THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 21, 2024

2023 Annual Report

FOREWORD

When creating this annual report, we had two goals: to give you insight into the adversary's playbook and to assess future scenarios so that your organization can reasonably prepare for them.

In 2023, attack surfaces expanded, software supply-chain vulnerabilities were widely exploited, and the expanded use of generative AI increased the velocity of malicious content at scale.

Get insights from the adversary's playbook of tactics, techniques, and procedures (TTPs).

The report presents the industry's most comprehensive analysis of intelligence from 2023. It covers threat actors and their playbook of targets, methods, and attacks to help you eliminate blind spots in your current security posture. You'll discover how:

Threat actors exploited enterprise software at scale, as observed in CL0P ransomware group's attack on third-party managed file transfer (MFT) services such as Fortra's GoAnywhere and Progress Software's MOVEit.

Offensive tooling is increasingly targeting Linux and macOS systems: Ransomware kits continue to expand beyond Windows environments, facilitating an expanded range of victims.

Nation-states such as China-linked Spamouflage Dragon (tracked by Insikt Group as Empire Dragon) are already using AI-generated images to improve information operations (IO).

Recorded Future®

Prepare for upcoming threats with a roadmap for 2024 and beyond.

The report also offers our predictions regarding key vulnerabilities, third-party threats, extortion groups, and more for the year ahead. Wherever you are in your threat intelligence journey, you can use this report as a roadmap. It will help you strengthen your operations, create a forward-looking strategy, and protect your organization's data, intellectual property, and brand reputation.

Ransomware groups will likely increase their targeting of technologies supporting hybrid and remote work.

The "phishing" landscape will become the "spearphishing" landscape as generative AI helps attackers create particularized lures.

The rise of passwordless logins will likely drive criminal activity away from infostealers and back to email-based credential harvesting.

Levi Gundert
Chief Security Officer

Executive Summary

2023 was a year of unrealized expectations. A rumored global recession failed to materialize. The Ukrainian counteroffensive did not decisively shift the tide of its war against an invading Russia. Any movement toward Israel-Saudi rapprochement was significantly set back following the October 7 Hamas terrorist attack in Israel and the launch of a new war in Gaza. Despite the initial hype around ChatGPT, disruptive applications of generative AI are likely still years off.

Nonetheless, Insikt Group continued to track cyber threat actors capitalizing on this chaos and uncertainty to steal data, conduct espionage, and disrupt their geopolitical rivals. Occasionally, these objectives converged. Chinese state-associated threat actors increasingly targeted Taiwanese semiconductor companies to gain both an economic and political advantage in that industry. At the same time, profit-minded actors took advantage of the surge in hacktivism to sell tools (such as DDoS-as-a-service) or monetize "hack-and-leak" operations.

2023: The Year of the Enterprise Software Hack

While "zero trust" may be a buzzword in enterprise security, the reality is that the internet relies on trust now more than ever. The work-from-home era accelerated the adoption of "as-a-service" enterprise software, shared cloud infrastructure, and virtualized workspaces. As a result, even the most security-focused companies rely on a vast array of third-party services and tools to get work done.

Cybercriminals are taking advantage of this increasingly interconnected environment to amplify their attacks. The number of weaponized vulnerabilities in enterprise software increased fourfold from the previous year. Some of the year's most high-profile attacks targeting enterprise services, such as the MOVEit File Transfer Application exploit in May 2023, garnered attention due to the high volume of second- and third-party entities whose data was exposed. The ransomware gang behind MOVEit, CL0P, is estimated to have earned between $75 to $100 million in profit on that hack alone, suggesting these types of attacks will continue well into 2024.

Exploitation of enterprise software wasn't the only way threat actors took advantage of trusted technologies and services. Abuse of legitimate internet services — such as messaging platforms and cloud services — was detected in almost 25% of malware families in one Recorded Future study, allowing threat actors to hide their command-and-control (C2) communications by blending in with ordinary traffic. Threat actors also increasingly incorporated exploits for Linux and macOS operating systems into their attack sequences, breaching the "walled garden" and allowing ransomware to be deployed on a wider variety of systems. Finally, threat actors compromised business process organizations (BPOs) to facilitate SIM swapping and other social engineering scams.

Key Findings

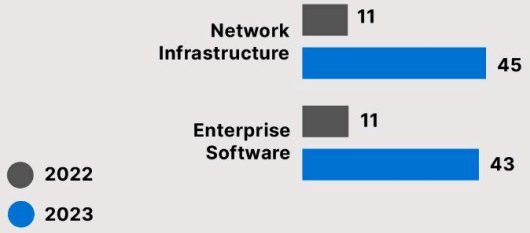
- **Expanding attack surfaces increased the opportunity for mass exploitation of vulnerabilities:** Throughout 2023, threat actors increasingly favored vulnerabilities that would allow the exploitation of multiple victim enterprises through a single vulnerability in a third-party product. The continued hybrid and remote work environment likely fueled this trend.
- **Early malicious use of generative AI focused on social engineering and influence operations:** Initial use cases for malicious use of generative AI have facilitated the creation of large amounts of convincing, fraudulent content. Modified versions of large language models (LLMs) for sale on the dark web have made it easier for users to evade safety guardrails on legitimate tools.
- **Software supply-chain attacks remain prevalent:** The increasingly interdependent nature of software has allowed threat actors to exploit third- and fourth-party dependencies in new ways, such as through the first double-software supply-chain compromise.
- **Criminals targeted business process organizations to facilitate social engineering:** Social engineering scams run through business process outsourcing (BPO) made it easier for criminals to commit fraud, such as SIM swapping.
- **Trusted tools are being abused through legitimate internet services:** Threat actors increasingly exploited trusted tools and services to gain access to an organization's infrastructure and remain undetected. This included abuse of cloud services for command-and-control.
- **Regulation abuse failed to take hold:** Ransomware and extortion campaigns experimented with new ways to coerce their victims into paying, including reporting their breach to regulators. However, the increased government scrutiny that followed likely made adversaries reconsider this extortion approach.
- **Offensive tooling is increasingly targeting Linux and macOS systems:** Ransomware kits continue to expand beyond Windows environments to provide the opportunity to exploit an expanded range of victims.
- **The war in Gaza increased hacktivist activity, capitalizing on chaos:** While most claims were false or exaggerated, hacktivist activity contributed to the terror and confusion surrounding the October 7 terrorist attack. Hacktivists are increasingly taking advantage of growing "grassroots" interest in their cause by selling exploits, DDoS-for-hire, and other services.
- **Valid accounts are increasingly being used for initial access, while phishing tactics evolve:** While phishing prevention measures have increased in sophistication, threat actors have adapted by adopting new phishing techniques and other initial access vectors, including valid accounts.
- **There is a convergence of influence narratives between ideological groups:** 2023 was characterized by an increasing convergence in narratives used in Chinese covert influence operations with narratives originating from the Russian disinformation ecosystem and US domestic violent extremists, coupled with an increased presence on alt-tech platforms.

Table of Contents

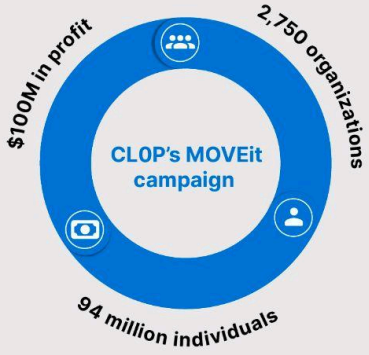
2023 by the Numbers

Increased Attack Surface Drives Mass Exploitation

Internet-facing appliances are a threat actors' best friend. This year saw an **increase in network infrastructure and enterprise software exploits**.



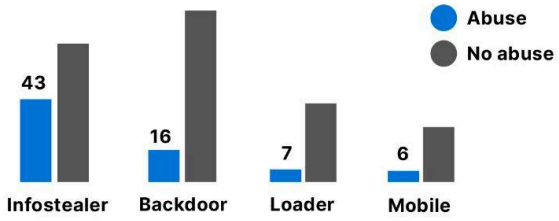
Called **"the biggest hack of 2023"**, CL0P's MOVEit campaign had far-reaching effects for organizations and industries globally.



Exploits of Legitimate Internet Services Take Advantage of Trust

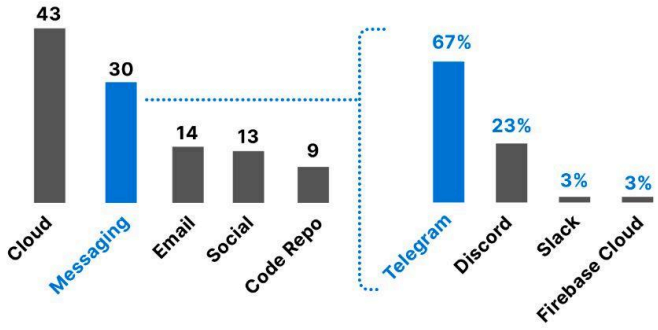
Malware

Infostealer malware most commonly exploited legitimate internet services (LIS). Among abused LIS, cloud services were the primary target, closely followed by messaging apps.



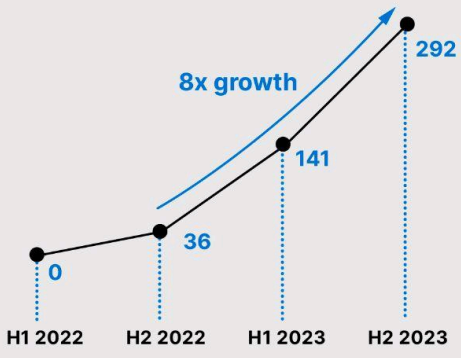
Services

Within messaging we can see Telegram and Discord are the leaders, but **Telegram is by far a fan favorite for attackers**.



