THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 2, 2023

2022 Annual Report

The annual report surveys the threat landscape of 2022, summarizing a year of intelligence produced by Recorded Future's threat research team, Insikt Group. We analyze global trends and evaluate significant cybersecurity events, geopolitical developments, vulnerability disclosures, and more, providing a broad, holistic view of the cyber threat landscape in 2022.

Executive Summary

The physical conflict in Ukraine, and the effects it has had on the cyber threat landscape throughout 2022, frames our discussion of significant cyber threat events and geopolitical trends that occurred in 2022 and underscores the increased convergence of the cyber and geopolitical threat landscape.

Before and throughout the physical invasion, Recorded Future has observed increased instances of distributed denial-of-service (DDoS) attacks, hacktivist activity, and the widespread deployment of wiper malware. And while Russia's invasion of Ukraine dominated the discussion of kinetic and cyber-hybrid operations, threat actors affiliated with other prominent nation-states, specifically Iran, China, and North Korea, carried out cyberattacks throughout the year, informed by an era of heightened geopolitical tension, competition, and politically charged affiliations.

We also analyzed cyber threat events across the broader threat landscape, including those carried out by cybercriminal groups. While phishing campaigns and ransomware attacks continue to plague organizations across industries and geographies, Recorded Future identified a 600% increase in the number of credentials sold via information stealing malware between Q1 and Q4, a significant year-over-year increase in targeting of software frequently used in organizations' supply chains, and a shift toward an increasingly managed service model as "as-a-service" offerings proliferated on dark web marketplaces and underground forums. Initial access brokers are increasingly active, likely due to the increased use of infostealer malware and the ability to monetize stolen data.

The effective use of infostealers often relies on the successful exploitation of vulnerabilities. Notable vulnerability-related trends in 2022 included ransomware and Chinese state-sponsored threat actors rapidly exploiting zero-day vulnerabilities, the ongoing exploitation of Log4Shell across all quarters in 2022, and the impact of Microsoft's oscillation about the automatic disablement of macros.

Finally, ransomware remained an ever-present threat in 2022. While certain ransomware gangs disbanded, others were quick to assert their dominance and used their significant resources to undertake campaigns against organizations of all sizes across industries. Although ransomware payments decreased by about 60% between 2021 and 2022, likely due to increased guidance from governments to forgo making ransomware payments and increased due diligence on cybersecurity standards from insurance companies when underwriting policies for ransomware attacks, ransomware will continue to pose a major threat to organizations throughout 2023.

Key Takeaways

- Self-proclaimed hacktivist activity, likely a mix of grassroots and state-sponsored activity, surged in the first half of the year, as threat actors groups carried out attacks based on their allegiance to either Russia or Ukraine. While the majority of this activity was limited to targeting organizations involved in the conflict or located in areas close to eastern Europe, some hacktivist activity involved organizations in other regions.
- Spillover effects of the deployment of wiper malware and the hacktivist activity were the primary cyber threats to organizations not directly involved in the war in Ukraine.
- North Korea will most likely continue to test ballistic missiles in 2023. US military buildup in the western Pacific and increased defense spending and preparedness measures in Japan are likely to be met with equivalent actions by China.
- Diplomatic negotiations over the Joint Comprehensive Plan of Action (JCPOA; commonly referred to as the Iran nuclear deal) are unlikely to make any progress. Meanwhile, the Islamic Republic of Iran continues to enrich uranium in an effort to achieve a nuclear weapon. The Israeli government is likely to continue kinetic strikes on elements of the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF) operating in Syria while keeping its options open for strikes on nuclear facilities inside of Iran.
- 2022 was the year of "as-a-service", as we identified the presence of new phishing-as-a-service (PaaS) offerings in the threat landscape, the continued success of the ransomware-as-a-service (RaaS) model, and the development and use of new strains of malware-as-a-service (MaaS) offerings.
- Open source or proprietary software packages were targeted throughout 2022. Given their effectiveness over the past year, these types of attacks will likely grow in severity in 2023.
- Infostealers were increasingly used by threat actors, and the increased advertisement of authentication information collected by infostealers poses a risk to multi-factor authentication (MFA) security solutions.
- While the adoption of countermeasures such as the disablement of macros by default has been highly effective, many threat actors have also pivoted their operations to subvert newly developed or implemented security protections, underscoring the need for a implementation of a defense-in-depth security strategy.
- The exploitation of widely used products, as well as continued exploitation of previously reported vulnerabilities like Log4Shell, underscores threat actors' ongoing focus on attack vectors that can be used for extended periods of time.
- The volume of ransomware attacks is unlikely to shrink in 2023. However, if the finance gain from ransomware attacks continues to decrease, as observed from 2021 to 2022, threat actors are likely to adjust their tactics to continue realizing the historical financial incentives for ransomware attacks.

Table of Contents

Section I: Geopolitical Intelligence

Geopolitical tension, advancing technology, and an intensely interdependent global economy are conditions that have created a world in which no cyber activity is siloed. Cyber operations, especially when combined with kinetic activity, have far-reaching and indirect effects on the public and private sector. What drives these cyber operations varies geographically, insofar as cyber activity mirrors the nations that wield it.

While Russia's invasion of the Ukraine in early 2022 may dominate the discussion of kinetic and cyber hybrid operations, throughout the year several other prominent cyber events have occurred, spurred by 3 other key players in cyberspace: Iran, China, and North Korea. All 4 of these big players take cyber actions informed by the current era of heightened geopolitical tension, competition, and politically charged affiliations.

Russia

Russia's Invasion of Ukraine: Recurring Failures Expose Russian Weaknesses, Bolster Ukrainian Resolve

What began as offensive cyber actions taken by the Russian government towards Ukraine, including DDoS attacks targeting government websites and banks and an intensified military presence at the Ukrainian-Russian border in early February 2022, culminated in Russia's military invasion of Ukraine on February 24, 2022. Since then, hacktivist, cybercriminal, and state-backed groups have launched cyber offensives to support either Russia or Ukraine in the war. Despite Russia's well-resourced cyber apparatus, composed of hacktivist and state-sponsored groups, its influence operations throughout the course of the invasion have not been as profound as some cybersecurity experts predicted. Meanwhile, Ukrainian advances, on and off the battlefield, have been a surprise.

Key Players in Russia-Ukraine War

Self-proclaimed hacktivist groups have actively participated in the Russia-Ukraine war, with grassroots and state-sponsored threat actors conducting cyber operations on behalf of their own or their respective governments' objectives. In particular, the pro-Russia hacktivist group Killnet targeted organizations in several Western countries allied with Ukraine, launching DDoS attacks against several state websites, including those of the European Parliament, the Bulgarian government, the Italian government, and various US states. While the longstanding effects of these DDoS attacks have been limited, Killnet has been successful in crafting and publicizing a pro-Russia narrative both for its followers on Telegram and in the Western media. On the other side of the conflict, anti-Russian hacktivist groups like Anonymous and IT Army of Ukraine have acted on behalf of Ukraine. For example, Anonymous leaked data sourced from Russia's Ministry of Culture in April 2022.

Outside of hacktivist groups, the Russian Foreign Intelligence Service (SVR) employed its well-resourced arsenal of threat groups throughout 2022 to advance its strategic aims and policy goals in the Russia-Ukraine war. For instance, the Russian APT group UAC-0113 (linked with moderate confidence to Sandworm Team) masqueraded as telecommunications providers to target Ukrainian organizations, among others, beginning in August 2022. In March 2022, Russia-aligned Lorec53 (Lori Bear, UAC-0056) launched a phishing campaign aimed at Ukrainian public entities, as well as a cyberattack against a Ukrainian energy provider. Finally, BlueBravo (APT29, Cozy Bear, The Dukes, UNC2452), launched a phishing campaign aimed at European diplomats in November 2022.

Decreased Sophistication, Increased Breadth: The Cyber Lead-Up to Russia's Invasion of Ukraine

In the leadup to Russia's full-scale invasion of Ukraine, Russia launched 4 phases of offensive cyber events against Ukrainian targets. Between each phase, Russian state-sponsored and state-nexus cyberattacks decreased in coordination and technical sophistication but increased in the number of attackers and targets. The first wave began in mid-January of 2022, igniting concerns that Russia was launching cyberattacks ahead of a full-scale invasion of Ukraine. The second wave began in mid-February, with further concentrated and coordinated cyber activity. During the third wave, consisting of the 2 days before to Russia's invasion of Ukraine, cyberattacks escalated again in preparation for Russia's kinetic assault. Finally, the fourth wave comprised the cyberattacks on February 24, 2022, the day of Russia's full-scale invasion of Ukraine. The types of attacks varied throughout each phase and included website defacement, DDoS, destructive malware (such as wipers), phishing, and fraudulent SMS. Of all the Russia-backed destructive wiper operations since the start of the invasion in February 2022, 55% affected Ukrainian critical infrastructure. Additional notable cyber events related to the Russia-Ukraine War can be found in Appendix A below.

Targeting and Pace of Russian Cyber Operations May Shift in 2023

While threat actor groups affiliated with Ukraine have focused their efforts on targeting organizations in Russia, Russian-aligned groups have targeted a broader array of victims, carrying out attacks against organizations and government bodies in Ukraine as well as countries that have publicly announced their support for the Ukrainian cause. In one case, Russia's Iridium (Sandworm Team) deployed Prestige ransomware against both Ukrainian and Polish transportation and logistics networks in October 2022. About a month later, Killnet claimed responsibility for a DDoS attack against the European Parliament after the agency proclaimed Russia a sponsor of terrorism. Such events display that cyberattacks on Ukraine's allies are in some instances targeted, not just the result of spillover activity. Underscoring the strain that this by-association targeting puts on Ukraine's neighbors and allies, Poland's security agency released a statement in December 2022 that the country has been a "constant target" of pro-Russian hackers since Russia's military invaded Ukraine.

More recently, Russia has been employing "quick and dirty" methods, aiming for edge devices (such as firewalls, routers, and email servers) and maintaining a quick operational tempo to outpace detection. Russian threat actors have emphasized maintaining persistence, sometimes targeting the same entity multiple times. From the onset of its invasion, Russia used an array of multifaceted wipers and ransomware in its cyberattacks against Ukrainian entities. To support its fast-paced incursions, Russia shifted from these complex wipers to a simpler strain, CaddyWiper, which infected 5 Ukrainian organizations from May to June 2022 and another 4 in October 2022.

With an emphasis on speed, careless errors or execution failures have rendered some of the cyberattacks sloppy or unsuccessful in achieving their destructive aims, like Sandworm's failed attempt to deploy CaddyWiper and ZeroWipe malware on Ukraine's national news agency (following a similar thwarted attack in April 2022). Similarly, quick kinetic strikes have been plagued by coordination blunders, enabling Ukrainian militants to push back against Russian ground forces and even intercept communications to expose Russian military intelligence.

Despite these missteps, we can expect that an emphasis on speed and repeated targeting of the same entity will be a continuing strategy of Russian influence operations, as Russia struggles to find where it can collect real-time intelligence and gain power in the ongoing conflict.

In months ahead, we expect Russia to continue to target critical infrastructure and logistical hubs for arms that aid the Ukrainian war machine. Echoing this sentiment, Microsoft cautioned that Russian attacks over the winter, which we have surged in recent months, would continue to merge cyber operations and kinetic campaigns to weaken Ukrainian resources and resolve.

Russia-Ukraine War Creates Ripple Effects for Geopolitical Movements

Over the last year, the geopolitical landscape changed in response to the uncertainty and lessons learned from the Russia-Ukraine war. Altered relationships between countries and a heightened risk of war have further complicated the analysis and forecasting of geopolitics. For instance, Chinese operations throughout 2022 showed an interest in collecting any information on relevant stakeholders to determine what actions to pursue and when to pursue them, as would be expected of a prominent country in times of volatility [1, 2, 3]. Russia will likely seek to strengthen ties with allies, including Belarus, China, Iran, and North Korea, as a result of increasing geopolitical isolation. These partnerships, if lasting, pose numerous threats to Ukraine and the broader international community.

