and distribution of malware.

The impact and prospect of AI also likely motivated an XSS forum administrator to create a new section called the "AI / ML" subforum in late January 2023. The forum section is dedicated to the topics of AI, deepfake synthetic media, machine learning (ML) and neural networks. Some notable posts included a modified version of an information stealer using ChatGPT to revise and improve the code, as well as a keylogger for a browser, allegedly created in the same manner. We also observed actors request AI to write Python scripts to exploit an improper input validation and a random number generator (RNG) vulnerability. Multiple threat actors also discussed developing Discord and Telegram bots connected to the OpenAI application programming interface (API).

We reported a few examples of actors implementing AI in their offers during the second quarter of 2023. A notorious initial access broker (IAB) offered free translation services that allegedly could translate large files in the PDF, PowerPoint presentation and Word processing document file formats using AI, although the actor did not name a specific AI tool or model. Another actor offered tools via a Telegram channel, including one that allegedly could bypass ChatGPT chatbot restrictions. This actor claimed users could ask any

question regardless of the context and receive a response. Another actor allegedly integrated AI into software to draft spam emails and numerous actors showed interest in using it.

The sentiment across the underground at the start of the year suggested ChatGPT could be used to assist with certain tasks if properly asked, but in many cases the chatbot proved to be too immature. In numerous instances, ChatGPT made errors that included suggesting incorrect code or using nonexistent or unrelated functions. Many actors with backgrounds in programming expressed similar concerns and we observed threat actors voicing corresponding opinions regarding the use of ChatGPT for cryptocurrency trading.

Our observations of activity related to AI both in the underground and in open source indicate most use cases require human interaction and supervision to achieve accurate or sophisticated results. Therefore, actors are best suited to leverage the technology to alleviate trivial demands and supplement greater activity such as creating phishing emails and tools to augment, rather than innovate, the technology they already have in place. We still assess AI cannot be fully relied upon for more intricate cybercrime and doing so, in its current form, would likely render flawed results. Nevertheless, threat actors will continue to experiment with AI and remain cognizant of any progress made with AI-related applications so they can attempt to capitalize on the improvements when the opportunities present themselves.

Numerous forum threads were created to discuss the possibility of leveraging **ChatGPT in social-engineering attacks,** as well as the **collection of personal information** and **distribution of malware.**

LAW ENFORCEMENT ACTION AGAINST CYBERCRIME

While cybercriminal activity continues to grow in strength and numbers, the fight against cybercrime is also on the rise. Since the start of 2023, we have already released 21 Spot Reports covering instances of law enforcement operations, disruptions, takedowns, arrests, indictments and more; suggesting we will far outstrip the previous year's total of 23 Spot Reports.

January

Jan. 26, 2023: U.S. DOJ announces disruption campaign against Hive ransomware.

Feb. 9, 2023: U.K. authorities announce sanctions individuals involved in Conti and TrickBot operations.

Feb. 22, 2023: U.S. DOJ unseals indictment against individuals.

Feb. 28, 2023: Europol carries out joint law enforcement action against DoppelPaymer ransomware members.

February

March 9, 2023: U.S. DOJ announces seizure order against domain advertising/selling NetWire RAT.

March 15, 2023: U.S. law enforcement arrests Conor Brian Fitzpatrick aka pompompurin, owner/administrator of Breached forum.

March

March 15, 2023: U.S. DOJ unseals indictment against operator of ChipMixer cryptocurrency mixing service.

March 24, 2023: Investigative Committee of Belarus announces charges against alleged carder/leader of cybercriminal gang.

April 3, 2023: Media reports arrest of alleged operator of underground search engine of stolen data dubbed Udyat.

April 4, 2023: Europol announces law enforcement operation against Genesis Store infrastructure.

April 15, 2023: Actor Killmilk claims Belarusian authorities arrested alledged founder/former member of Anonymous Russia.

April

May 1, 2023: SBU announces takedown of criminal proxy/VPN services provider.

May 1, 2023: Law enforcement seizes Monopoly Market.

May 2, 2023: National Police of Ukraine announce law enforcement action against nine underground cryptocurrency exchange services.