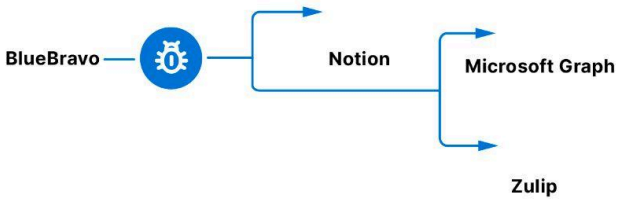
Hacktivist Resurgence

Mentions of DDoS-as-a-Service



DDoS-as-a-service mentions became significantly more common in the second half of 2023.

Examples of an APT abusing LIS



Active Hacktivist Groups
First 18 days

103 hacktivist groups were active within the first few weeks of the war in Gaza, compared to 25 active in the same time period following the invasion of Ukraine.

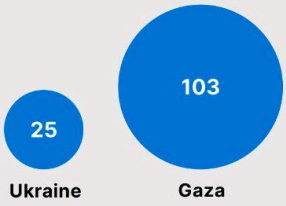


***Figure 1**: Metrics associated with key themes in the 2023 cyber threat landscape*

Section I: Setting the Stage: Technology, Geopolitics, Economics, and Policy

Major Technology Trends

It is nearly impossible to talk about trends in 2023 technology developments without acknowledging the ubiquitous discussions around generative artificial intelligence (AI) — specifically, following the release of products such as ChatGPT by OpenAI in November 2022. Immediate uses ranged from global companies debuting AI customer-facing chatbots to research developments in healthcare. We also saw developments in different kinds of AI models, like Microsoft's research on Explainable Boosting Machines, or AI models that focus on transparency for users to understand how a model reached its conclusion. Further discussion of artificial intelligence trends, specifically how threat actors are using AI, can be found in the **Evolution of Cyber Threats** section of this report.

In 2023, increased demand for services like cloud computing and generative AI drove vendors to seek increased computing power. Most organizations report deploying applications on at least two infrastructure-as-a-service platforms, while almost half (47%) follow a cloud-first strategy for deploying new applications in their enterprise. Reports estimate that OpenAI will require nearly 30,000 graphics processing units (GPUs) to meet customer demand, according to current projections. The expansion of cloud service providers (CSPs) to meet demand means that certain regions that are powerhouses for cloud computing data centers, like Southeast Asia, are increasingly strategically important locations for the technology industry as a whole.

Another trend in technology products, specifically in customer-facing applications, was increased offerings of passwordless authentication, such as through magic link logins. To balance security and convenience for users, some companies began to allow users and even employees to log into accounts (such as from Microsoft) using a link delivered to their inboxes. The use of magic links was accompanied by passwordless products launched by Google, which now allow users to sign into Google accounts using their phone's authentication methods.

Geopolitical Events: Global Conflicts Reshape Strategic Partnerships

In its second year, Russia's full-scale invasion of Ukraine entered a phase in which both sides wrestled to maintain their territorial gains and the world's wavering attention. As fighting continued unabated in 2023, both Russia and Ukraine faced threats of resource depletion, personnel shortages, and military offensives that have, at this point, failed to achieve their desired gains. For Ukraine, foreign aid saw more uncertainty this year than the year prior; the resounding tone of NATO's "unwavering" support for Ukraine took a conditional edge in 2023, with EU members flagging in their support for Ukraine, and US funding stalled in Congress. Meanwhile, the Kremlin turned to partners in Iran, China, and North Korea to secure weapons transfers and logistics. Russia is almost certainly emerging from 2023 emboldened

and continues to inject funds into its defense industrial base (DIB), reaching levels higher than any DIB investments since the end of the Soviet Union.

Exacerbating Ukraine's struggle to maintain its foreign aid from NATO partners is the threat of another geopolitical conflict: the Israel-Hamas War, which began with Hamas's kinetic terrorist attack on Israel on October 7, 2023. In response, Israel launched a military campaign in the Gaza Strip, supported by $3 billion in military aid from the United States (US). Fears of regional escalation continue to characterize the ongoing war, especially in light of fighting by Iran proxy forces at regional flashpoints, the most capable of which is Hezbollah, an Iran-backed Lebanese militia group. Meanwhile, Russia used the attack as an opportunity to reframe the violence as a direct result of failed US foreign policy initiatives in the Middle East. Moscow's growing ties to Iran have alienated its once-warming relationship with Israel, and in turn, have demonstrated once again Russia's direct ideological opposition to perceived Western (especially US) hegemony.

United through anti-Western bloc sentiment, China's strategic partnerships with both Russia and Iran played out in political, economic, and military areas throughout the year. Robust trade ties and shared geopolitical interests have forged a close relationship between Iran and China, and China has continued to extend military and economic support to Russia in its ongoing invasion of Ukraine. That said, China's "peace plan" for Ukraine signaled an attempt to keep the US and Europe from alienating it due to its association with Russia. Meanwhile, the US continues to see China as a "competitor" and a "challenger"; this relationship has been exemplified in the last year in a series of tariffs and controls on microchip technology.

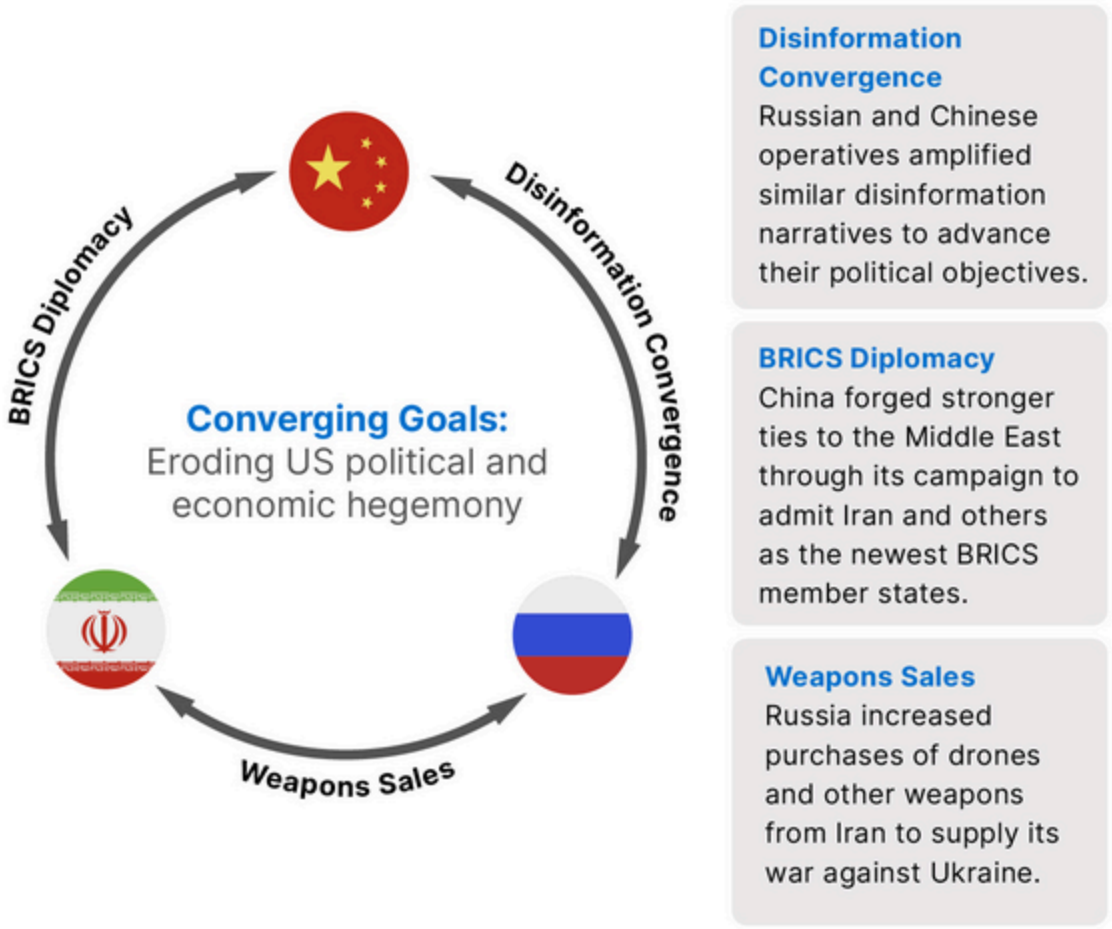


***Figure 2**: The trilateral relationship between Russia, China, and Iran is based on converging goals*

Macroeconomic Trends

Entering 2023, the macroeconomy faced headwinds marked by an ongoing global health crisis, growth slowdowns, geopolitical uncertainty, and shifting trade alliances. A wave of mass layoffs also began in the first quarter of 2023, spurred by efforts to readjust after hiring sprees over the previous couple of years. This downsizing hit the technology sector the hardest, with 260,000 jobs lost in 2023. For cybercrime, a sudden pool of unemployed workers exposes prospective job seekers to scam campaigns preying on job uncertainty and job-seeking platforms, and — from a tactical standpoint — exposes the technology sector to the potential loss of talent and innovation.