China

Chinese Cyber Threat Activity Maintains Steady Tempo in 2022

Chinese APT and cybercriminal activity remained at a steady high level throughout 2022, on par with the aggressive cyber espionage programs we have seen from Chinese threat actors in recent years. Chinese state-sponsored groups have traditionally been highly active in targeting China's rival territorial claimants, such as in the South China Sea and India, as well as Taiwan, with the operational tempo often mirroring increased geopolitical tensions. China has been assertive in its approach to managing international relationships; in pursuit of its own national defense, political security, international standing, and territorial integrity, the Chinese Communist Party (CCP) regularly engages in a wide range of coercive behavior. China uses its cyber capabilities both against regional targets like Taiwan, India, and Afghanistan as well as against larger strategic adversaries abroad, namely the US.

The COVID-19 pandemic has greatly influenced the Chinese government's policies at home and abroad in 2022. As part of a scheduled rollback of its "zero COVID" policies, but also in response to widespread protests in November 2022 over lockdown requirements, the Chinese government began loosening COVID-19 restrictions on December 7, 2022. Prior to this, the zero COVID policies, which restricted movement and strictly enforced a disease control strategy, bred impatience and discontent among citizens. Rather than China's aggressive stance showcasing the superiority of centralized control (as Xi likely intended), Western nations (for all their faults handling the virus) have fared no worse than China. Instead, China faces frustrated civilians, low GDP growth (only 3% in 2022), and now rising cases of COVID-19 in a country with low levels of immunity. Now, the Chinese government is unlikely to take risks without further intelligence-gathering efforts, internally and externally, to avoid potential misjudgments and make informed projections.

Trends in Chinese Infrastructure and Capabilities

Despite the large number of distinct Chinese state-sponsored groups currently active, there are notable overlaps in the infrastructure and capabilities across groups. For infrastructure, this included increased adoption of compromised internet of things (IoT) devices for operational infrastructure, alongside continued trends in preferred virtual private server (VPS) providers used by Chinese state-sponsored actors. For capabilities, Chinese state-sponsored actors consistently exploit zero-day and publicly disclosed vulnerabilities in internet-facing corporate appliances for initial access and share exploit and malware capabilities between groups. Regardless of their specific modes of operation, Chinese cyber operations typically aim to acquire intelligence in order to achieve asymmetric advantages over government adversaries, target minority groups inside and outside of China, and help the Chinese government gather intelligence about potential domestic threats.

Compromised IoT devices as operational infrastructure: High-tier Chinese state-sponsored threat activity groups are increasingly amassing large anonymization networks, typically built from compromised internet of things (IoT) devices, such as small or home office (SOHO) routers and network devices, for use as operational infrastructure. These networks can also allow threat actors to rapidly cycle infrastructure and use internet service provider (ISP) IP addresses geolocated in the same country as targeted entities. Specific examples of this trend include TAG-38 activity targeting Indian critical national infrastructure, RedBravo (APT31) activity targeting European governments, and TAG-51 (BlackTech) targeting entities within Taiwan and Japan.

Zero-day and rapidly weaponized vulnerabilities targeting public-facing appliances: In 2022, Chinese state-sponsored threat actors increasingly exploited zero-day vulnerabilities in external-facing appliances and rapidly adopting publicly disclosed exploits [1, 2, 3]. This activity focused on internet-facing corporate appliances such as Mail Servers (like Zimbra, Microsoft Exchange), VPN products (like Pulse Secure and Citrix), Firewalls (Sophos XG), and other external-facing appliances (such as Zoho ManageEngine, Atlassian Confluence, Log4J, and F5 BIG-IP). The exploitation of these vulnerabilities is commonly followed by the use of publicly available web shells, such as China Chopper, Godzilla, or BEHINDER Rebeyond [1, 2, 3]. More information about this trend can be found in the vulnerability section below.

Sharing of capabilities across multiple distinct state-sponsored groups linked to the People's Liberation Army (PLA) and the Ministry of State Security (MSS): Distinct threat activity groups associated with China's military and civilian intelligence organizations commonly share custom malware families and exploit code, with prominent examples including ShadowPad, Winnti, PlugX, and Royal Road, as well as zero-day exploits like ProxyLogon and CVE-2022-1040 [1, 2, 3].

Use of open source and offensive security tooling: Like many other threat actors, Chinese state-sponsored groups have increasingly adopted publicly available capabilities, including offensive security tooling, public exploit code, and other open-source malware. In particular, Recorded Future has regularly observed Chinese state-sponsored groups use offensive security frameworks such as Cobalt Strike and BEHINDER (1, 2); proxy tools such as Fast Reverse Proxy (FRP) and Stowaway [1, 2, 3, 4], VPN software such as SoftEther VPN [1, 2], and scanning tools such as FScan and Acunetix [1, 2, 3].

Growing Concern over China's Aggression in Asia-Pacific Region

Beijing is likely watching and learning from Russia's ongoing military invasion in Ukraine, particularly Russia's struggles on the battlefield, and reevaluating the feasibility and wisdom of taking Taiwan by force. Nevertheless, China's leadership remains committed to achieving unification with Taiwan, through force if that is ultimately necessary.

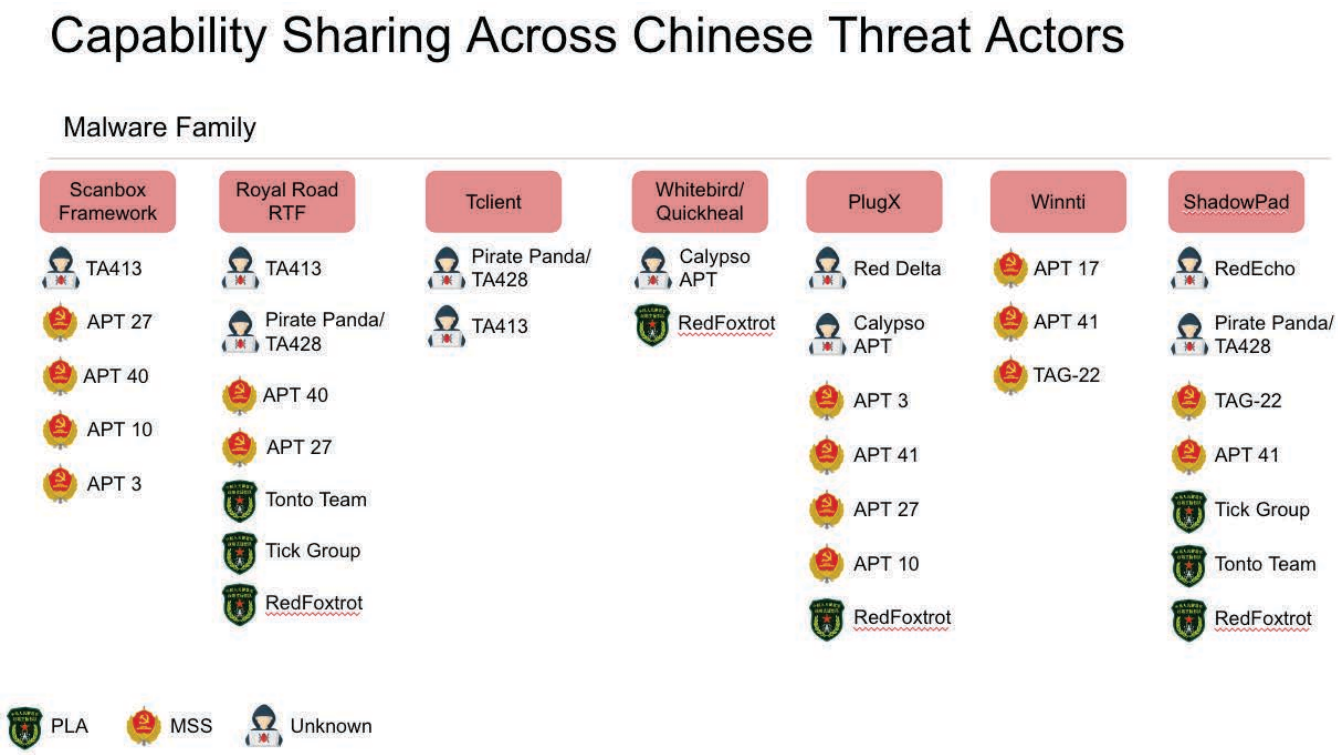

Figure 1: *Malware families used by multiple Chinese threat actors (Source: Recorded Future)*

Figure 2*: Zero-day vulnerabilities exploited by multiple Chinese threat actors (Source: Recorded Future)*

Throughout 2022, China-linked cyber threat actors carried out various cyberattacks against Taiwan in an attempt to assert China's claim over the territory and have continued to display an interest in attacking critical infrastructure. In November 2021, Insikt Group reported on a series of ShadowPad network intrusions targeting integrated circuit and semiconductor equipment manufacturers, logistics, and other manufacturing organizations in Taiwan. Additionally, Cycraft researchers identified a BRONZE RIVERSIDE (APT10, Stone Panda) campaign from November 2021 to February 2022, dubbed "Operation Cache Panda", that targeted software systems of Taiwanese financial institutions. In a separate instance identified in February 2022, Chinese state-sponsored APT group Antlion targeted 3 separate Taiwanese entities in an 18-month long campaign with the motive likely being cyber espionage.

Against tightening US-Japan relations and longstanding maritime disputes over islets in the East China Sea, the China-Japan bilateral relationship remains strained. In June 2022, 2 Chinese APT groups, BRONZE RIVERSIDE and BRONZE STARLIGHT (also known as DEV-0401), used HUI Loader to deploy RATs, malware, and ransomware in victim networks across industry verticals. In 1 of the 2 activity clusters, BRONZE RIVERSIDE, a group associated with the Chinese MSS, exfiltrated intellectual property from Japanese organizations, indicating a cyber-espionage motive behind the attack. In December 2022, ESET detailed a campaign linked to BRONZE RIVERSIDE that targeted Japanese politicians in the weeks preceding the July 2022 Japanese House of Councilors election.

Like Japan, India has strengthened ties to the US over the last 2 decades, and its technological boom has led to synergies between US corporations and IT services companies in India. In contrast to (and partially as a product of) India-US cooperation, the bilateral relations between China and India have continued to worsen. As disagreements over the Line of Actual Control (LAC) in the Galwan Valley have worsened, India has been the target of several Chinese state-sponsored cyberattacks. In an April 2022 report, we identified ongoing intrusions for at least the prior 18 months by suspected Chinese state-sponsored threat activity groups targeting Indian power grid assets like State Load Despatch Centres in northern India. Consistent with known goals of the PRC, Insikt Group assesses that the motive behind the campaign was intelligence gathering and potential pre-positioning on Indian power grid targets. In another instance, a ransomware attack against New Delhi-based All India Institute of Medical Sciences (AIIMS) in late 2022 was traced back to Chinese threat actors based on forensic data from the incident.

Chinese Relations Outside of Local Spheres

Beyond regional competitors, Chinese cyber activity is also driven by geopolitical trends and competition. After Russia invaded Ukraine, we saw Chinese APT activity targeting Western and Russian entities, signifying how the war prioritized increased Chinese intelligence-gathering initiatives on both friends and foe alike. For example, in June 2022, Insikt Group identified (and SentinelOne corroborated) activity attributed to the Chinese state-sponsored threat activity group Tonto Team (COPPER, CactusPete, Karma Panda, BRONZE HUNTLEY) targeting Russian government and state institutions. Chinese groups RedDelta, Twisted Panda, and Curious Gorge also conducted cyber-espionage activity targeting Russia [1, 2, 3].