May

May 3, 2023: U.S. authorities announce takedown action against Try2Check payment card validity-checking service.

May 8, 2023: U.S. DOJ announces seizure of 13 domains linked to DDoS-for-hire platforms.

May 16, 2023: U.S. DOJ unseals indictment against Russian national Mikhail Paviovich Matveev aka wazawaka.

June 15, 2023: U.S. DOJ unseals indictment against Russian national Rusian Magomedovich Astamirov for his alleged involvement in the LockBit ransomware operation.

June 28, 2023: Media reports Nikita Kislitsin, employee of F.A.C.C.T. cybersecurity firm, formerly Group-IB, was detained in Kazakhstan upon a U.S. extradition request.

June

Figure 10: This timeline depicts notable instances of law enforcement action from the first half of 2023.

Notable instances of law enforcement action from the first half of 2023 include the disruption campaign and eventual takedown of the Hive RaaS group in January; Europol's joint law enforcement operation with the German regional police and the National Police of Ukraine that targeted suspected core members of the criminal group believed to be behind the DoppelPaymer ransomware in late February; the arrest of Conor Brian Fitzpatrick in March, who is believed to be behind the **pompompurin** handle, that subsequently led to the closure of the Breached cybercrime forum; and a disruption attempt against the popular one-stop shop for compromised hosts and their associated account logs, browser cookies and fingerprints, Genesis Store, in April.

With this rise in law enforcement action and disruptions against cybercriminal activity, we assess threat actors will almost certainly strive to develop TTPs and enhance OPSEC to circumvent apprehension or interference to their illicit activity. Law enforcement action against cybercrime can appear cyclical — cyberattacks grow in prominence, causing a proportionate increase in arrests, takedowns and disruptions. Threat actors respond by altering their activity, such as avoiding certain targets or attack vectors, until law enforcement abates, at which point threat actors become emboldened. As a result, law enforcement's goal is likely to disrupt cybercriminals for a protracted time as opposed to the greater, unlikely goal of stopping it altogether.

Drainers

As previously mentioned, in the first half of 2023, we observed actors offer a large volume of drainer malware. Cryptocurrency drainers typically come in the form of phishing pages designed to convince a victim to connect a cryptocurrency wallet to a fake service. The victim then receives a prompt asking to accept a condition to verify the authenticity of the wallet or allow access to non-fungible tokens (NFTs). However, the prompt actually is an overlay of the adversary's script and instead authorizes the transfer of the wallet's contents to the threat actor's address.

Cryptocurrency is one of the key components of the underground, enabling cybercriminals to turn illicit goods into legal tender securely and secretly. The digital nature of the currency may be one of its greatest strengths, but also is what makes it so alluring to threat actors. Targeting cryptocurrency wallets with drainers allows actors to reduce their workload, since there is no requirement to purchase

cryptocurrency as part of the laundering cycle. Threat actors can simply wash stolen assets through any number of cryptocurrency mixing services. Another reason for drainer popularity is likely due to its simplicity and ease of development. The cost benefit of creating it is low and as such leads to their ubiquity. An additional contributor is likely the rebound in the value of cryptocurrency this year. A burgeoning cryptocurrency market almost certainly generates an upturn in new users who are more likely to be unfamiliar with the security pitfalls.

Downward trends

Dump shops

Underground dump shops offering compromised payment card data have dropped in popularity over the past few years alongside notable closures of shops such as Joker's Stash and UniCC. No other offerings have risen within the market to fill those gaps at the time of this report. The first half of 2023 saw a failed attempt by a likely imposter of the actor **JokerStash** to relaunch the notorious shop as well as the takedown of Try2Check, which was the checker of choice used at many popular underground dump shops. Increased efforts from law enforcement, credit card issuers, banks, e-commerce and other retailers to improve security has caused the acquisition, sale and use of compromised payment card data to become more difficult. This likely led threat actors to seek other ways to obtain illicit profits. Based on the aforementioned key and upward trends, we assess cybercriminals likely moved away from the once popular ecosystem of dump shops to the ransomware and/or cryptocurrency markets that offer much easier and greater profits.