International businesses and corporate decision-makers were forced to reconcile with the cyber and non-cyber effects that geopolitical events are having on the macroeconomy. China's cyber-espionage program, for example, has become more mature, stealthy, and coordinated over the past half-decade. This year, Chinese cyber threat groups conducted focused geopolitical targeting on strategic technologies, defense industries, governments, and critical infrastructure, all of which are industries in line with China's continued striving for military modernization and regional hegemony. Continued

economic sanctions on Russia by the West have fractured the global market, placing supply chains under growing tension. In some instances, corporations had to choose between Western and Russian markets based on perceived support to either Ukraine or Russia and were the target of cyberattacks or "hack-and-leak" operations as a result of their decision to leave the Russian market.

Cyber Policy's Uphill Battle

In cybersecurity law enforcement, 2023 was a major year of law enforcement takedowns against cybercriminal operations, including ransomware extortion domains as well as dark web forums and marketplaces — primarily in the context of an explicit strategy from the US Department of Justice to focus on direct takedowns versus prolonged investigations. These takedowns were the result of coordinated international efforts by countries including the US, the UK, Germany, and others. While many operations had immediate success in taking down cybercrime infrastructure, replacements eventually popped up in their place. As a result, it remains unclear whether or not these takedown efforts will result in long-lasting reductions in criminal activity levels, or if these actions serve more as an international show of force.

Plenty of sector-specific cybersecurity regulations emerged in 2023, particularly in the US, which affected the transportation and healthcare sectors, among others. With more regulation planned for 2024, the White House is eyeing a set of minimum cybersecurity hygiene standards for entities in the healthcare sector (mirroring other sector-specific efforts). But perhaps one of the most anticipated cyber policy developments this year was the finalization of the Securities and Exchange Commission's (SEC) regulations for covered entities to report incidents of "materiality" within four business days, following industry feedback that stretched back to mid-2022. While the full effects and implications of this regulation have yet to be seen (especially in the face of reconsideration from some US lawmakers), early examples of effects include companies that reported a drop in stock prices on the same day they reported attacks.

On the other hand, we also observed a focus on regulating cybersecurity in all industries. While Singapore's cybersecurity law was originally focused on regulating critical infrastructure industries (CII), in late 2023, it proposed amendments to add more requirements for CII while also expanding its scope to regulate more non-CII entities. In Brazil, the country's national telecommunications agency (ANATEL) updated a national regulation that tightened an existing minimum security requirement for covered entities by adding specific requirements, including password requirements and software vulnerability updates. Both cases are examples of national governments fine-tuning landmark cybersecurity policies that, at the outset, were likely too broad to effectively regulate cybersecurity requirements. At the global level, the UN's ad hoc cybercrime committee failed to vote on a final treaty text that would set international legal standards to combat cybercrime following negotiating sessions in 2023, meaning that the committee will now have to add an extra session's worth of work to attempt to pass a viable international treaty.

Additionally, we observed two examples of cyber threat actors using extreme extortion tactics, in the form of reporting victims to their respective regulatory agencies. Threat actors reported the victims

under the pretext that because the threat actors were able to breach the victims, the latter had subpar cyber defenses and were, therefore, not in compliance with various regulations. However, we assess that this extortion tactic is unlikely to become commonplace, and is more likely based on garnering public attention. This trend is further discussed in the **Extortion Trends** section of this report.

Section II: Cyber Threat Intelligence

Evolution of Exploited Vulnerabilities

Expanding Attack Surfaces Increase Opportunity for Mass Exploitation of Vulnerabilities

In 2023, threat groups successfully exploited several vulnerabilities at scale in singular third-party tools (GoAnywhere, MOVEit, and Citrix NetScaler devices) to inflict widespread damage on thousands of organizations. Increasing instances of successful mass exploitation in recent years can be explained, in part, by two factors: enterprises' increasingly complex and difficult-to-manage attack surfaces, driven by a widespread transition to hybrid work and cloud computing; and increasingly sophisticated ransomware groups that are improving their strategies and tradecraft, including the development and exploitation of zero-day vulnerabilities. Some security researchers have also suggested that enterprise software, like that targeted in numerous mass exploitation events this past year, makes a good target because the software is updated in periodic maintenance cycles that are not conducive to real-time patch deployment.

The most notable instances of mass exploitation this year were carried out by the CL0P ransomware group (CL0P) on two third-party managed file transfer (MFT) services, Fortra's GoAnywhere MFT and Progress Software's MOVEit MFT. In a particularly concerning case study, from May 2023 to mid-August 2023, CL0P attacks on MOVEit alone are estimated to have affected a staggering 2,750 enterprises and approximately 94 million individuals. CL0P first exploited the vulnerabilities that enabled these attacks as zero-days, prior to their disclosure and patching, and then systematically exploited those vulnerabilities after they were remediated, as organizations struggled to identify the vulnerabilities in their systems and apply a patch. CL0P's development of zero-day exploits prior to their disclosure and patching likely assisted in the rapid staging and successful exploitation of those vulnerabilities, even after their disclosure.

In another notable example of mass exploitation, from August to December 2023, both nation-state and ransomware threat actors exploited Citrix Bleed (CVE-2023-4966), affecting NetScaler ADC and NetScaler Gateway devices, to carry out successful attacks on hundreds of organizations. Again, ransomware groups accounted for the majority of reported attacks, including prominent groups like LockBit gang, Medusa gang, and ALPHV.

There are some commonalities among product vulnerabilities that enable mass exploitation. Each case of mass vulnerability exploitation observed this year had the following characteristics in common:

- The vulnerabilities were discoverable via public scans of internet-facing infrastructure, setting threat actors up for easy vulnerability discovery and exploit deployment.
- The vulnerabilities were exploited before they were publicly known (as a zero-day) and patched, and they continued to be widely exploited after being disclosed, as enterprises struggled to patch them.

While zero-day vulnerabilities are cause for concern, it should be noted that in most instances of mass exploitation, successful attacks took place after a vulnerability was disclosed and patched. This trend probably reflects different levels of resourcing for victim organizations. While some organizations have sophisticated security programs, implementing behavioral analytics to combat the exploitation of zero-day vulnerabilities, many organizations still struggle to implement the patch management measures necessary to prevent the most basic opportunistic attacks. Recent Microsoft research suggests that 99% of cyberattacks can be prevented through basic security practices like maintaining a strong patch management program, the application of zero trust principles, the use of extended detection and response (XDR) solutions, and the use of multi-factor authentication (MFA).

Technology Product Types That Were Repeatedly Exploited

The increased virtualization and migration to the cloud are driving more dependency on a narrowing supply chain of vendors, introducing new security risks to the enterprise environment. Aligning with a trend from 2022, threat actors continued to target vulnerabilities in operating systems across major software vendors such as Microsoft, Google, Apple, and Cisco in 2023, as befits their high market share. However, compared to high-risk vulnerability exploitation observed in 2022, we observed increasing instances of active exploitation targeting vulnerabilities in enterprise software and network infrastructure in 2023. **Figure 3** shows an approximately 290% rise in the number of vulnerabilities exploited in attacks against enterprise software in 2023 compared to 2022, both by volume and by individually targeted software. Due to the prevalent use of these products in enterprise environments, these high-risk vulnerabilities can be exploited to provide widespread unauthorized access to corporate environments and the sensitive data that ransomware groups desire. Similarly, we saw a 309% increase in the number of vulnerabilities exploited in attacks against network infrastructure.

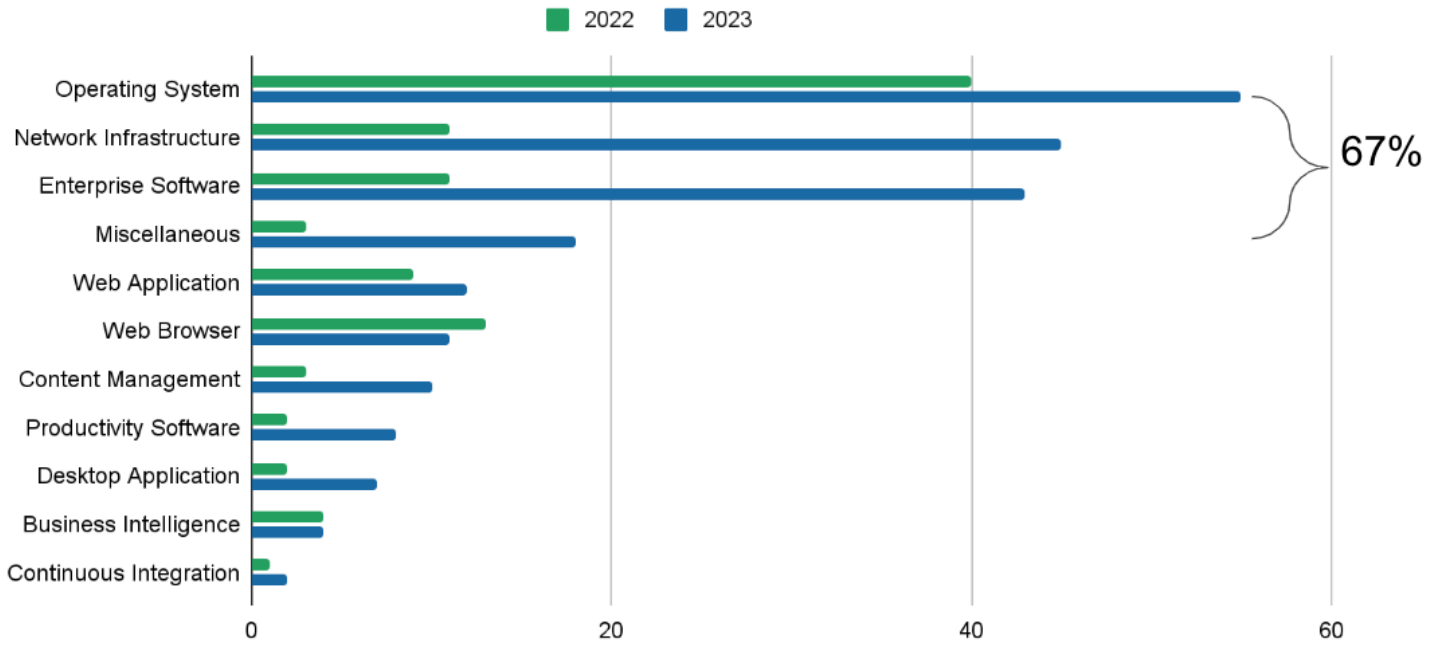


Figure 3: *High-risk vulnerabilities actively exploited in 2022 and 2023 per the Recorded Future® Intelligence Cloud*