Before Russia invaded Ukraine, China, like Russia, viewed the West as in decline and fractured, unable to justify international structures like NATO and politically unwilling to embark on painful revisions of the status quo [1, 2, 3]. Many of these assumptions are now in doubt by China, following numerous decisions by Western allies to support Ukraine that have proved these ideas false; the West, including the US, has new reason to remain united, and Europe has made plans to shift its dependence on Russian energy supplies faster than expected. This unity, however, has not been effortless; for one example, Germany has been reluctant to provide arms to Ukraine. Still, NATO has managed to implement substantial sanctions and provide aid to Ukraine throughout the war effort [1, 2].

The unity and breadth of sanctions imposed by the West on Russia throughout 2022 likely startled the CCP, resulting in a flurry of intelligence-gathering efforts to ascertain just how well-resourced Western powers are. For instance, in late February 2022, roughly corresponding with the initial Russian invasion of Ukraine, Recorded Future and security researchers at ProofPoint observed RedDelta conducting phishing campaigns against various European entities, with the end goal of delivering a new variant of the PlugX malware. In July 2022, Insikt Group detected an intrusion campaign attributed to TAG-22, a suspected Chinese state-sponsored threat activity group, that used ShadowPad malware and Cobalt Strike to compromise a US government organization, among other high-profile targets.

In light of ongoing support for Ukraine in the Russia-Ukraine war and strengthening bilateral relations between the US and key competitors such as India and Australia, the PRC's intelligence-gathering efforts to ascertain US military's and cyber capabilities will almost certainly continue.

Iran

Iranian Information Operations Amid Civil Unrest

Widespread protests broke out in Iran in mid-September 2022 after the death of Mahsa Amini, a young woman, at the hands of Iranian security forces. Iran's Islamic guidance patrol (گشت ارشاد), also known as morality police, initially arrested Ms. Amini for allegedly violating the theocratic regime's policy requiring women to cover their hair with hijabs. Popular demonstrations quickly broke out in cities and towns all over Iran. The Iranian regime's response has been swift and violent, suppressing peaceful demonstrators with lethal force. As of December 22, 2022, Iranian security forces had killed nearly 480 demonstrators and detained over 18,000 others. The regime sentenced 100 protesters to death and executed 4.

Parallel to the physical response, the Iranian regime has resorted to blocking access to social media applications and imposed Internet blackouts in parts of Iran in an effort to prevent anti-regime demonstrators from communicating and organizing. From the highest levels of the autocratic Tehran regime, including Iran's supreme leader, Ayatollah Khamenei, regime officials have orchestrated a disinformation campaign on state-controlled media, social media, and in the international press to discredit the protest movement and blame the US, Israel, and their Western allies of conducting information operations to interfere in Iran's domestic affairs.

As recently as January 2023, Iranian security forces executed a former deputy defense minister on charges of spying, leading some in the media to infer that "cracks" are forming inside Iranian regime ranks. Such paranoia and mutual distrust is not uncommon in autocratic regimes, however, and despite media rumors there are few facts to suggest that the protests have had any significantly destabilizing effect on the Iranian regime or the coherence of its response to the protest movement.

Failed Efforts to Revive the Iran Nuclear Deal

As the likelihood of Iran and the US reaching an agreement to revive the JCPOA diminishes, Iranian authorities signaled decreased incentive to rejoin the accord. In an August 2022 speech, Major General Hossein Salami, the commander of the IRGC, reiterated his belief that Iran is successfully combating the long-term effects of Western sanctions, minimizing the need to reenter the deal. Also in August 2022, Iran's trade minister said that Iran has successfully used cryptocurrency to pay for imports, offsetting the harms of Western trade sanctions on Iran. The enforcement of sanctions is complicated by the use of cryptocurrency as attribution of transactions can be obfuscated.

As JCPOA negotiations remain at a standstill, the Iranian government's lack of cooperation with ongoing International Atomic Energy Agency (IAEA) investigations, as well as recent statements about increased uranium enrichment operations, will very likely prevent advancements of JCPOA negotiations in the near term.

Revelations of the IRGC's plot to assassinate John Bolton and other US government officials, coupled with Iran's increasingly violent crackdown on peaceful protests and support to Russian combat operations in Ukraine, further decreases the short-term feasibility of a new Iran deal. Iranian leadership is likely to prolong negotiations to maintain the current status quo since a complete breakdown of talks will likely result in further US sanctions and a greater willingness of the US to openly oppose Iran's revisionist geopolitical agenda in the Middle East and Central Asia. Western negotiators have given Iranian mediators little reason to take seriously their proposed deadlines and pleas that time is running out. Moreover, Iranian leaders sense a willingness on the part of the current US administration to do whatever it takes to secure a deal. As such, it is likely that Iran will continue to press for concessions from the US until the latter grants them or until Iran achieves enough fissile material to assemble a nuclear weapon, whichever comes first. If Iran achieves enough fissile material for a nuclear weapon, negotiations will almost certainly cease.

Iranian Offensive Cyber Operations

Multiple Iran-based APT groups remain highly active in waging cyber offensive operations against Iran's geostrategic enemies. Various prominent APT groups led campaigns that involved vulnerability scanning and exploitation, were enabled by a new arsenal of tools, or relied upon tried-and-tested techniques. Groups such as APT34 (OilRig), MuddyWater, UNC788, LYCEUM, and APT35 (Phosphorus) were among the most active. Specifically, APTs with well-established tradecraft like UNC788, APT35, and APT34 were each identified and reportedly involved in broad espionage operations, identifying and exploiting vulnerabilities and developing custom malware, and were linked to aggressive social engineering attacks. Government agencies, foreign affairs bodies, and think tanks are high-priority targets for these groups.

A group of politically motivated cybercriminals, seemingly operating like "faketivists" and using custom tools, also executed offensive and influence operations throughout the first half of 2022. These included MosesStaff, BlackShadow, and Homeland Justice, which led a broad ransomware operation against the Albanian government. This conglomerate of threat actors is the most aggressive element of Iran's cyber operators.

Hacktivist forces with pro-Iranian regime agendas also waged broad attack operations around the world. These included groups like ALtahrea Team, Sharp Boys, and Open Hands. These groups have targeted as many sectors as possible, and in ALtahrea's case, have focused on adversely affecting the Israeli ecosystem. While many of their capabilities are not fully known, they are likely to continue offensive operations in the future in support of Iranian regime interests.

North Korea

North Korean Nuclear Weapons Testing

The United Nations described activity at North Korea's Punggye-ri nuclear test site on August 4, 2022, and provided evidence that North Korea was testing "nuclear triggers", substantiating prior US and South Korean assessments of an impending nuclear weapons test by North Korea. This news coincided with a meeting of the signatories of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in New York from August 1 to 26, 2022. The talks included the chief parties to the treaty, most notably the US and Russia, who voiced their intent to strengthen the New START treaty at the meeting. North Korea has historically timed its weapons tests during key dates in the US and China to achieve maximum disruption.

The last time North Korea conducted a nuclear test was in September 2017. However, the Kim regime regularly fires ballistic missiles, often into the Sea of Japan and sometimes, more aggressively, over Japan and into the Pacific Ocean. In 2022 alone, North Korea launched at least 92 ballistic missiles, more than in any previous single year. 46 of those ballistic missiles were launched in November alone.

The North is seeking to build an intercontinental ballistic missile (ICBM) that can strike as far away as the US mainland, and its ballistic missiles tests are likely in service of this goal. Before the end of November 2022, the North test fired its most powerful ICBM to date, the "Hwasong-17", into space. Flight data reportedly demonstrated that if fired at a "normal" angle, the Hwasong-17 was capable of striking the US mainland.

Reports from South Korean intelligence agencies on May 25, 2022, claimed that North Korea was testing what appeared to be nuclear detonators in preparation for another nuclear test at the Punggye-ri test site, the location of all 6 nuclear tests that North Korea has conducted to date. US officials' speculations about a North Korean underground nuclear test in November proved false, however.

North Korean APT Operations: BlueNoroff and Lazarus Group

While the North Korean state-sponsored threat group BlueNoroff (APT38) has traditionally focused on financially motivated operations targeting banks and SWIFT-connected servers, it has lately shifted to targeting cryptocurrency businesses and private investment firms as its main source of illegal income. Our research identified BlueNoroff spoofing cryptocurrency exchanges, investment firms, and banks, with a likely objective of stealing crypto assets.

BlueNoroff's "SnatchCrypto" campaign went after small and medium-sized businesses that deal with cryptocurrencies and smart contracts, decentralized finance, blockchain, and financial technology. The infection chain used decoy documents embedded with VBScripts that exploited CVE-2017-0199, a remote template injection vulnerability in Microsoft Office and several other Windows Server Service Packs. Despite BlueNoroff's shift away from the theft of fiat currency, BlueNoroff remains a threat to financial institutions, particularly those that trade cryptocurrencies. These operations are also tracked under the campaign names CryptoCore and CryptoMimic.

Lazarus Group, another prominent North Korean APT, has recently waged 2 campaigns against the US aerospace and defense sectors. The first campaign appeared to be a continuation of "Operation Dream Job", which was first observed in August 2020. Although Operation Dream Job originally targeted US aerospace and defense, Symantec revealed in April 2022 that Lazarus Group expanded its victimology to include organizations in South Korea's chemical and IT sectors. Symantec tied the activity to Operation Dream Job based on file hashes, file names, and tools used in previous campaigns. This iteration of Operation Dream Job begins when a malicious HTM file is downloaded, beginning a chain of events that eventually allows the hackers to get into a system and move laterally in a network using Windows Management Instrumentation (WMI). Lazarus Group operators also used techniques to persist in the network like dumping credentials from the registry and installing a BAT file.

The second Lazarus Group campaign targeted blockchain technology and cryptocurrency industries via spearphishing, using malware to steal cryptocurrency. The campaign starts with a vast number of spearphishing messages that use the pretext of recruitment and job opportunities sent to cryptocurrency companies' employees on various communication apps; the messages lure victims into downloading the malicious cryptocurrency applications. The malicious applications are written using cross-application JavaScript code with the Node.js runtime environment using the Electron framework. The US government refers to the malicious applications as "TraderTraitor". TraderTraitor lures victims through modern-designed websites advertising the malicious cryptocurrency application's features. The malicious cryptocurrency applications in the campaign are DAFOM, TokenAIS, CryptAIS, AlticGO, Esile, and CreAI Deck. The malicious applications include JavaScript code highlighting its core functions, which include downloading and executing the malicious payloads. According to the cybersecurity advisory, the malicious payloads included updated macOS and Windows variants of Manuscrypt, a custom remote access trojan (RAT) that gathers system information, executes arbitrary commands, and downloads additional payloads.

North Korea will very likely remain highly engaged on the cyber and kinetic fronts as 2023 unfolds. The US is expanding its military footprint in the western Pacific with new bases in Guam and in the Philippines. These are central to American strategies of deterrence and countering increasingly belligerent behavior (mainly by China) but also by North Korea. Furthermore, the US is increasing its cooperation with regional allies, namely Japan and South Korea, to establish a more prepared and united posture in the region in response to escalating aggression from China and North Korea. In response, North Korea will likely continue to fire ballistic missiles in tests geared toward developing an ICBM that can deliver a nuclear warhead to the US mainland. Similarly, we expect North Korean APT groups to continue to wage cyber offensive operations against critical sectors in the West.

Information Operation Trends

Paid Patriots: Russia Rebrands Its Information Operations

Russian information operations have seen multiple significant shifts over the course of 2022, the main cause of which remains the invasion of Ukraine. Firstly, interfering in Western elections like the US 2022 midterms was almost certainly retrograded as a strategic priority in favor of controlling domestic narratives over the war and fulfilling increasingly tactical aims to support the war effort. Second, much like Wagner's increasingly overt role in the conflict, Russia has had to enlist external support in information operations by painting troll farms as "patriotic" initiatives.