ATM malware, physical attacks

In addition to the aforementioned improvement of protection and security measures that likely impede the use of stolen card data, we observed a large change in how society interacts with money since the COVID-19 pandemic. One of the most notable changes was the reduction in ATM usage. For example, since the pandemic, the U.K. has seen a near 20% reduction of ATMs nationwide, while the U.S. saw a slower decline with a near 5% reduction. This could signal a literal reduction in targets; however, it also demonstrates a likely decline in relevance that has permeated to the underground threat environment. The need to physically penetrate ATM exteriors to enable access to internal software requires additional skill sets and an actor to conduct them in person. This increases the risk to the perpetrator and as such is less likely to be adopted by the cybercriminal community, which likely prefers to remain behind the keyboard.

to enable access to internal software requires additional skill sets and an actor to conduct them in person. This increases the risk to the perpetrator and as such is less likely to be adopted by the cybercriminal community, which likely prefers to remain behind the keyboard.

Point-of-sale malware

The closure and lack of resurgence of notable underground dump shops, decline in ATM attacks and improved security measures that likely curtail carding activity could be correlated to a similar trend in the PoS malware market. It appears few actors offering PoS malware are active these days and we have not observed many worthy new offerings as of late. Further to this, dump shop closures likely inhibited cybercriminals' ability to cash out large quantities of compromised payment cards obtained via ATM and PoS attacks. As a result, even when threat actors have compromised payment card data to sell, it is not as easy as it once was. The most likely reason we continue to see fewer PoS-related attacks is actors who once were involved heavily in PoS malware activity switched to conducting or participating in ransomware attacks. We assess this to be a likely course of action due to ransomware's persistent popularity and proven success, which continues to play a large role in changes we noted regarding formerly prevalent services — especially considering we previously reported threat actors from an array of underground services migrated to ransomware for the opportunity to increase profit margins.

The most likely reason we continue to see **fewer PoS-related attacks** is actors who once were involved heavily in PoS malware activity switched to conducting or participating in **ransomware attacks.**

KEY TAKEAWAYS

This report drives home the dynamic nature of the cyber threat landscape: constantly shifting as threat actors respond to global events, refine their skills and exploit new opportunities for their own gain. Only by pinpointing the key trends, actors and events within this flux will organizations be able to identify the cyber threats looming beyond the horizon. Intel 471 is proud to be your voice of reason and truth in this field. Our key takeaways divulge the critical information that organizations must equip themselves with if they are to cut through the noise and enable a proactive cybersecurity strategy.

Across the globe, ransomware persists as a dominant force in the cyber environment. Our statistics display an increase of more than 76% for the first half of 2023 compared to 2022, suggesting it is a threat that will continue to plague enterprises and agencies. This report identifies the rise of smaller groups who are moving away from the affiliate business model (aka RaaS), potentially as a way to ensure better OPSEC and/or promote internal collaboration. Nevertheless, the RaaS space remains active and largely dominated by LockBit, Cl0p and ALPHV. It is possible additional smaller groups could emerge as other schemes fall victim to their dominance. Intel 471 has also observed subtle changes such as the steady increase in ransomware groups who are moving to extortion-only attacks. This unique change may be the result of organizations implementing more effective backup policies which render encryption less impactful or deliver the ransomware group greater control over the naming and shaming of its victims, as demonstrated by Cl0p.

Another key driver maintaining its prominence in the cyber underground is the market for access and those who provide it. Access and Initial Access Brokers are integral to the underground ecosystem. They act as critical enablers for several other variations of cybercrime. Access is becoming the key good offered in the underground market, surpassing payment cards and data offers. This also correlates with the most frequent TTPs observed by our researchers and analysts.

The prevalence of information-stealer malware is increasing due to the relative ease with which logs can be parsed and sold, and the growth in ransomware continues to perpetuate and generate a market for access.

Critical vulnerabilities also will not disappear from the threat landscape in the near future. If ransomware precipitates access, access could be seen to precipitate the use of vulnerabilities. Ransomware groups and access brokers are highly likely to continue to seek and exploit public-facing vulnerabilities. Consequently, organizations will continue to face risks from both known and unpatched vulnerabilities.