Several ransomware threat actors deliberately targeted vulnerabilities in file transfer software as part of their extortion operations. The most prominent example of this trend is CL0P's data theft campaign targeting Progress Software MOVEit Transfer instances vulnerable to CVE-2023-34362. Other similar instances involved CL0P, ALPHV, and LockBit's exploitation of CVE-2023-0669 affecting GoAnywhere secure managed file transfer (MFT) software, as well as Reichsadler's exploitation of CVE-2023-40044 in Progress Software's WS_FTP Server. Additionally, IceFire and Buhti were observed exploiting CVE-2022-47986 affecting IBM's Aspera Faspex file-sharing solution. In hindsight, file transfer platforms are an obvious target for ransomware groups — they can contain high volumes of sensitive data, and they offer the potential to compromise organizations at scale.

In 2023, ransomware groups, including the newly identified ALPHV ransomware gang UNC4466, also exploited vulnerabilities in backup software for initial access to networks. UNC4466 targeted Veritas Backup Exec, a data recovery solution for small and medium businesses, exploiting three vulnerabilities that were patched in 2021. Cuba ransomware gang attacked critical infrastructure organizations in the US and IT firms in Latin America by exploiting a newer, but already-patched vulnerability, CVE-2023-27532, in Veeam Backup & Replication, Veeam's proprietary backup application developed for virtual environments. Although CVE-2023-27532 was patched in March 2023, Cuba Ransomware Gang conducted the campaign in June 2023. By exploiting CVE-2023-27532, the threat actors were able to extract credentials from configuration files, enabling access to the backup infrastructure hosts.

Evolution of Cyber Threats

Early Malicious Use of Generative AI Focuses on Social Engineering, Influence Operations

Generative artificial intelligence (AI) is a paradigm-shifting technology that is already widely used; for example, over 95% of smartphone users have used AI through the use of voice assistants like Alexa or Siri. The breakout of generative AI in 2023 has led to a surge in new services — while defenders have experimented with AI for threat intelligence, incident response, and code patching, cybercriminal and nation-state threat actors are experimenting with novel ways to enable and amplify their tactics using AI.

Currently, the most tangible risks associated with generative AI are linked to influence operations, social engineering, data privacy breaches, and intellectual property violations. Security researchers have observed threat actors using AI-powered chatbots to craft convincing phishing emails, support scam operations, and analyze e-commerce merchants' anti-fraud systems to facilitate payment fraud. More sensationalized fears, such as AI autonomously developing and executing complex cyberattack strategies, remain largely speculative and have not been observed in the wild.

An emerging concern still not fully understood is the potential misuse of uncensored LLMs. A study by Indiana University conducted at the end of 2023 uncovered fourteen LLMs for malicious services that were generally advertised as subscription services similar to ChatGPT Plus, and 198 malicious open-source LLM projects advertised on the dark web. Many of these models advertise the ability to produce malware, create phishing emails, and construct ready-to-use scam sites. However, it must be reiterated that there have not yet been definitive, comprehensive studies on the real-world use or impact of AI-created malware, phishing, or scam sites.

While it is almost certain that threat actors will eventually be able to exploit AI for more sophisticated attacks, this capability will take time to mature. Like legitimate practitioners, cyber threat actors almost certainly had to wrestle with generative AI's limitations in 2023, such as "hallucinations", processing power, context window limitations, and the need for problem- and sector-specific datasets. The complexity of effectively integrating AI into advanced cyber threat operations requires not just access to LLMs, which is now nearly ubiquitous, but also a deep understanding of how they work and a unique skillset in using them. Threat actors will require knowledge of advanced prompt engineering techniques, as well as access to models that can process large context windows before they will be capable of being used for truly advanced cyber operations. Consequently, the cybersecurity community has a window of opportunity to prepare and adapt to these emerging threats. The timeline necessary for threat actors to reach AI-enabled operational maturity will vary significantly across threat types, with state-sponsored threat actors almost certainly already employing AI and cybercriminals likely experimenting with advanced uses in order to develop more capable malware.

Third-Party Threats

Software Supply-Chain Attacks Remain Prevalent, Evolving

In 2023, Insikt Group identified an 11.8% increase (from 2022 to 2023) in reported software supply-chain attacks. PyPI and npm package managers retained the top spots as the most frequently targeted technologies by cybercriminal threat actors, suggesting a focus on the development stage of the software supply-chain cycle to deploy infostealers. North Korean threat actors also demonstrated how supply-chain attacks can benefit nation-state espionage and theft operations in support of geopolitical objectives, by targeting software products by 3CX, Jetbrains, and CyberLink to deploy malware.

Software supply-chain compromise continued to involve known techniques, such as impersonating legitimate packages, and to be largely used to distribute malware and steal information and cryptocurrencies. That said, we observed two trends showcasing the attack vector's evolving nature. First, throughout 2023, threat actors used novel techniques to conceal malicious packages and increase the chances of infection. This involved the likely first supply-chain attack against PyPI to take advantage of Python bytecode (PYC) execution for obfuscation, probably chosen as a target because security products often scan exclusively for Python source code (PY) files and because using PYC can prevent malicious code from being flagged and blocked. Threat actors also used abandoned Amazon S3 buckets associated with historic versions of the package manager bignum to spread data-stealing malware, likely to take advantage of such buckets' capacity to scale operations.

While the above software supply-chain attacks highlight the one-to-many nature of many of these attacks, attackers can exploit software supply chains in a more targeted fashion. For the first time, in 2023, cybercriminals targeted the banking sector with npm packages designed to attach malicious functionalities to specific components in the online resources of the targeted banks to intercept data and steal customer login information.

Lastly, 2023 also saw the first instance of a double-software supply-chain compromise. This occurred in a supply-chain compromise attack that targeted 3CX Desktop App software and was attributed to North Korea's nation-state threat actor Lazarus Group. Lazarus Group's compromise of 3XC was reportedly initiated by a previous software supply-chain compromise involving a trojanized software installer of the X_TRADER trading platform hosted on the Trading Technologies website. Taken together, the software supply-chain threat landscape demanded that companies increasingly account for third- and fourth-party dependencies in their security strategies.

Criminals Target Business Process Organizations to Facilitate Social Engineering

In 2023, we observed several instances of cybercriminals specifically targeting business process outsourcing (BPO) organizations in what were almost certainly financially motivated attacks. BPO organizations are likely prime targets for cybercriminals due to their criticality to supply chains. By

targeting BPO organizations, threat actors increase their ability to compromise many downstream customers through a single point of compromise.

More specifically, Scattered Spider sought to gain access to mobile carrier networks from compromised telecommunications or BPO environments to perform SIM swapping and further facilitate criminal operations beyond the primary victims, such as cryptocurrency theft. The motivations behind the uptick in SIM swapping attacks observed in recent years have almost certainly led to the surge in attacks on BPOs, given these companies' integral relationship with telecommunications providers. Another factor likely explaining the observed targeting of BPOs in 2023 is their increased access to corporate data — companies have been increasingly using BPOs as an option to optimize costs, gain access to specialized skills, and help ensure business continuity. Given that the BPO market is expected to grow from $266.8 billion to $544.8 billion between 2023 and 2032, targeting of this sector will likely grow as well over the next decade.

Trusted Tools Abused Through Legitimate Internet Services

In 2023, threat actors abused legitimate internet services (LIS) to host malware and blend C2 communications with legitimate traffic, lowering the chances of detection. Per recent Insikt Group research, roughly 25% of over 400 malware families currently abuse LIS in some way as part of their C2 infrastructure. Infostealers are most likely to use LIS for C2 infrastructure, due to their data exfiltration objectives and ease of infrastructure setup. Cloud storage platforms were the LIS most commonly abused, followed by messaging applications such as Discord and Telegram. Payment fraud offered threat actors another use case for abusing messaging applications, particularly when relaying Magecart e-skimmer payloads and exfiltrating stolen data. GitHub was also featured as a commonly abused platform in 2023.

Although the current absence of comparable reporting and datasets makes it difficult to quantify or even demonstrate a clear trend, it is likely that abuse of LIS is increasing and evolving, driven partially by threat actors' increasing focus on the software supply chain. Several malware families have gradually incorporated LIS in their infrastructure in recent years, and it has become common for more recent commodity infostealer families and malicious PyPI packages to abuse LIS, especially for C2 communications. Also, in December 2023, ReversingLabs reported on a novel technique whereby malware hidden in a PyPI package abused GitHub commit messages for C2 purposes.