Since the 2016 US elections, academics have questioned the effectiveness of professional troll farms like the Internet Research Agency (IRA) in influencing voter behavior. The US government formally attributed the funding of the IRA to Yevgeny Prigozhin, "a close Putin ally with ties to Russian intelligence", shedding a light on the Russian government's covert information operations. In 2022, IRA-linked troll farms like Cyber Front Z have begun branding themselves as patriotic, distributed movements and have adopted a hybrid approach of centrally coordinated paid and patriotic trolls.

The self-branded "people's movement" began operating on Telegram on March 11, 2022, and picked up more than 65,000 followers by April 2022 (115,000 followers by January 2023). The channel's administrators instructed their followers to use VPNs to post under their real entities across all major social media platforms in order to support narratives around the war. These operational security measures were almost certainly implemented as a lesson from the 2016 and 2018 US elections, as social media platforms have been able to consistently detect coordinated inauthentic behavior (CIB) and attribute campaigns to troll farms like the IRA.

***Figure 3**: Chart showing the number of followers on Cyber Front Z's Telegram channel since March 2022 (Source: TGStat.com)*

An investigation by Russian media Fontaka revealed that Cyber Front Z used a hybrid approach: paid trolls and Russian volunteers (coordinated via Telegram groups and internal communications channels) were used to conduct information operations, while branding the entire effort as a distributed, patriotic movement. Despite this claim, undercover Fontaka journalists discovered overlap in staff between Cyber Front Z and the IRA, demonstrating that this initiative is yet another iteration of known troll farms funded by Prigozhin. On December 13, 2022, Wagner announced that Cyber Front Z had become a tenant at its "PMC Wagner Centre" headquarters, casting further doubt on the troll farm's self-described "distributed" model and supporting the hypothesis of the group's affiliation with Prigozhin.

In an August 2022 assessment of the troll farm's effects on public opinion, Meta described Cyber Front Z as "clumsy and largely ineffective", marking yet another failure by Prigozhin, whose latest iteration of information operations has failed to learn lessons from previous campaigns.

However, Cyber Front Z remains symptomatic of the Russian government's intent in 2022 to use information operations at a tactical level. The group's objective was explicitly geared towards supporting the war effort. Even before the outbreak of the war in February, Russia used both overt and covert influence networks to help justify the war by conducting false-flag operations at the border or accusing Ukraine of developing biological weapons in US-funded labs. However, as identified in our report "Malign Influence During the 2022 US Midterm Elections", Russia information operations targeting the US midterms were almost certainly rendered ineffective in their "strength, capabilities and reach", highly likely as a result of Russia's tactical focus. While previous elections had seen hack-and-leak operations at the forefront of Russia's playbook to create discord and influence voters, as evidenced by the 2016 DNC hack or the 2020 Hunter Biden files, no such instances were observed during the 2022 midterm elections.

One of the more pronounced Russian efforts in the 2022 midterm elections was identified on alt-right forums like Donald Trump's Truth Social, Gab and Parler, which was also linked to Prigozhin's Foundation to Battle Injustice, and equally assessed as having little effect. The campaign attempted to undermine public opinion on the US's ongoing support of Ukraine, demonstrating that even attempts in interfering with foreign elections were largely focused on tactical aims related to the invasion.

The Russia-China Narrative Nexus

A distinct trend in adversarial information operations is the consistent nexus in narratives between Russian and Chinese information operations. In 2022, overt and covert PRC channels amplified Russian government narratives around the invasion of Ukraine in a bid to criticize the United States and NATO. A May 2, 2022, press release by the US Department of State points towards Chinese information operations amplifying Russian narratives prior and during the invasion, including amplifying narratives around US biolabs in Ukraine, denying Russian war crimes in Bucha, and echoing Russia's framing of the invasion as a "special military operation". Leaked documents have since shown that Russia and China signed a bilateral agreement in 2021 for joint media projects and respective campaigns promoting each other, indicating a closer cooperation between the 2 states' strategic communications. While Recorded Future cannot confirm whether this agreement extends to covert information operations, we believe that this nexus of narratives between Russia's and China's overt channels will continue consolidating in 2023, including covert information operations.

In addition to narrative similarities of Russian and Chinese information operations, China has also attempted to follow the Russian playbook for covert information operations this year, as evidenced by the scale of activities tied to the Spamouflage Dragon network, also known as DRAGONBRIDGE. In January 2023, Google announced that it had disrupted over 50,000 assets tied to the network, making it the single largest influence network tracked by the company. However, analysis from Insikt Group corroborates Google's data indicating that the network has largely failed to create any significant engagement or followings on targeted platforms, marking an overall failure to use the network to durably influence Chinese-speaking and foreign audiences. Large-scale, low-quality networks like Spamouflage Dragon remain a consistent tool in Chinese information operations that have also been deployed for domestic information operations, such as during COVID protests in major cities in November, which were drowned out on social media platforms by thousands of automated accounts.

Despite this, Insikt Group believes that, to the extent China similarly views recent covert operations as failures (as defined by Meta), Chinese information operations may continue to shift to a "retail" approach to covert operations to build organic followings and engagement (or at the very least pursue both a retail and covert approach in parallel). We have already observed such a shift in terms of using influencers to target Western audiences.

Section II: Attacker Intelligence and Trends

Introductory Overview: Top MITRE TTPs

The top 10 referenced MITRE TTPs within Insikt Notes for 2022 are listed in the table below, based on the total number of individual references. This list aligns well with a threat landscape in which criminals and APT actors have prioritized exfiltrating data (T1005) from victim systems, whether that is for follow-on compromise (such as credential data), the threat of public data leak, or sensitive data access. Several initial access vectors help threat actors to steal this data, including account compromise (T1078, T1586), vulnerability exploitation (T1190), and phishing attacks (T1566). Befitting its ongoing significance as a threat, the main technique associated with ransomware (T1486) also appears in this list.

Rank	T-Code Identifier	Descriptor	Tactic
1	T1005	Data from Local System	Collection
2	T1078	Valid Accounts	Initial Access
3	T1021	Remote Services	Lateral Movement
4	T1133	External Remote Services	Initial Access
5	T1586	Compromise Accounts	Resource Development
6	T1486	Data Encrypted for Impact	Impact
7	T1190	Exploit Public-Facing Application	Initial Access
8	T1059	Command and Scripting Interpreter	Execution
9	T1566	Phishing	Initial Access
10	T1027	Obfuscated Files or Information	Defense Evasion

Table 1: *Top MITRE TTPs by reference count in Insikt-produced Analyst Notes, 2022 (Source: Recorded Future)*

The Rise of Infostealers

Credentials sales remain popular on dark web marketplaces, typically for use in account takeover and credential stuffing attacks. This tactic has grown in sophistication with the rise of information stealing malware and the proliferation of the malware-as-a-service model. Infostealer malware is designed to steal full fingerprints of logins from victim devices, including items like session tokens that can bypass multi-factor authentication (MFA). As a result, infostealers can provide criminal groups with immediate account access without requiring threat actors to test thousands of credentials and use paid proxy traffic services.

The high volume of infostealer logs available on criminal marketplaces like Russian Market and 2easy Shop makes them an easier source for immediate account compromise than combolists fed into credential stuffing tools. Between Russian Market and 2easy Shop, there has been a marked increase in credential dumps containing data compromised in infostealer campaigns, with the most popular infostealers in 2022 being Vidar, RedLine, and Raccoon Stealer. Specifically, Raccoon Stealer emerged with a new version following a lull after one of the lead developers was killed in the Russian invasion of Ukraine.

New infostealer variants, including RisePro, MetaStealer, Inno Stealer, and Prynt Stealer, have proliferated in 2022, with many including capabilities to steal cryptocurrency wallet data as well as browser and system data. Cybercriminals have used a variety of tactics to spread infostealers, including phishing, malvertising, and SEO poisoning. The rise of the sale of infostealer logs for both online platforms and remote access services corresponds to the rise in initial access services advertised on the dark web, likely a response to the increased demand for access by ransomware affiliates seeking to further expand their operations.

Cryptocurrency, Unregulated and Exploited

As cryptocurrency emerges as a fast-growing and largely unregulated space, cybercriminals have directed their attention toward targeting decentralized finance (DeFi) via new malware and attack vectors. Criminal groups have quickly exploited vulnerabilities in platforms like Confluence or compromised Alibaba or AWS cloud services and NAS devices to plant cryptominers like z0miner. When Microsoft reported a new variant of the Sysrv botnet in May 2022 that exploits vulnerabilities in the Spring Framework and some WordPress instances, security personnel could easily guess the botnet's purpose: to mine cryptocurrency in Windows- and Linux-based servers by deploying the XMRig miner. Vulnerability exploitation in particular has shown to be a popular infection vector, with 1 in 6 cases of infection in Q3 2022 via vulnerability exploitation resulting in a cryptominer infection.

***Figure 4**: The volume of listings for infostealer logs on Russian Market and 2easy Shop has grown substantially since 2021 (Source: Recorded Future)*

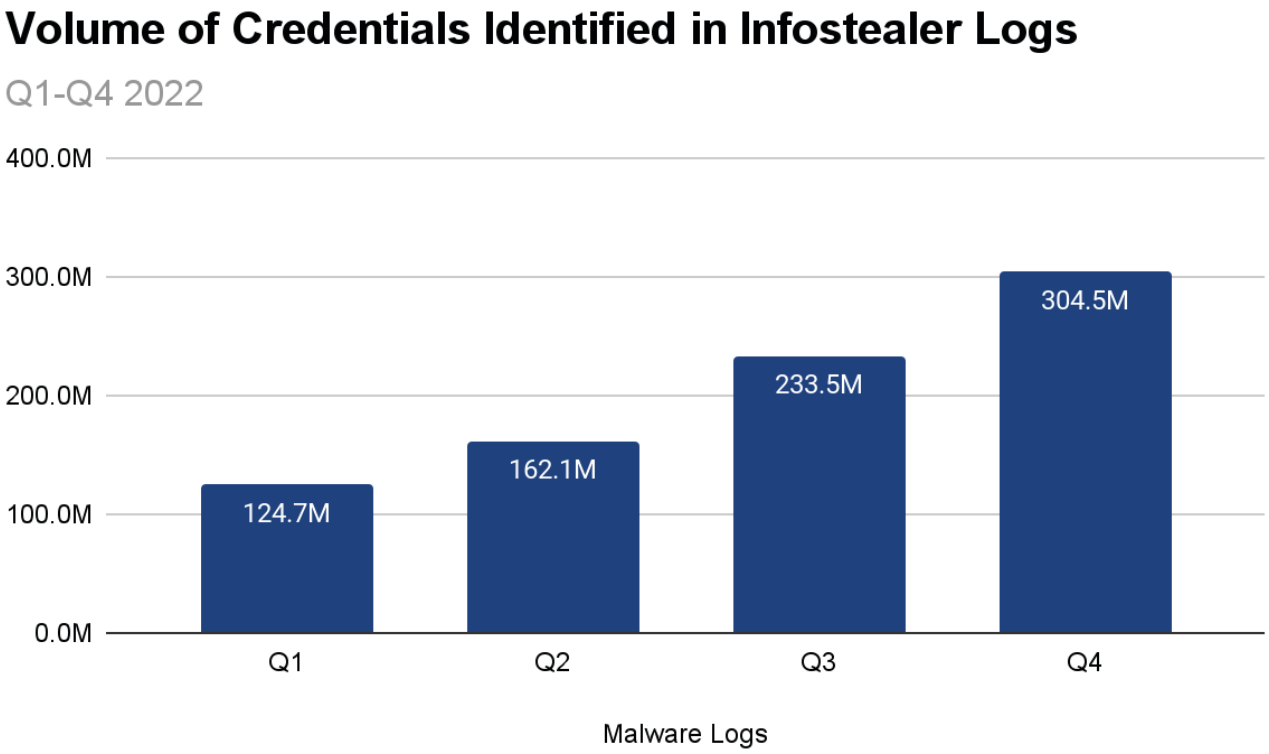

***Figure 5**: Increase in volume of data collected by infostealer malware throughout 2022 (Source: Recorded Future)*

The number of cryptominer variants significantly increased in 2022, with over 150,000 observed in the wild in 2022. Cryptomining has emerged as a relatively reliable source of passive income for cybercriminals; although it may not bring in as much immediate revenue as a successful ransomware operation, cryptominers can remain undetected on infected systems for months at a time. The financial damages of crypto mining operations can be staggering for infected hosts: according to experimental research by Sysdig, the cost to the victim of mining 1 XMR (Monero) on a single AWS EC2 instance was roughly $11,000 as of April 2022.