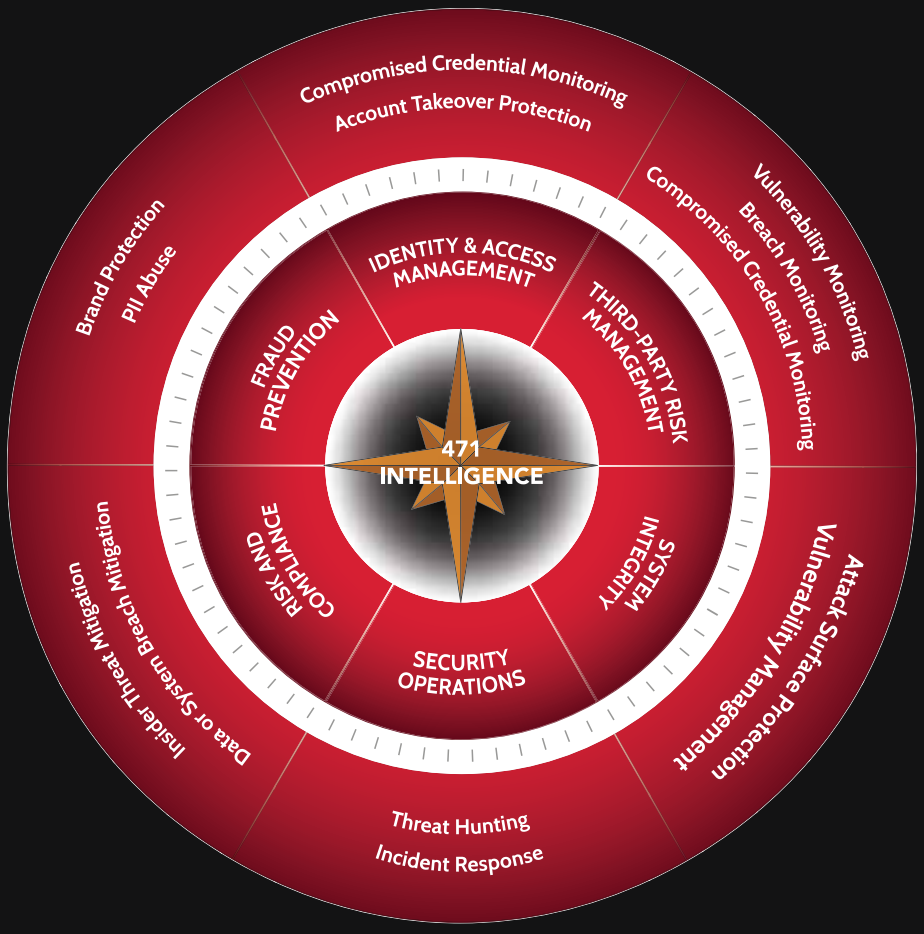
Among the key trends shaping the cyber underground, the situation in Ukraine and Russian-aligned hacktivism was a far more dominant force in 2022 than it has been in 2023 so far. The impact lessened as the most active groups redirected their attention to problems closer to home. Additionally, figurehead groups struggled for funding or to enact real disruption. While we expect hacktivism to remain troublesome, we assess the downward trend will continue.

Lastly, upward trends to note within the cyber threat landscape are law enforcement action and the growing interest in AI. With the prevalence of the aforementioned prominent threats, law enforcement will continue to take action against cybercriminal operations. Additionally, AI remains a top subject in the headlines, but we assess it has been minimally abused thus far. In the short term, AI will likely be leveraged for website-building capabilities to help threat actors quickly develop forums, marketplaces or sites. It also could be used for assistance in phishing and typosquatting activity. In the long term, we expect threat actors will persevere with their attempts to leverage large language models (LLMs) for more intricate cybercrime.

HOW INTEL 471 CAN HELP

Enterprises and government agencies leverage the Intel 471 centralized platform, TITAN, to deliver real-time insights from the cyber underground made easily accessible via our dashboards. Our customers rely on Intel 471 intelligence reports curated by our global team of analysts for complete visibility of their organization's threat landscape. We protect from costly security breaches and cyber incidents by solving real-world use cases including third-party risk management, security operations, attack surface protection, fraud and more.

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).



Intel 471's core competencies provide solutions to real-world use cases.