Nation-state groups also showed creativity and rapid innovation in abusing legitimate services to mask malware communications. In January 2023, Insikt Group reported that GraphicalNeutrino, a malware attributed to BlueBravo, a threat actor that overlaps with Russian nation-state groups APT29 and NOBELIUM, abused the US business automation service Notion for its C2. A few months later, in July and August 2023, Palo Alto's Unit 42 and EclecticIQ reported observing APT29 using new techniques for C2 that involved the abuse of Microsoft Graph API and the open-source chat and collaborative software Zulip.

Extortion Trends

Regulation Abuse Fails to Take Hold

New cyberattack disclosure rules from regulators in the US and Europe in 2023 were feared to cause a widespread shift in tactics from extortion groups, but so far, such a shift has not materialized. In the US, the SEC proposed new rules in July 2023 requiring publicly traded companies to report cyberattacks with a "material" impact on business operations to the SEC within four days of one occurring.

Several months later, in November 2023, the ALPHV (BlackCat) ransomware gang reported financial software company MeridianLink to the SEC for allegedly violating the new disclosure rule after the group posted an extortion notice for MeridianLink on its dark web ransomware extortion blog. While MeridianLink confirmed that it suffered a cybersecurity breach (and claimed that no unauthorized access to its network actually occurred), the organization was not in violation of the new SEC rule because the rule had not yet taken effect at the time ALPHV reported MeridianLink to the regulator.

In the wake of ALPHV's notice to the SEC about its alleged attack on MeridianLink, cybersecurity researchers awaited indications that other ransomware groups were implementing this technique, or that ALPHV was reporting additional victims to the SEC. But in the nearly two months since the MeridianLink incident and news of the SEC's plans were first publicized, there have been no other reported incidents like the one involving ALPHV and MeridianLink. Although another ransomware gang threatened in the summer of 2023 to report companies to regulators in Europe for alleged violations of the General Data Protection Regulation (GDPR) — the EU's comprehensive privacy law — if they did not comply with attackers' ransom demands, this technique is not being widely adopted or repeatedly used.

Offensive Tooling Increasingly Targets Linux and macOS Systems

Due to Microsoft Windows' widespread global use in both home and enterprise environments, most malware and offensive tooling is aimed at Windows rather than macOS or Linux and other Unix-like operating systems (OSs). However, reporting shows that cyberattacks and malware targeting Linux and macOS systems increased from 2022 to 2023. For macOS, Objective-See reported that at least 21 new malware families or variants surfaced in campaigns targeting macOS environments, compared to just 13 new macOS malware families in 2022. For Linux platforms, reporting from Trend Micro showed a 62% increase in ransomware detections on Linux systems when comparing the first half of 2022 to the first half of 2023. Threat actors transitioning to developing malware in programming languages that are compatible with multiple OSs, such as Rust, is likely a large contributing factor to increased targeting of both macOS and Linux. Additionally, Linux has become increasingly popular in servers, cloud environments, and critical infrastructure, which are attractive targets for threat actors endeavoring to steal sensitive data, disrupt services, or launch large-scale attacks. This shift in TTPs is indicative of threat actors' continued opportunism and desire to expand their pool of possible targets, particularly as the user base of these platforms continues to increase over time.

In 2023, TTP instance notes, which analyze tools and TTPs potentially used by adversaries, published by Insikt Group contained 81 references to macOS, Linux, or Unix-like OSs, a 79% increase from 17 references in 2022. Of the TTP Instance notes published in 2023, 55 of them pertained to either offensive tools and exploits available for download from code repositories or malware samples observed in the wild. There were 41 TTP Instance notes that discussed offensive tooling targeting Linux and Unix-like OSs (including multi-platform tools and malware). Echoing Trend Micro's research, the prevalence of ransomware targeting Linux and Unix-like OSs was the one clear trend emerging among these notes, with 22 ransomware families mentioned targeting Linux, Unix, or ESXi. Several of these families were known to previously only target Windows environments, but added Linux, Unix, or ESXi variants to their toolkits in 2023, including Cactus, CL0P, Babuk, Monti, Akira, Agenda, Rhysida, and IceFire. We also observed ransomware families that solely target Linux environments, such as Buhti, Dimorf, and Ransomwhere. Finally, in 2023 we also observed newly discovered ransomware operations, like NoEscape, targeting both Windows and Linux platforms since their inception.

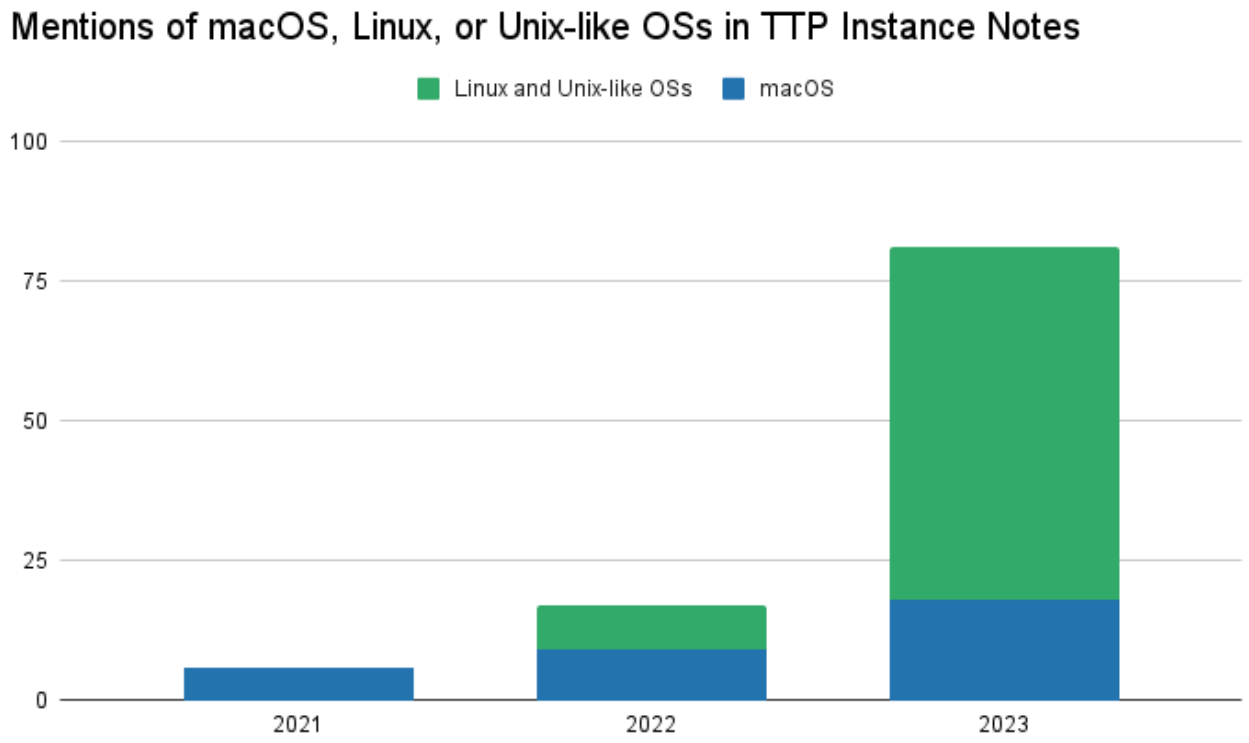


Figure 4: *References to macOS, Linux, or Unix-like OSs in TTP Instance notes over the last three years (Source: Recorded Future)*

Insikt Group published fifteen TTP Instance notes in 2023 related to offensive tooling or exploits targeting macOS environments. Several of these overlapped with the malware families highlighted in Objective-See's aforementioned research, namely Turtle, PureLand, JaskaGo, ObjCShellz, SparkRAT, and XLoader. We published individual TTP Instance notes on the macOS information stealers SparkRAT, MetaStealer, and Atomic in June 2022 and January 2024, all of which are mentioned in Objective-See's

research as well. PoC exploits targeting macOS vulnerabilities such as CVE-2023-41993, CVE-2023-32407, and CVE-2023-32422 were also prevalent.

Multiple threat groups added macOS malware to their arsenal in 2023, akin to the trend we observed of ransomware operations extending their reach to Linux and Unix-line OSs. In November 2023, researchers at Jamf Threat Labs attributed macOS malware ObjCShellz to BlueNoroff, a North Korea-sponsored APT group known for financially motivated attacks targeting cryptocurrency exchanges, venture capital firms, and banks. Based on public reporting, the debut of ObjCShellz marks a novel expansion into macOS malware for BlueNoroff. Similarly, the first samples of a macOS variant of LockBit ransomware surfaced publicly in April 2023. To date, no attacks involving the LockBit macOS variant have been reported in the wild. However, the aforementioned sample showed signs that the variant was still experimental; the sample has the execution password "test" and does not implement any exfiltration or persistence techniques. The LockBit group was in operation for over two years before its first variant targeting Linux/ESXi surfaced in the wild, and it is possible the macOS variant is still in development.

Gaza War Increases Hacktivist Activity: Capitalizing on Chaos

The year 2023 saw an acceleration of hacktivist activity associated with ongoing and emerging geopolitical conflicts. Similar to the surge in grassroots and state-sponsored activity we observed after Russia's invasion of Ukraine in 2022, the latter half of 2023 saw an unprecedented rate of emergence of new hacktivist groups and alliances taking advantage of the chaos following the October 7 attack against Israel by Hamas. These groups targeted both Israeli and Palestinian entities with distributed denial-of-service (DDoS), website defacement, and data leak attacks. Insikt Group noted that an overwhelming majority of claims by these actors, mostly regarding claims of compromising critical infrastructure, emergency services, and government websites, were false or exaggerated in impact.