Cyber threat groups interested in cryptocurrency have also created new malware or campaigns to target cryptocurrency exchange servers or wallets directly to exfiltrate funds. DeFi platforms generally rely on smart contracts, which are automated agreements that lack an intermediary, like a broker. However, that has left many platforms, and the assets investors entrust to them, at risk. According to an advisory issued by the FBI in August 2022, cybercriminals have begun exploiting vulnerabilities in flash loans, signature verification, and cryptocurrency pricing to defraud investors and steal cryptocurrency.

Crypto wallet and private key information also remains a popular commodity targeted by infostealer malware, with numerous infostealer variants featuring cryptocurrency data exfiltration and mining capabilities. Due to the potential for large valuation gain in a short time period of cryptocurrencies, the losses from cryptocurrency exchange theft can be massive. Unauthorized withdrawals from cryptocurrency exchange app Crypto[.]com in January 2022, for example, totalled 443.93 BTC, or nearly $20 million at the time. Throughout 2022, the North Korean state-sponsored Lazarus Group and its reported subsidiary BlueNoroff repeatedly targeted cryptocurrency exchanges for large heists, with at least $725 million in losses reported this year.

Non-fungible token (NFT) drainers and crypto drainers, which are phishing pages designed to lure victims into unknowingly signing unauthorized transactions, rose in popularity in 2022. Crypto clippers are another increasingly popular type of malware, which hijack a victim's copy-and-paste clipboard and replace it with a cryptocurrency wallet address controlled by the threat actor. This process allows the threat actor to rent and sell stand-alone versions of this malware and allows for the unintentional transfer of cryptocurrency funds from victim to threat actor. The largely unregulated nature of DeFi has also resulted in widespread fraud, with several NFT scams uncovered this year.

Dependency Dangers: The Risks of Open Source

Following several large scale software supply chain incidents in 2021 (SolarWinds, Kaseya) and the disclosure of the Log4j vulnerabilities, cybercriminals have increasingly targeted widely used software in supply chain and package dependency attacks.

Many enterprises rely on open source or proprietary software packages (such as the Python Package Index [PyPI] or the Node Package Manager [npm] for JavaScript) to outsource the creation of basic or niche functionality in certain scripts, allowing developers to focus on the development of new capabilities. The security and provenance of these packages is often explicitly trusted, but there have been several instances of abuse of these package managers to deliver malware or gain backdoor access.

Attackers have used dependency confusion attacks as a form of typosquat, slightly modifying common package names to trick developers into installing malware using their package manager. In the July 2022 "IconBurst" operation, for example, adversaries impersonated well-known NPM modules, including "umbrella.js" and packages published by ionic[.]io, to distribute over 24 malicious NPM packages used to steal and exfiltrate form data from victims. These malicious packages were likely used by hundreds, if not thousands, of downstream mobile and desktop applications and websites. In one case, a malicious package was reportedly downloaded more than 17,000 times. In August 2022, Checkpoint's CloudGuard Spectral published a blog detailing its discovery of 10 malicious packages within PyPI that installed information stealers that targeted developers' personal data, credentials, and API tokens.

Given the hundreds of packages stored in PyPI, npm, and others, the attack surface for this space is diverse and expansive. Companies will be required to implement effective monitoring solutions to stay ahead of this growing threat over the next few years, particularly as the adoption rate of open source continues to grow.

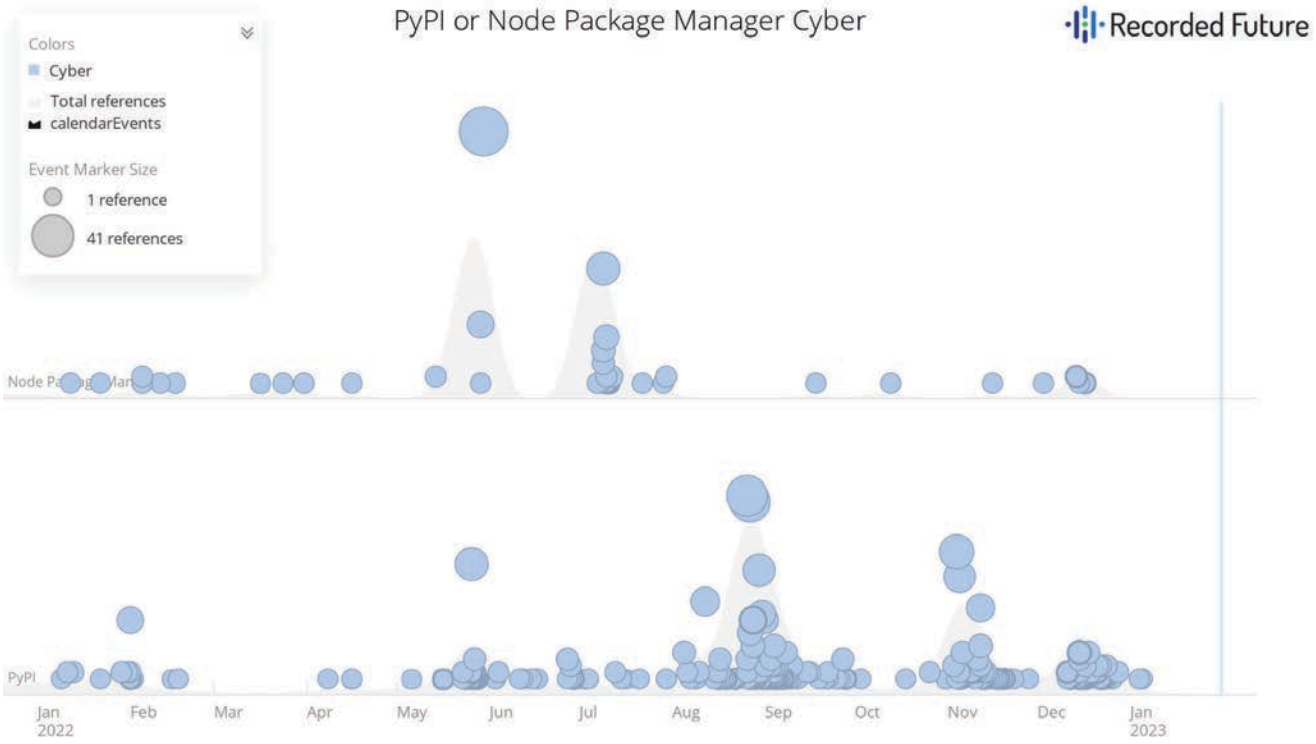

Figure 6: *Cyber events related to PyPI or NPM in 2022 (Source: Recorded Future)*

Attackers have also targeted widely used software suites across industries in third-party compromise attacks. Supply chain attacks via third-party compromise act as a force multiplier, allowing attackers to capitalize on widely used tools to exploit their targets. On April 15, 2022, GitHub revealed a malicious campaign involving an undisclosed adversary abusing OAuth user tokens issued to 2 third-party OAuth integrators, Heroku and Travis CI, which were then exploited to download and steal data from private repositories belonging to dozens of organizations using the Heroku and Travis CI-maintained OAuth applications. WordPress also experienced several major third-party compromise attacks in 2022, both taking advantage of vulnerable plugins to access and inject malicious code in websites that used them. The expansion of the cybercriminal initial access market is another important indicator of the increased attack surface for third-party compromise, with third-party vendor RDP credentials and databases increasingly likely to appear in dark web listings.

C2 Trends a Continuation of Past Patterns

The command-and-control (C2) landscape of 2022 continued to be dominated by commonly used tools such as Cobalt Strike, Meterpreter, and PlugX. While several new families, such as Brute Ratel (BRc4) and Bumblebee Loader, were introduced, the largest increase in use has been for older, more established tooling. This may indicate that a larger percentage of threat actors favor being unattributable, rather than undetectable, as commodity tools are more likely to be detected by antivirus software. As the barrier for entry for cyber threat actors lowers with the expansion of the "as a service" criminal framework, it is likely becoming increasingly attractive for lower-level threat actors to buy commodity tools or use open-source malware rather than develop custom variants.

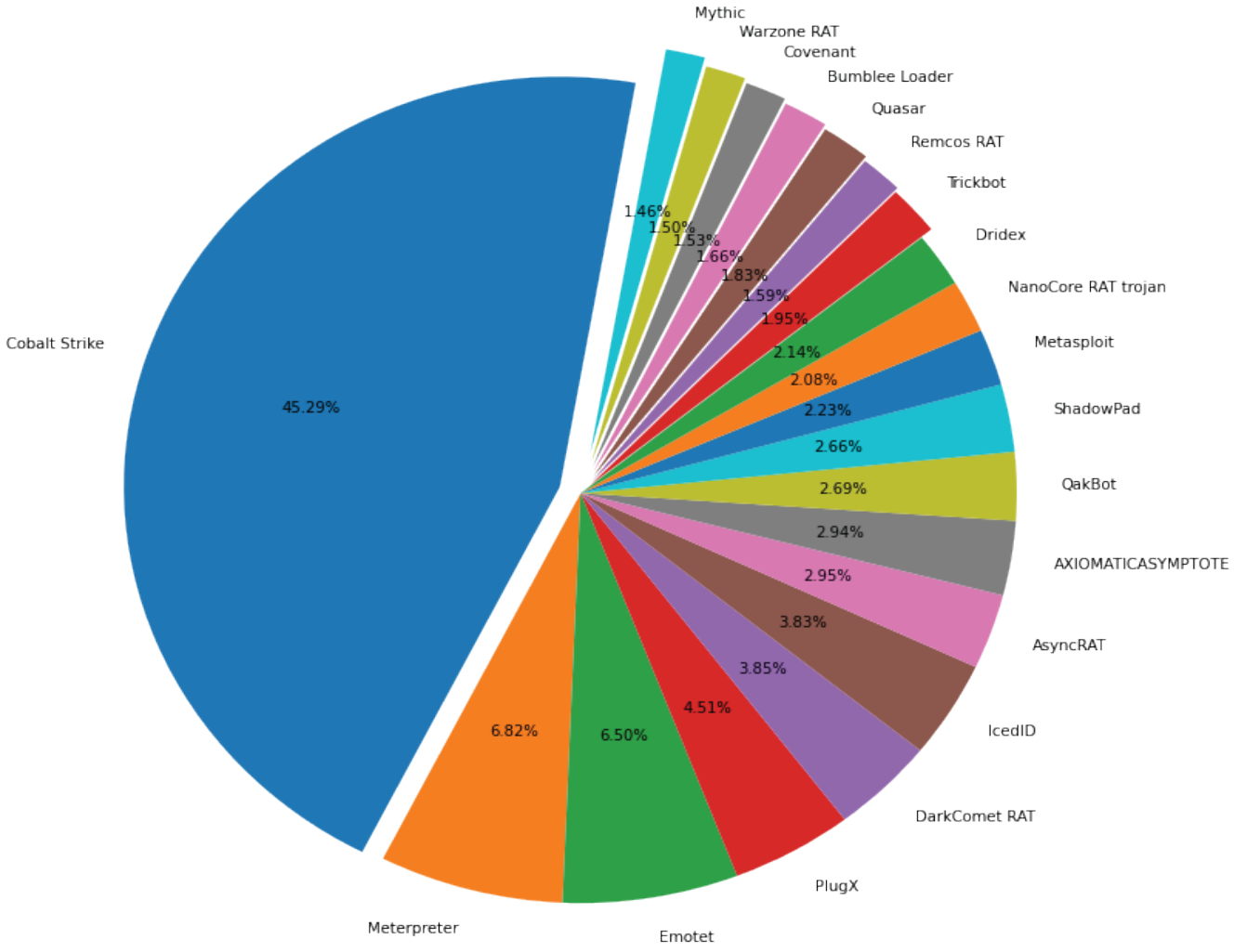

Figure 7: *C2 detections by malware family as seen by Recorded Future*

Botnets also continue to make up a significant portion of C2 traffic, with Dridex, Emotet, IcedID, QakBot, and TrickBot having the most C2 detections this year. Emotet in particular has demonstrated its resilience and made a full resurgence following the multinational law enforcement takedown of its infrastructure in 2021.