Cybercrime Underground General Intelligence Requirements Handbook

Three years ago, Intel 471 developed the CU-GIR. The framework is a baseline tool to assist in organizing, prioritizing, measuring and producing cyber underground intelligence. Central to this framework are General Intelligence Requirements (GIRs). GIRs provide a taxonomy of the threats and activities that pose risks to organizations – such as malware, vulnerabilities, access brokering, etc. – and the relevant questions around those activities that practitioners should focus on to create actionable intelligence products. By mapping their PIRs to this framework, organizations ensure relevant and measurable intelligence.

After years of feedback-driven development, we're excited to announce the initial open source release of the GIR framework on GitHub under the open source GNU General Public License v3.0. This allows practitioners to ingest the GIRs directly into their organizations' intelligence platforms and supercharge their threat intelligence programs. The CU-GIR framework is in JSON STIX version 2.1 format and the latest iteration of the framework, as well as historic versions, can be accessed directly from our GitHub.

Access to the GIR Handbook 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.

Intelligence Domains

Adversary Intelligence

Intel 471's Adversary Intelligence provides proactive and groundbreaking insights into the methodology of top-tier threat actors. This allows a better understanding of what threat actors are planning and attacking and how they operate. By learning the "why" and "how" of their behavior, you can proactively plan for, and help outwit, their attacks. Intel 471 provides ongoing automated collection, local human intelligence reporting and high-fidelity alerting of threat actors. We customize these results to your business, industry and geography, enabling you to make critical decisions based on trusted intelligence.

Credential Intelligence

Our Credential Intelligence delivers coverage across the entirety of the underground marketplace offering. Our clients are empowered to proactively monitor and mitigate the risk associated with compromised credentials as they hit the marketplace. We provide constant monitoring and notifying of compromised credentials, alerting you to breaches involving your employees, VIPs and customers, as well as third-party suppliers and vendors. We also aim to identify how leaks occurred, whether they are new and the scope of damage so you can take appropriate action. This allows you to mitigate the exposure of compromised credentials that could be used to impersonate users, gain unauthorized network access, steal data and commit fraud.

Malware Intelligence

The core of Intel 471 Malware Intelligence is our unique and patented Malware Emulation and Tracking System (METS). METS provides ongoing surveillance of malware activity at the C2 level, delivering near-real-time insights and deep context to its users. This allows you to actively track weaponized and productionized threats that could cause security breaches, revenue loss and customer harm; gain real-time monitoring of malware activity and C2 infrastructure that is paired with targeted human analysis; and access Intel 471's stream of technical indicators, campaign reporting and deep technical insights on top malware families. Use these to harden your defenses against the latest threats.

Vulnerability Intelligence

Our Vulnerability Intelligence offers an analyst-driven assessment of priority vulnerabilities. It is purposefully designed to offer both relevant and timely intelligence about the adversary scenario and lifecycle view of vulnerabilities, including weaponized and productionized threats. We provide ongoing monitoring and reporting of key vulnerabilities prioritized by risk and impact. This allows you to evolve your vulnerability management program with patch prioritization through the use of our Vulnerability Intelligence Dashboard in our TITAN platform to better understand how threats change and reduce your risks over time.

Marketplace Intelligence

Our Marketplace Intelligence offers insights into the most important and active underground marketplaces. Monitoring for stolen cards or compromised credentials and taking appropriate actions as soon as they are discovered is an effective way of preventing additional repercussions. Underground marketplaces are one of the areas where such items are routinely offered for sale and where threat actors go to obtain these items to facilitate their attacks. By illuminating the data being offered for sale in the top-tier marketplaces, Intel 471 helps customers detect when relevant items are being offered for sale and allows them to take measures to mitigate any impact that may follow from actors using these items in attacks.

Intel 471 arms enterprises and government agencies to win the cybersecurity war using real-time insights from the cyber underground.

Organizations leverage our cyber threat intelligence platform to protect from costly security breaches and cyber incidents by solving real-world use cases including third-party risk management, security operations, attack surface protection, fraud and more.

Your Voice of Reason and Truth

Intel471.com

1209 N Orange St
Wilmington, DE 19801