However, we observed several incidents that did demonstrate notable effects, including AnonGhost's compromise of Israel's RedAlert application to send false notifications of an incoming nuclear attack; Anonymous Sudan's attack against The Jerusalem Post, which resulted in website downtime; and Cyber Av3ngers' attack on an Irish town's water system, which targeted Israeli-made operational technology (OT) devices and resulted in a two-day water outage. The Israel-Hamas war also saw the reappearance of self-proclaimed hacktivist groups Moses Staff and Predatory Sparrow from hiatus, the latter of which has a reputation for effective cyberattacks against Iranian critical infrastructure; indeed, on December 18, 2023, the group took responsibility for a cyberattack that took 70% of gas stations in Iran offline.

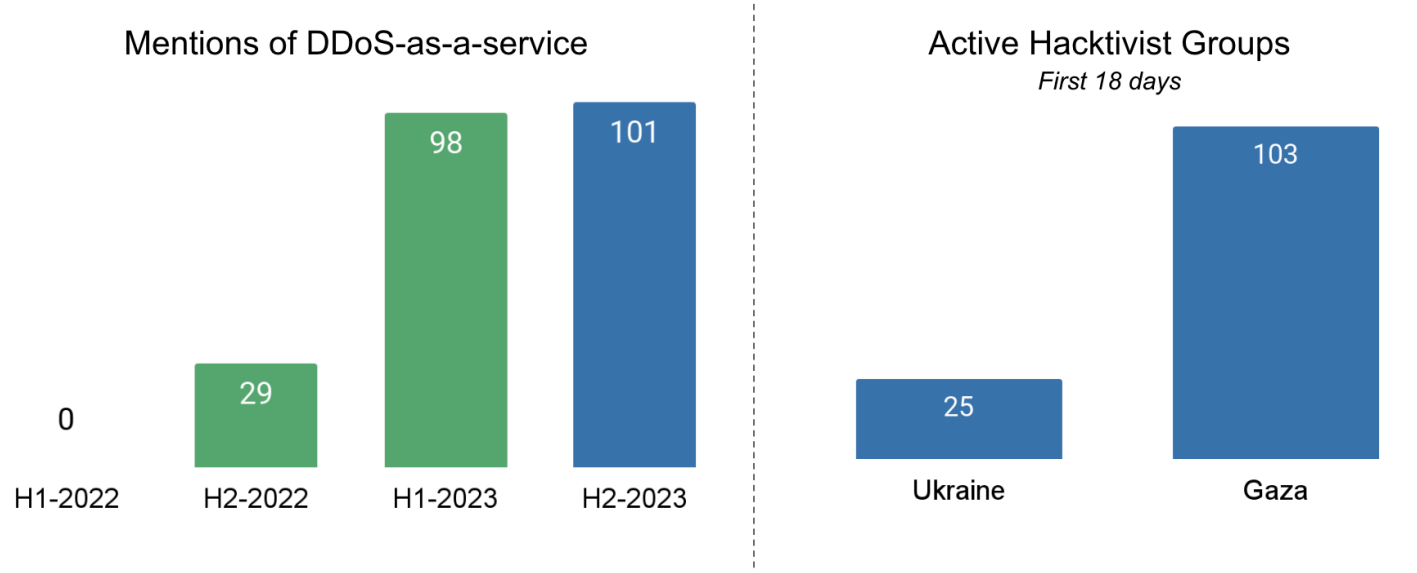


***Figure 5**: Mentions of DDoS-as-a-service between 2022 and 2023 and the number of hacktivist groups active within the first eighteen days of the Ukraine/Gaza wars (Source: Recorded Future)*

Furthermore, cybercriminal actors appeared to increasingly take advantage of the geopolitical instability and "grassroots" interest in hacktivism. Several groups in the latter half of 2023 adopted TTPs more traditionally associated with cybercriminals than hacktivists, selling or sharing credential leaks, especially personally identifiable information (PII) affecting Israeli and Ukrainian nationals, as well as continuing the previously observed tradition of selling exploits and DDoS-for-hire services (as done by Anonymous Sudan and UserSec). Killnet, for example, has been known to expand its hacktivism into several minimally successful financial, educational, and ideological cybercriminal side projects, such as operating a cryptocurrency exchange, and launching both a Russian cybercriminal forum and a cybercrime-focused education platform in January and May 2023, respectively. In another instance, in June 2023, Anonymous Sudan, Killnet, and REvil appeared to announce collaborative plans to attack European financial institutions, though there has since been no evidence of such an attack taking place.

DDoS attacks, website defacement, compromised infrastructure, and exploitation of public-facing applications were the most prevalent hacktivism-related TTPs in 2023. Notably, unlike pro-Russian hacktivist groups, whose activity is almost exclusively confined to claiming responsibility for alleged DDoS attacks and website defacements, numerous hacktivist groups operating out of the Middle East and Southeast Asia employed a broader range of TTPs, including "hack-and-leak", vulnerability exploitation, and even the deployment of destructive wiper malware. Killnet originally claimed responsibility for the December 2023 wiper attack against Kyivstar, which resulted in the shutdown of Ukraine's largest telecom provider; however, it was later revealed that Solnstepek (known to have links to Russian APT Sandworm and the GRU) was responsible for the attack, consistent with the more technically capable nature of Russian APT actors compared with hacktivists and reflecting Killnet's attempt to falsely capitalize on the fear, uncertainty, and doubt (FUD) associated with the attack. Russian groups were also observed to increasingly promote attacker infrastructure services, likely a

further testament to their integration into the more technically advanced Russian-language cybercriminal community.

Valid Accounts Increasingly Used for Initial Access, While Phishing Tactics Evolve

Among the initial access methods Insikt Group observed in 2023, phishing, external remote services, and the use of valid accounts stood out for their high volume of reported attacks, effectiveness, and adoption of new and evolved trends.

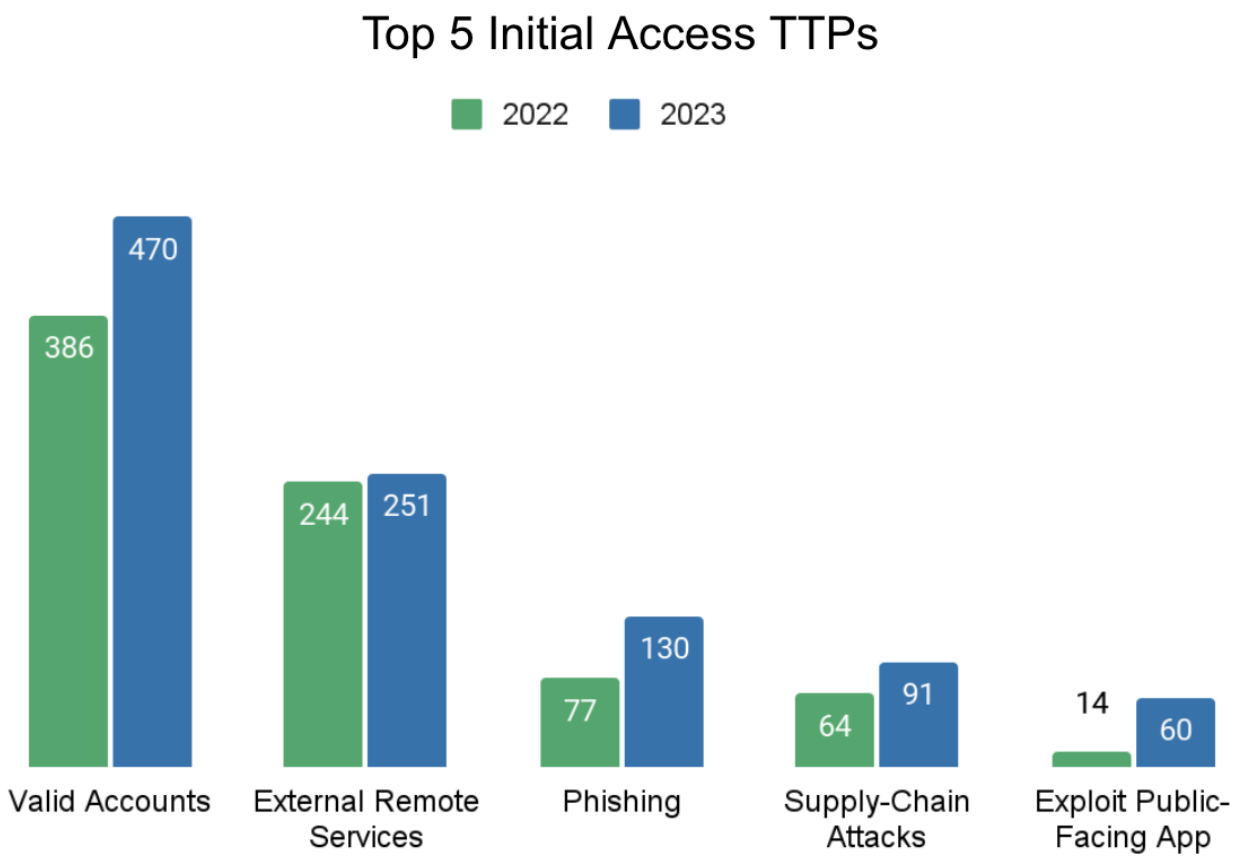


***Figure 6**: Top five TTPs used to gain initial access in validated cyberattacks (Source: Recorded Future)*

In 2023, cybercriminals and nation-state actors increasingly used a variety of file formats in phishing attacks to evade detection by email security systems and adapt to the evolving security environment. Similar to what we observed in 2022, malicious attachments using archive formats included the prevalent use of ZIP and RAR archive formats. These formats, especially when password-protected, help conceal malicious content from web proxies, sandboxes, and email scanners. Additionally, attackers extensively used HTML formats, like Compiled HTML Help (CHM) and LNK files. These formats are often ignored by email security software due to their common, benign use in regular

communications. CHM attachments disguise malicious scripts, while LNK files can prompt trusted Windows applications to download malware, further reducing detection risk.