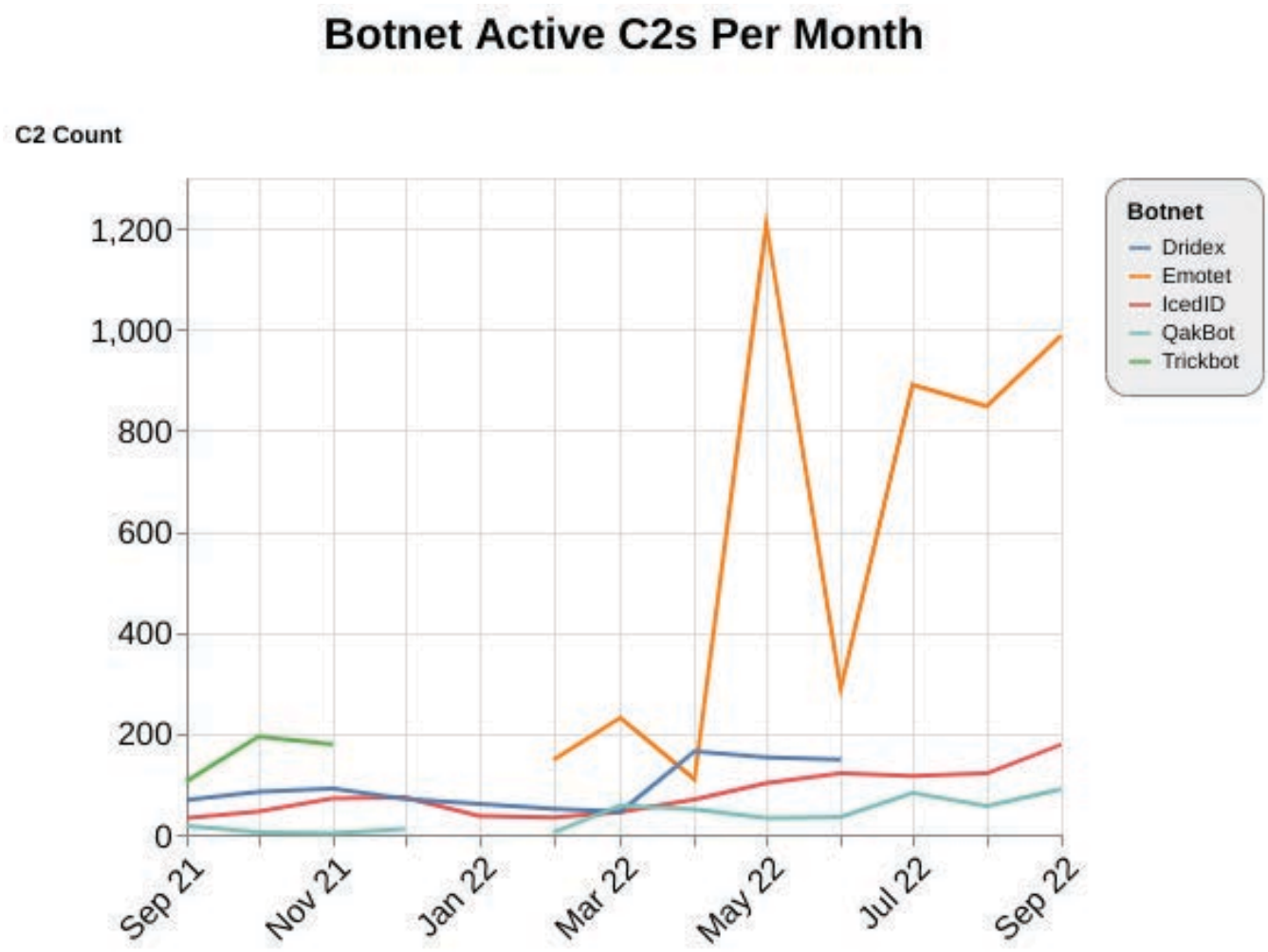

Figure 8: *Comparison of detected Dridex, Emotet, IcedID, QakBot, and TrickBot C2s (Source: Recorded Future)*

These botnets deliver ransomware such as BlackBasta, ALPHV, and Quantum. There has been a significant shift in C2s to Chinese hosting providers: while the US share of C2 servers dropped from 34% to 22% in 2022, China's shares increased from 14% to 24% mostly due to substantial increase in C2 detections at Chinese hosting provider Shenzhen Tencent Computer Systems. Overall, all top 10 C2 hosting providers recorded substantial increases in the number of detected C2 servers.

The Expansion of the As-a-Service Model

Mirroring the shifts in the business world, the underground market has moved toward a managed service model in recent years in which threat actors offer their tools and expertise as subscription services, lowering barriers to entry and allowing an increasing number of less-sophisticated threat actors to engage in malicious activity. This trend continued throughout 2022, as evidenced by the ongoing popularity of the ransomware-as-service (RaaS) model, activity from IABs (see sections Section V: Ransomware and Data Extortion Intelligence and Section II: Initial Access Trends), and discovery of new malicious platforms offered as services.

Since the beginning of 2022, we observed 3 new malware-as-a-service (MaaS) infostealer variants being developed and released in the wild, namely DuckLogs, Mars Stealer, and Aurora Stealer. We also identified a new MaaS seller platform, Eternity Project, which is a Tor website listing a variety of malware, including stealers, clippers, worms, cryptominers, ransomware, and DDoS bots.

The ongoing popularity of MaaS was also evidenced by a statement from the threat actors behind Mars Stealer, an infostealer that gained significant traction within the threat landscape following the voluntary and temporary shutdown of the highly popular Raccoon Stealer: Following its release, Mars Stealer's developers claimed to have received too many sale requests to process.

In addition to malware, the number of other products and tools offered as services increased in 2022. Since the beginning of the year, Recorded Future's Insikt Group detected the presence of 2 new phishing-as-a-service (PaaS) offerings Caffeine, and EvilProxy. The PaaS platform Robin Banks reemerged in November 2022 following its disruption by Cloudflare in July 2022. As phishing remains among the most common infection vectors, the underground economy has adjusted accordingly in its embrace of the as-a-service model, with developers releasing customizable, automated, and user-friendly phishing kits that tap into the demand and cater to a pool of different threat actors.

The offerings and capabilities of these platforms are increasingly sophisticated. For example, the EvilProxy PaaS variant, previously observed in targeted campaigns attributed to APTs and cyber espionage groups, uses reverse proxy and cookie injection methods to bypass 2FA authentication. The PaaS platform Frappo, initially identified in early 2021, increased the number of organizations for which it can generate phishing web pages. And Raccoon Stealer added the capability to resolve malicious API functions dynamically instead of statically, making detection more difficult.

As the MaaS and PaaS marketplace becomes increasingly crowded and competitive, developers will look to improve their offerings, likely focusing on improving the ability to bypass security mechanisms and remain undetected.

Dark Utilities, a new platform that offers command-and-control as-a-service (C2aaS), was discovered by Cisco Talos in August 2022. It provides full-featured C2 capabilities and features pre-built and user-friendly interfaces and detailed guidelines that render otherwise sophisticated tools and services accessible to even the least-skilled threat actors. C2aaS is not entirely novel in the threat landscape, as commodity RATs were observed providing their customers with readily available C2 nodes in 2018. References to C2aaS across media and dark web sources, however, remained low between 2019 and 2021, rising in 2022 concurrently with the disclosure of Dark Utilities.

This seeming resurgence of C2aaS in 2022 likely mirrors the increasing adoption of the as-a-service market model across the underground landscape, with the threat actors behind Dark Utilities likely starting to occupy a niche that answers a specific demand. Dark Utilities' currently low price (€9.99), for instance, likely reflects its developers' attempt to cater to as many threat actors as possible, even those with significantly less resources, and position themselves as the go-to platform for C2aaS. Dark Utilities' price is relatively low in comparison to the amount of functionality the platform offers, and is significantly lower than prices commonly seen among MaaS and PaaS, which usually cost hundreds if not thousands of dollars depending on the subscription tier. Should Dark Utilities prove lucrative and surge in popularity, however, we expect other similar platforms to follow suit, as a greater number of threat actors attempt to seize market share.

Threat Actors Diversify Files and Vectors in Phishing Attacks

Phishing remains among the most common infection vectors, with threat actors relying on human error to gain access to accounts, corporate networks, and sensitive information. Throughout 2022, phishing campaigns used a diverse pool of files to increase chances of bypassing email security mechanisms and successfully infecting devices with malware. In addition to traditionally common file types, such as various types of Microsoft Office documents and PDFs, threat actors used formats such as HTML and ISO, as well as password protected archives.

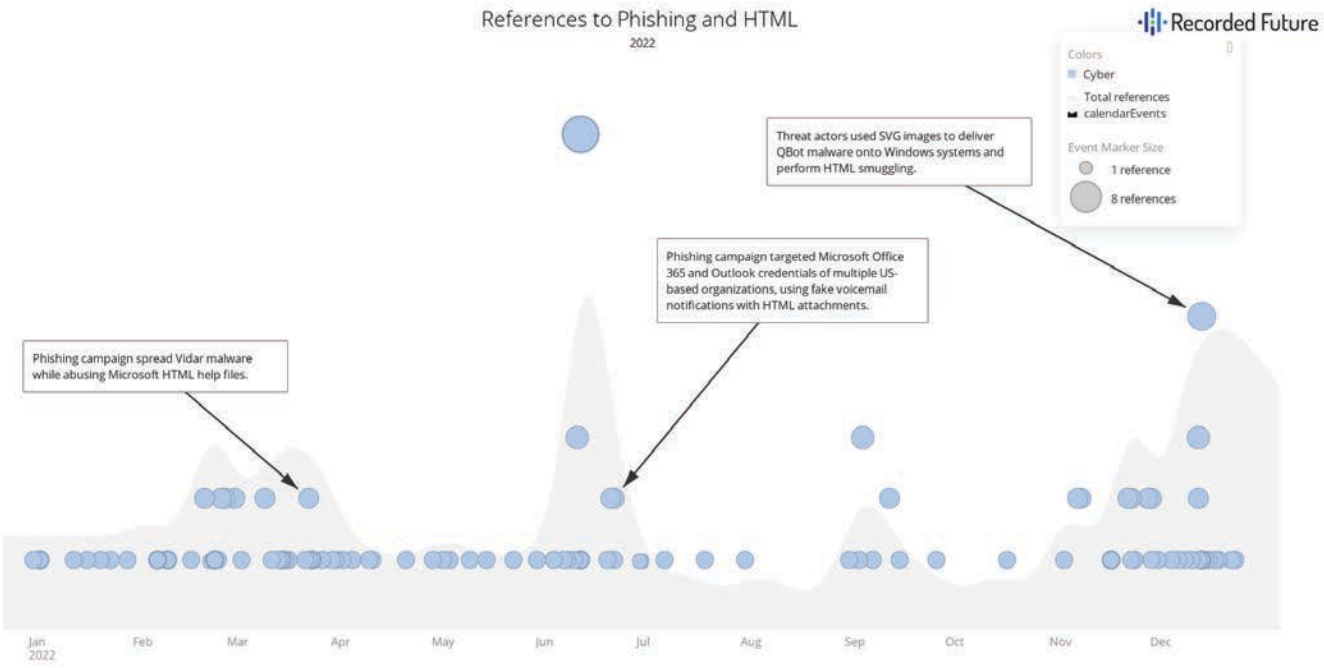

***Figure 9**: References to phishing attacks involving HTML remained consistent throughout 2022 (Source: Recorded Future)*

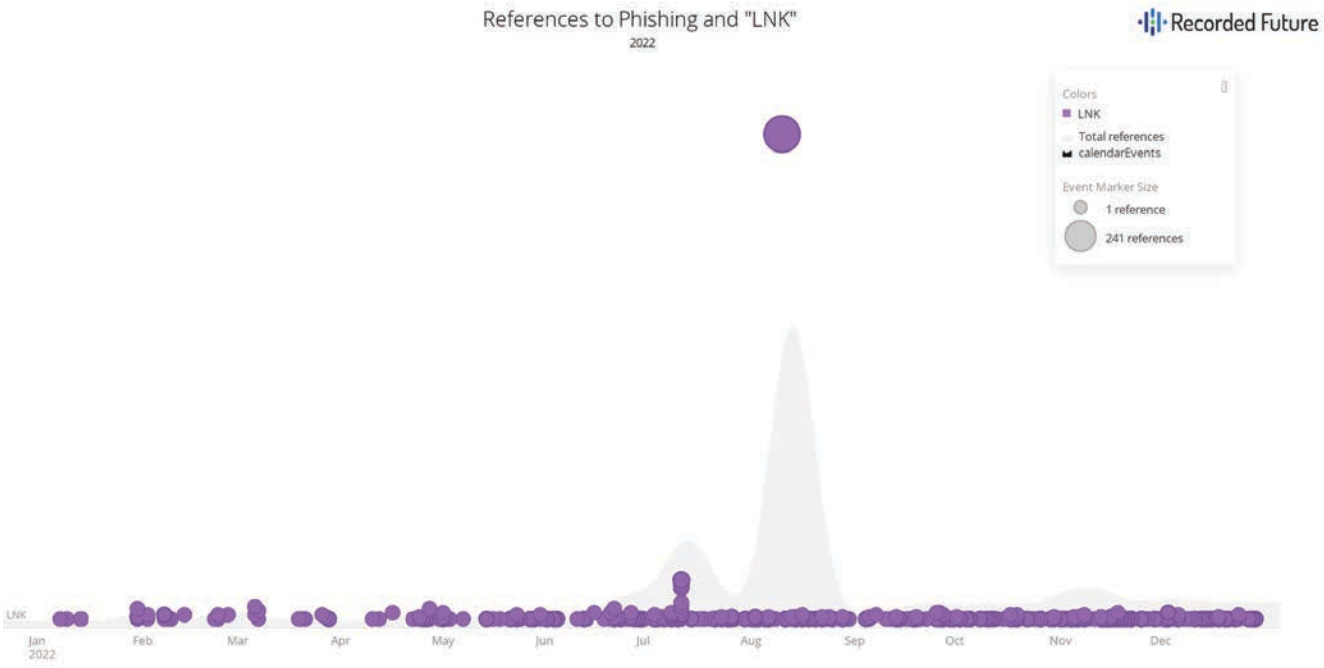

***Figure 10**: Following Microsoft's reveal of plans to block macros by default there has been an uptick in references involving phishing and LNK (Source: Recorded Future)*

Although not novel to 2022, the use of some of these file formats increased: Statistics unconfirmed by Recorded Future showed that ZIP and RAR files overtook Office documents for the first time in 3 years as the most commonly used files to deliver malware, likely because these file types provide better ways to hide malicious payloads and lower chances of detection by web proxies, sandboxes, and email scanners.

Threat actors also adapted to changing standards among defenders. Following Microsoft's decision to block macros by default in its Office product line in Q3 2022, LNK files were increasingly used to deliver RATs and infostealers such as QakBot, IceID, Emotet, and RedLine Stealer. We also observed an increase in references involving LNK in Q3 2022. LNK files are an attractive alternative for threat actors as they allow code execution without the use of macros.

In addition to emails, threat actors also broadened their reach through a variety of phishing attack vectors:

- Social media, including Facebook [1] and LinkedIn
- SMS messages (smishing)
- Messages sent via instant messaging platforms like WhatsApp, Telegram, and Discord
- Messages sent over video streaming services like YouTube [1]
- Voice phishing (vishing) and callback phishing

Although not as scalable and replicable as other vectors (such as email and SMS messages), voice and callback phishing are attractive because they add to the personability of the attack, putting victims in direct contact with a human voice.

Threat actors continued to exploit seasonal events in 2022, such as tax season, Labor Day, Halloween, and Black Friday, as well as large sport events such as the 2022 FIFA World Cup, capitalizing on the fact that customers have now come to expect messages informing them of seasonal sales or major sporting events.

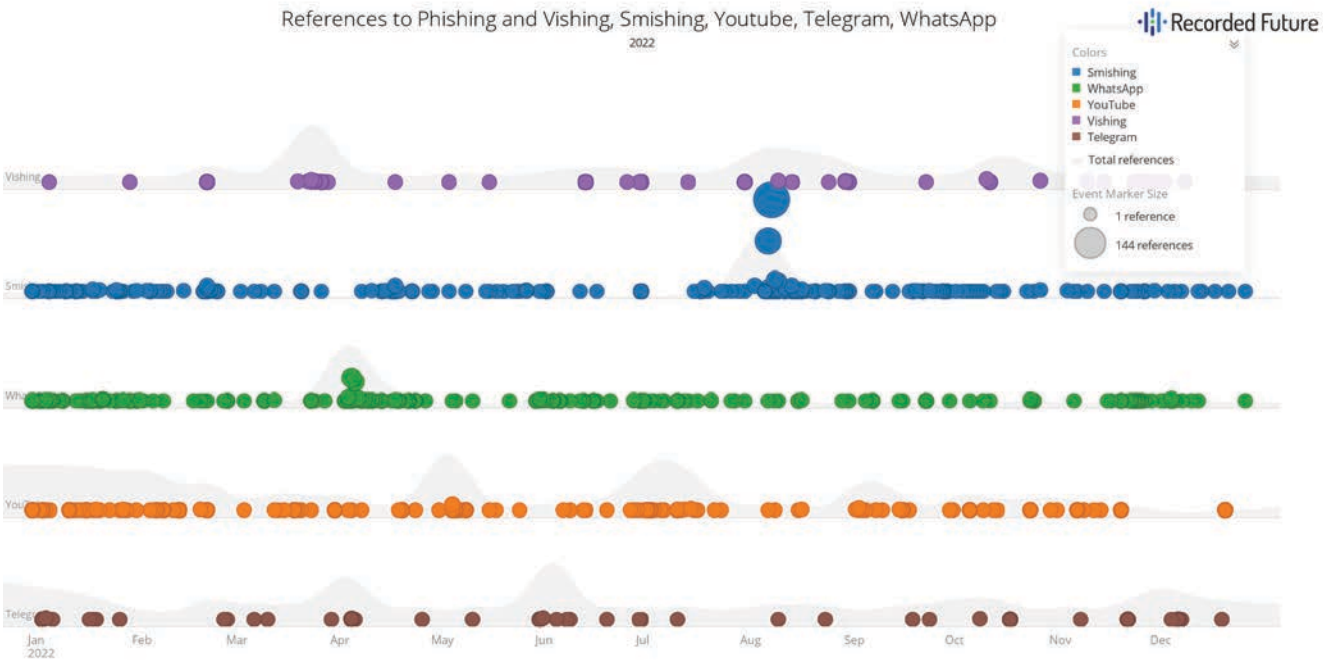

***Figure 11**: References to cyberattacks involving phishing and various techniques and platforms [**Vishing**, **Smishing**, **WhatsApp**, **YouTube**, **Telegram**] remained consistent throughout 2022 (Source: Recorded Future)*

Section III: Initial Access Trends

Increasingly, threat actors can gain initial access to networks through infostealer malware infections, initial access brokerage services on dark web and special-access forums, or the purchase of infostealer logs from dark web shops and marketplaces. Other attack vectors, such as phishing, spearphishing, and code injection, are also common on dark web and special-access forums, but their immediate effects are often much less public and visible than the sale of compromised credentials. Using BlackMatter and Conti as examples, we examine the role of credential access in the execution of the attack, from initial access to ransomware deployment.

Stolen credentials are often sold to ransomware affiliates on dark web and special-access forums by initial access brokers (IABs). While most high-profile accesses are brokered on top-tier Russian-language forums, such as Exploit, XSS, or RAMP, some IABs are present on low-tier or mid-tier English-language forums, such as BreachForums or the now-defunct Raid Forums. IABs commonly operate in multiple languages on different forums, often under different monikers (for example, "FuckerZ" connects to "Tokugaw4", "tokugawa", "xssisownz", and "Str0ng3r"), to avoid detection, tracking, and arrest. Many English-language cybercriminal forums, such as Cracked or Nulled, have banned IAB services and ransomware discussions outright, as the risk of law enforcement attention on the forum increases with such activity. Less commonly, ransomware operators and affiliates will work directly with a designated group of IABs that will conduct business off of the forums and in private messaging channels, such as Tox or XMPP (Jabber).

IAB advertisements follow a similar pattern on dark web and special-access forums. The template is loosely as follows: "victim country", "annual revenue", "industry", "type of access", "rights", "data to be exfiltrated", and "devices on local network". Additional useful information includes the type of antivirus software, IP address ranges, and other details.

On top-tier forums, sellers are typically required by the forum's rules to provide a sale price in the initial advertisement. As many of these deals are negotiable, with price ranges varying widely depending on multiple factors, the most common form of advertisement is the "auction" format. IABs will provide an acceptable starting price ("start"), the minimum price of bid hikes ("step"), and the full or "buy now" price if a threat actor is interested in purchasing immediately ("blitz"). This is often followed by a time range in which the posting will close, generally between 4 and 8 hours. The IAB will often indicate if a sale is made in the thread ("sold", продано), asking the forum's moderation staff to then close the thread for new replies. IABs, especially those who are working with unknown or low-reputation threat actors on the forums, will often request the use of escrow or middleman services to facilitate transactions.

Listings Across All Dark Web Forums

Based on our collections from dark web forums, the IAB market for network access grew substantially in 2022. We identified 1,292 listings for network access to organizations on dark web forums, nearly tripling the 431 listings identified in 2021. This data was sourced from analyst-verified entries from dark web forums and does not account for every dark web advertisement across the dark web. While this rise can partly be accounted for by an increase in analysts over this time period verifying advertisements, researchers across the cybersecurity industry have noted at least a 100% increase over the past year in initial access advertisements.

While it remains difficult to determine the exact factors behind the overall rise in listings, we suspect that the overall IAB market has gained maturity in tandem with increased demand for network access from ransomware groups.

One potential geopolitical factor in the growth of the IAB market is the Russian invasion of Ukraine. Listings spiked after March 2022, which may be due to emboldened actors using the opportunity to attack Western organizations at an increased rate, although Asian organizations were also increasingly referenced by IABs. While the Russian government had begun cooperating with US law enforcement in disrupting cybercriminal gangs in 2021, as demonstrated by the REvil arrests, the invasion likely halted any cooperation between the 2 governments, leading to less pressure on cybercriminal groups targeting Western targets. Furthermore, attacks by ransomware groups against European critical infrastructure in months preceding the invasion were likely conducted to advance Russian government interests, indicating a degree of cooperation between the Russian state and ransomware actors. Even prior to the conflict, Insikt Group assessed that Russian-language cybercriminal groups very likely act in alignment with Russian intelligence agencies, given the level of simultaneous surveillance of the groups by intelligence services and tolerance of operations targeting non-Russian entities.