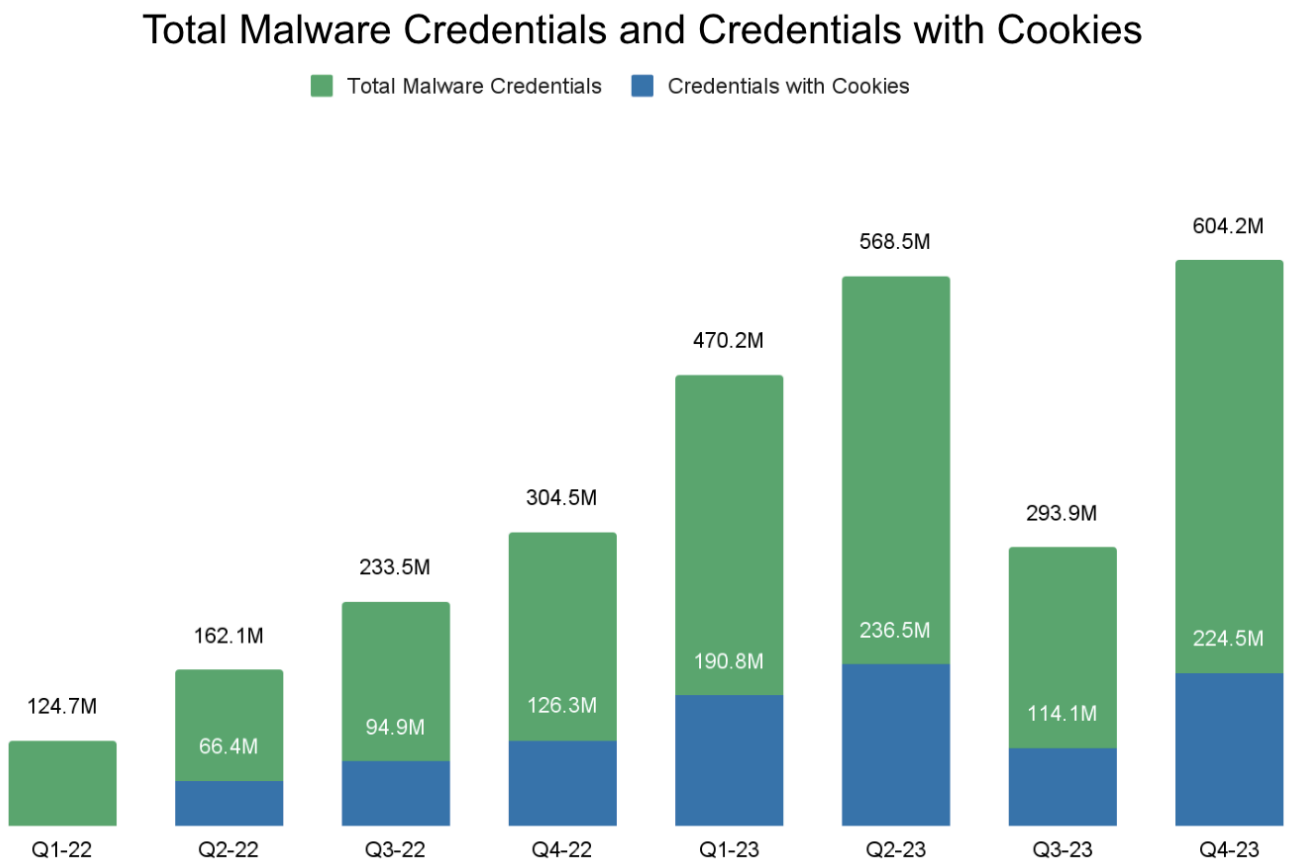


***Figure 7**: Stolen credentials observed in Recorded Future malware logs (Source: Recorded Future)*

By utilizing the Recorded Future® Identity Module and malware logs, we have observed an increased volume of valid accounts available to threat actors, who could use these accounts to bypass MFA. In 2023, there was a notable 135% rise in the overall number of harvested credentials and a 166% increase in credentials associated with cookies. We acknowledge that this increase partly results from the expanded source collection within the Recorded Future intelligence index. Nonetheless, the upward trend depicted in our graphs does correlate with a general rise in successful cyberattacks.

Security controls on email technologies have also prompted threat actors to find alternative means to distribute malware or redirect victims to phishing websites, such as QR code phishing (quishing), smishing (SMS phishing), and corporate messaging applications. Threat actors have also increased their abuse of legitimate internet services (LIS), such as Github Pages, to distribute malware payloads during phishing campaigns. In a parallel process, threat actors extensively leveraged legitimate programmatic advertising technology within a growing malvertising-as-a-service ecosystem to

distribute phishing pages and malware payloads as part of a greater effort to support payment fraud. Broader adoption of two-factor and multi-factor authentication (2FA/MFA) has almost certainly led threat actors to conduct a greater proportion of adversary-in-the-middle (AitM) and MFA fatigue attacks parallel to phishing campaigns.

Converging Influence Narratives Between Ideological Groups

2023 was the year of new records in covert influence operations. Companies such as Google, Meta, and TikTok all disclosed takedowns for some of the largest influence networks ever seen on their platforms, including Doppelgänger and Spamouflage Dragon. Both influence networks also displayed early signs of adopting generative AI.

Russia-linked Doppelgänger is very likely one of the most persistent covert influence networks currently operating. Between October and December 2023, Insikt Group observed 130 domains amplified by over 5,000 accounts linked to Doppelgänger. The operation is likely situated as part of broader Russian information operations targeting Ukraine, European partners, and the US. This broader operation involved the use of TikTok accounts attempting to highlight corruption in the Ukrainian government and fake celebrity quotes to erode domestic support for Ukraine in Europe and the US. Doppelgänger was observed using AI-generated text on a website targeting US politics. The lack of use of AI-generated text across a broader range of Doppelgänger-operated assets suggests that the use of generative AI remains limited, and has yet to be systematized across broader Russian influence efforts.

China-linked Spamouflage Dragon (tracked by Insikt Group as Empire Dragon) continued its high-volume, low-engagement operations. The network saw a notable acceleration of information operations from August 2022 onwards, with an increasing convergence in narratives used in Chinese covert influence operations with narratives originating from Russian disinformation.

Election influence has also become a priority for the Empire Dragon network. In addition to the network's targeting of Canadian elected officials, Insikt Group also observed attempted influence operations targeting Hong Kong's local elections in December 2023 and the Taiwanese presidential elections in January 2024. Additionally, Insikt Group observed Empire Dragon accounts using AI-generated images in a limited capacity during the Hong Kong elections.

***Figure 8**: Generative AI uploaded by Empire Dragon accounts during the Hong Kong local elections (Source: Recorded Future)*

Both Russian and Chinese covert influence networks have illustrated a strong intent in manipulating audiences in connection with their respective governments' geopolitical objectives, which we assess will almost certainly include influencing the outcome of the 2024 US elections. In such a scenario, influencers' objectives would likely focus on eroding domestic sentiment toward providing political and military support for Ukraine and Taiwan. While Russia and China may have different approaches to influencing the election outcome depending on the presidential candidates, both will almost certainly look to undermine the democratic process and increase political polarization ahead of the election.

Section III: Reflections on 2022 Predictions

Assessing the accuracy of past predictions is a crucial part of the intelligence lifecycle and facilitates the formulation of new predictions and assessments. In the graphic on the following page, Insikt Group reflects on three major predictions from the 2022 Annual Report, which have globally stood true, although with several nuanced developments.

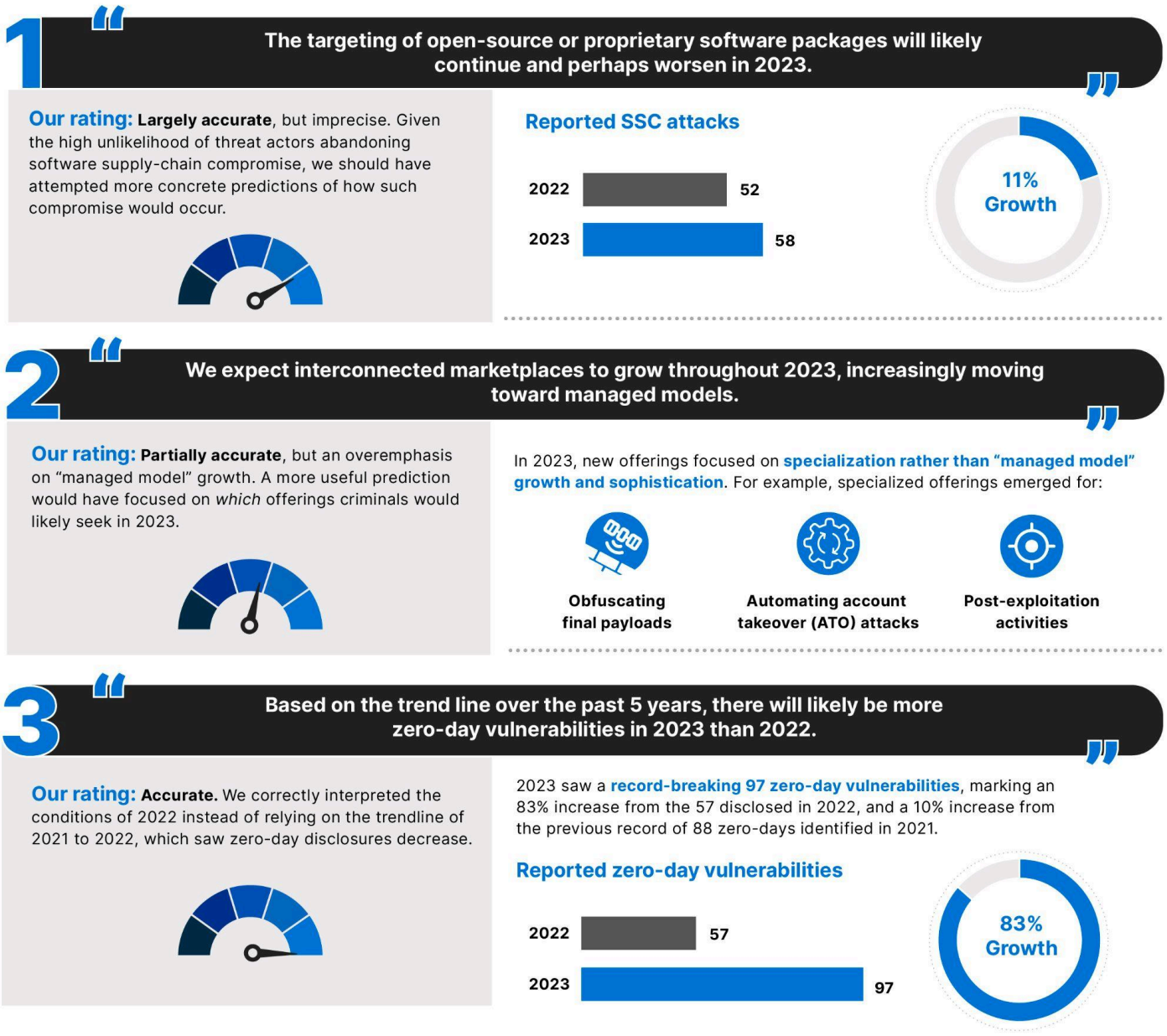


***Figure 9**: Reflections on three major predictions from our 2022 Annual Report*

Section IV: Outlook

Predictions about the future of cybersecurity face two major problems:

- Predicting too safely and therefore not providing information of much value
- Predicting too aggressively and therefore pushing defenders' attention in misguided directions

Faced with this dilemma, our preference for 2024 is to err more on the side of aggression than caution, since we would rather that our assessments increase the chances that defenders stay ahead of newer or less-reported threats. We do this because we believe that specific, even potentially disagreeable, assessments are usually more useful when developing effective cybersecurity strategies than generic statements aligning with well-known attributes of the threat landscape.

With those considerations in mind, here are our predictions for the cyber threat landscape in 2024, which include our predictions about larger contextual effects on that landscape, such as geopolitics and regulations.

Cyber Threat Landscape

- **Vulnerabilities:** Given ransomware groups' (especially CL0P's) success in mass exploiting vulnerabilities in enterprise file transfer solutions to carry out thousands of successful attacks (Accellion: 2020, 2021; GoAnywhere and MOVEit: 2023), we predict that at least one ransomware group will carry out a successful compromise of hundreds of targets via exploiting vulnerabilities in an enterprise third-party file transfer service in 2024. The impact from this event will be comparable to the MOVEit campaign from 2023.
- **Third-party threats:** In 2024, we expect to see software supply-chain attacks dominate the third-party threats landscape by number and severity of attacks, with at least a 15% growth in reported incidents. npm will highly likely continue to attract the most targeting due to its ubiquity and volume of new packets published.
- **Extortion groups:** As more companies adopt and sustain hybrid and remote work models, we expect that extortion groups will increasingly target technologies supporting and securing hybrid and remote work, especially cloud-based data storage, MFA solutions, and virtual private networks (VPNs), and that the majority of ransomware attacks will involve attacks against such assets.
- **Hacktivism:** We anticipate that shifts in the tides of the Russia-Ukraine war are likely to result in the strategic diversion of hacktivist activity from groups such as Killnet and Anonymous Sudan toward the war in Gaza, particularly as the conflict threatens to spill over elsewhere in the region. Targeting of Western entities aligned with NATO and the European Union will likely continue, while focus on entities supporting Israel will likely increase.
- **Initial access methods:** In 2024, we expect that attackers are likely to increasingly focus on stealing credentials and identities using techniques like password spraying and credential stuffing as organizations bolster their security perimeters. We also expect that the "phishing"

threat landscape will increasingly become the "spearphishing" threat landscape as criminals gain more experience and resources to utilize generative AI to craft highly personalized campaigns that are difficult to detect.

- **Information operations:** As we enter a year of high-profile and numerous elections worldwide, we anticipate the public's awareness of deepfakes and disinformation operations will be more disruptive than the aims or activity of adversary-driven campaigns, particularly in highly polarized electorates such as the US. Voters will likely be conditioned to write off unflattering images or press as artificially generated (regardless of authenticity).

Contextual Landscape

- **Technology:** Companies are almost certain to increasingly offer passwordless logins to users in 2024, such as access links to sign into websites and biometric-based authentication. This shift will greatly reduce the value of certain leaked credentials for sale on the dark web and will force threat actors to innovate to find new ways to exploit passwordless security, such as the creation of fake access link emails. For money laundering and external, customer-facing payment fraud threats, increasing reliance on passwordless logins may drive a shift away from account takeover (ATO) tactics toward new account fraud (NAF).
- **Geopolitics:** Should China's domestic economic performance worsen and become a more salient talking point on the global stage, it will likely use social surveillance and censorship to quell unrest in its own population. In its external relations, China may pre-position disruptive cyber operations to signal its continued fortitude and deter its adversaries (like the US) from taking advantage of its internal instability; however, it is unlikely China would "lash out", such as by initiating a noisy diversionary conflict or war. Iran will continue to rely on a mixture of proxy warfare and cyber influence operations to sow unrest in the region, including efforts to isolate Israel and oppose the US military's presence in the region. Russia will very likely exploit perceived "war fatigue" among Western nations to influence public opinion ahead of elections in the US and EU and will wait for election results to determine its next course of action in relation to its war in Ukraine and its relationship with the West.
- **Regulations:** The increase in vulnerability exploits will drive lawmakers to shift from regulating software safety to reforming software liability law. This would make it easier for consumers to take legal action against software companies that produce insecure code; however, determining what counts as coding negligence will be a significant challenge for policymakers. In response to ongoing policies and regulations for AI, AI companies will likely shift toward synthetic data for training their models to avoid privacy and copyright issues, speed up development, and reduce the chances of data poisoning from threat actors.

Appendix A: Top Exploited Vulnerabilities in 2023

Vulnerability	Affected Product	Description	Risk Score	CVSS
CVE-2023-44487	Any product that uses the HTTP/2 protocol	The HTTP/2 protocol allows a denial-of-service (server resource consumption) because request cancellation can reset many streams quickly. Fixes are vendor-specific.	89	7.5
CVE-2023-34362	Progress Software MOVEit Transfer	A SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.	89	9.8
CVE-2023-23397	Microsoft Outlook	Elevation of privilege vulnerability	89	9.8
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway	A sensitive information disclosure vulnerability that allows an attacker to read large amounts of memory after the end of a buffer	89	9.8
CVE-2023-21716	Microsoft Office (Word)	Microsoft Word remote code execution vulnerability	99	9.8
CVE-2023-24932	Microsoft Windows 10, 11, Server	Secure Boot security feature bypass vulnerability	99	6.7
CVE-2023-28206	Apple macOS, iPhone OS, iPadOS	An out-of-bounds write issue was addressed with improved input validation. An app may be able to execute arbitrary code with kernel privileges.	99	8.6
CVE-2023-2868	Barracuda Email Security Gateway Firmware	A remote command injection vulnerability that can enable remote code execution	99	9.8
CVE-2023-38831	RARLAB WinRAR	RARLAB WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive.	99	7.8
CVE-2023-41990	Apple macOS, iPhone OS, iPadOS	Apple-only ADJUST TrueType font vulnerability that allows remote code execution through a malicious iMessage attachment. Exploited in Operation Triangulation.	99	7.8
CVE-2023-43177	CrushFTP	CrushFTP prior to 10.5.1 is vulnerable to Improperly Controlled Modification of	99	9.8

Vulnerability	Affected Product	Description	Risk Score	CVSS
		Dynamically-Determined Object Attributes.		
CVE-2023-47565	QNAP QVR Firmware 4.0	An OS command injection vulnerability that can allow authenticated users to execute commands via a network	99	8.8
CVE-2023-4863	Google Chrome, Mozilla Firefox	Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out-of-bounds memory write via a crafted HTML page.	99	8.8
CVE-2023-4911 (Looney Tunables)	GNU glibc on x64 Fedora Red Hat Enterprise Linux	Buffer overflow vulnerability that can allow RCE with elevated privileges	99	7.8
CVE-2023-7024	Google Chrome	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	99	8.8

***Table 1**: Top high-risk vulnerabilities disclosed in 2023 (Source: Recorded Future)*

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com