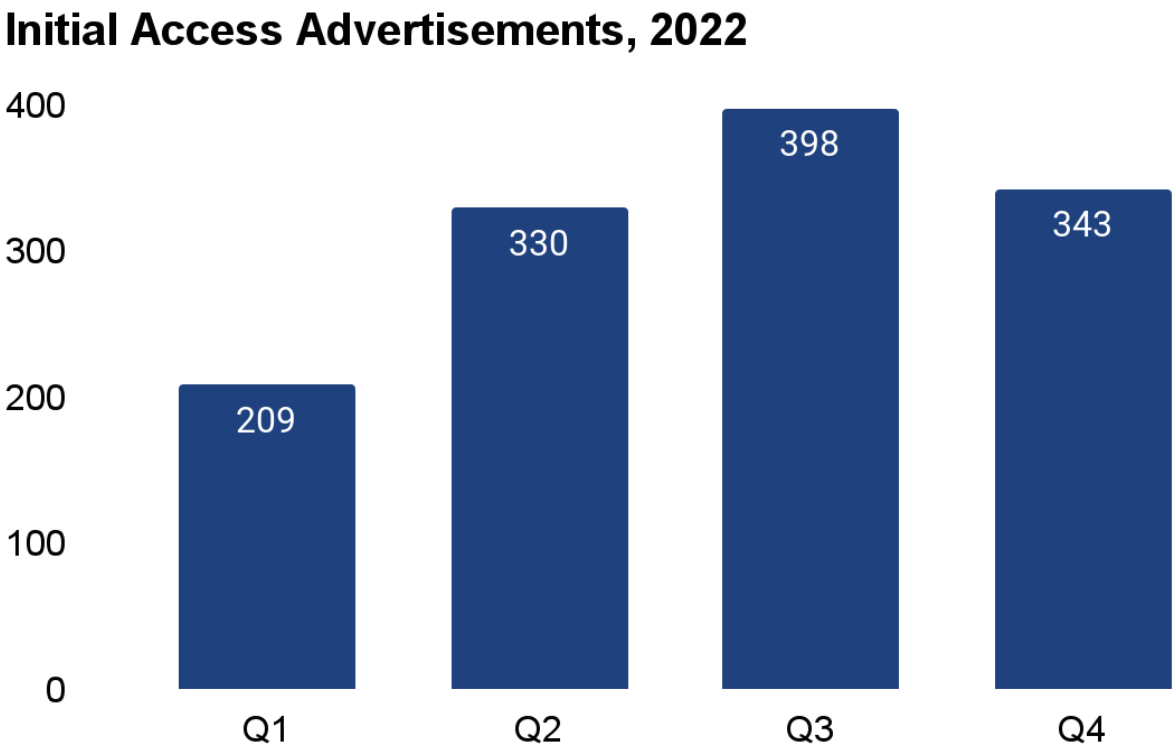

***Figure 12**: Dark web listings advertising initial access vectors (Source: Recorded Future)*

Prominent High-Credibility Actors

When categorizing network access sales in 2022 by forum, Exploit was by far the forum with the most listings (1,111), followed by XSS (234) and RAMP (54). Some listings were posted on multiple forums across threat actors' accounts. Among these posts, we identified 494 distinct threat actors, 114 of which Insikt Group has assessed as high credibility based on metrics such as length of time the threat actor has been a member of a particular criminal site, number of posts made, feedback from users, and known cross-site activity. High-credibility actors sold access in different forms, including VPN, email and mobile access, with RDP access being the most common. Accesses sold also came with different levels of privilege, from user privileges to domain administrator, with local administrator privileges being the most common. The following 5 actors most frequently listed network access to organizations across industry verticals and geographies:

- zirochka (Exploit) posted 46 listings
- Inthematrix1 (Exploit, Ramp) posted 35 listings
- sganarelle2 (Exploit) posted 33 listings
- orangecake (Exploit, Ramp) posted 26 listings
- yesdaddy (Exploit) posted 22 listings

Pricing Analysis

Pricing for initial access to networks on dark web forums depends on a variety of factors and can vary substantially. A recent analysis posted at DarkReading stated the average price for RDP access between H2 2021 and H1 2022 was $2,800. Recorded Future analyzed the final 2 weeks of December 2022 from our Threat Leads source and found the pricing largely to be in line with this number. The average "Buy Now" or "Blitz" price in our limited data set (See Appendix A) was $2,100 for RDP access with the range spanning as low as $400 to as high as $10,000. Numbers referencing the average cost of remote network access across the cybersecurity industry vary, but the average appears to have come down over the last year from the reported 2021 average of more than $5,000. This likely can be attributed to supply catching up with demand as ransomware operators and affiliates seek to outsource the difficult task of initial access to dedicated purveyors.

To corroborate this general trend in decreasing prices, Recorded Future analyzed one of the most prolific posters offering RDP access on the dark web in 2022, user "inthematrix". Recorded Future analyzed inthematrix's "blitz" price across the entire year and found that although prices varied significantly depending on the nature of the access being sold, the overall trend from the beginning of the year to the end was down. This is likely a result of the increasing volume of network access advertisements being offered on dark web forums and marketplaces. Prices advertised by inthematrix ranged from $1,500 USD "blitz" price for domain administrator access to a revenue per year US based company (with $5 million dollars in revenue) to $20,000 USD blitz price for RDP access to a "major" US real estate company with $1.2 billion in yearly revenue. Prices generally rose with the level of access and the quoted annual revenue of the company.

RDP and VPN access is the most common type of corporate network access advertised and is often differentiated between local and domain administrator access. Domain administrator access tends to command a higher price than local administrator access, depending on the size and reputation of the victim organization and quality of information or access available on the network.

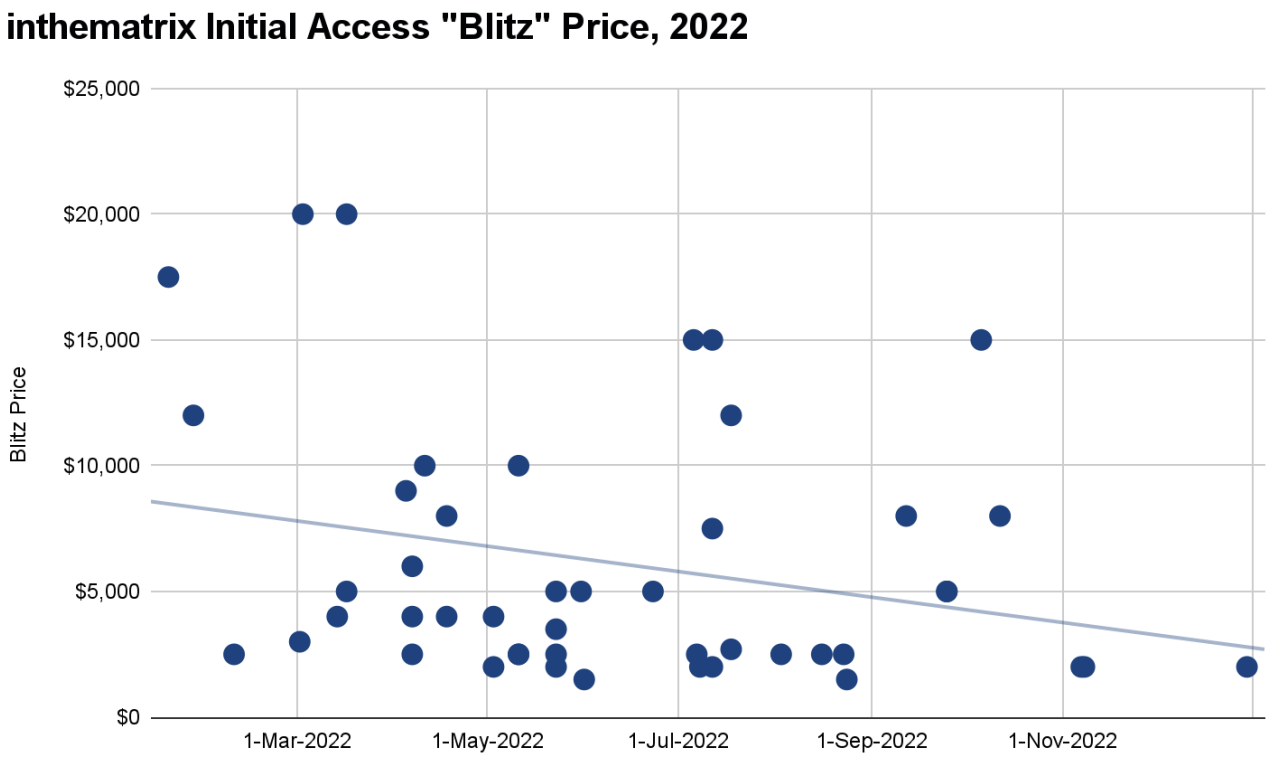

***Figure 13**: Dark web listings advertising initial access vectors posted by user inthematrix (Source: Recorded Future)*

Section IV: Vulnerability Intelligence

Vulnerability Disclosures

In 2022, we identified an unprecedented number of zero-day vulnerabilities, as well as a general increase in the disclosure of vulnerabilities, according to information sourced from the National Vulnerability Database (NVD). We have included our top 10 vulnerabilities by references in the Recorded Future Intelligence Cloud below.

The most-referenced vulnerability, CVE-2022-30190 (Follina), is a Microsoft zero-day vulnerability allowing threat actors to bypass security restrictions like Windows Defender on opened Word documents, enabling macro-less attacks. The 2 Microsoft Exchange zero-day vulnerabilities, CVE-2022-41040 and CVE-2022-41082 (collectively known as ProxyNotShell) was widely exploited in the wild. Exchange vulnerabilities are often exploited by ransomware gangs and nation-state groups because they provide widespread access to victim infrastructure upon successful exploitation. Ransomware gangs even proved effective in bypassing mitigations put in place by organizations for these vulnerabilities. Other notable vulnerabilities this year include vulnerabilities affecting proxy and access control products by vendors like VMWare and Fortinet, such as CVE-2022-40684 and CVE-2022-22954.

Vulnerability	Affected Product	Risk Score	CVSS
CVE-2022-30190	Windows	99	7.8
CVE-2022-26134	Confluence	89	9.8
CVE-2022-40684	Fortinet	89	9.8
CVE-2022-22954	VMWare Workspace One	89	9.8
CVE-2022-41040	Microsoft Exchange	89	8.8
CVE-2022-41082	Microsoft Exchange	89	8.8
CVE-2022-1364	Chrome	89	8.8
CVE-2022-22965	Spring	99	9.8
CVE-2022-24521	Windows	89	7.8
CVE-2022-2856	Chrome	89	6.5

***Table 2**: Top vulnerabilities disclosed in 2022 (Source: Recorded Future)*

The 4 most notable vulnerabilities, based on risk score, number of references within the Recorded Future Intelligence Cloud, and ongoing exploitation activity, were Follina, the ProxyNotShell vulnerabilities, the Mark of the Web bypass vulnerability, and CVE-2022-26134.

Follina

CVE-2022-30190, or "Follina", is a Microsoft RCE vulnerability, first publicized on May 29, 2022, that affects the Microsoft Windows Support Diagnostic Tool (MSDT). Follina allows a threat actor to gain RCE capabilities on a system without resorting to macros.

Following the vulnerability's initial disclosure, it was exploited by various threat actors, including the Chinese state-sponsored threat group TA413, the Chinese state-sponsored threat group BackdoorDiplomacy, an undisclosed nation state-sponsored group targeting government agencies in the US and Europe, and TA570, among others. The Computer Emergency Response Team of Ukraine (CERT-UA) released an advisory warning that Russian APTs are exploiting the Follina vulnerability in a phishing campaign to target media organizations in Ukraine. Cybercriminals quickly began advertising and sharing exploits for the vulnerability on various underground forums and marketplaces.

The widespread exploitation of this vulnerability by threat actors with varying degrees of expertise and resources underscores its ease of exploitation and applicability and secures the vulnerability's spot as one of the most prominent disclosed in 2022.

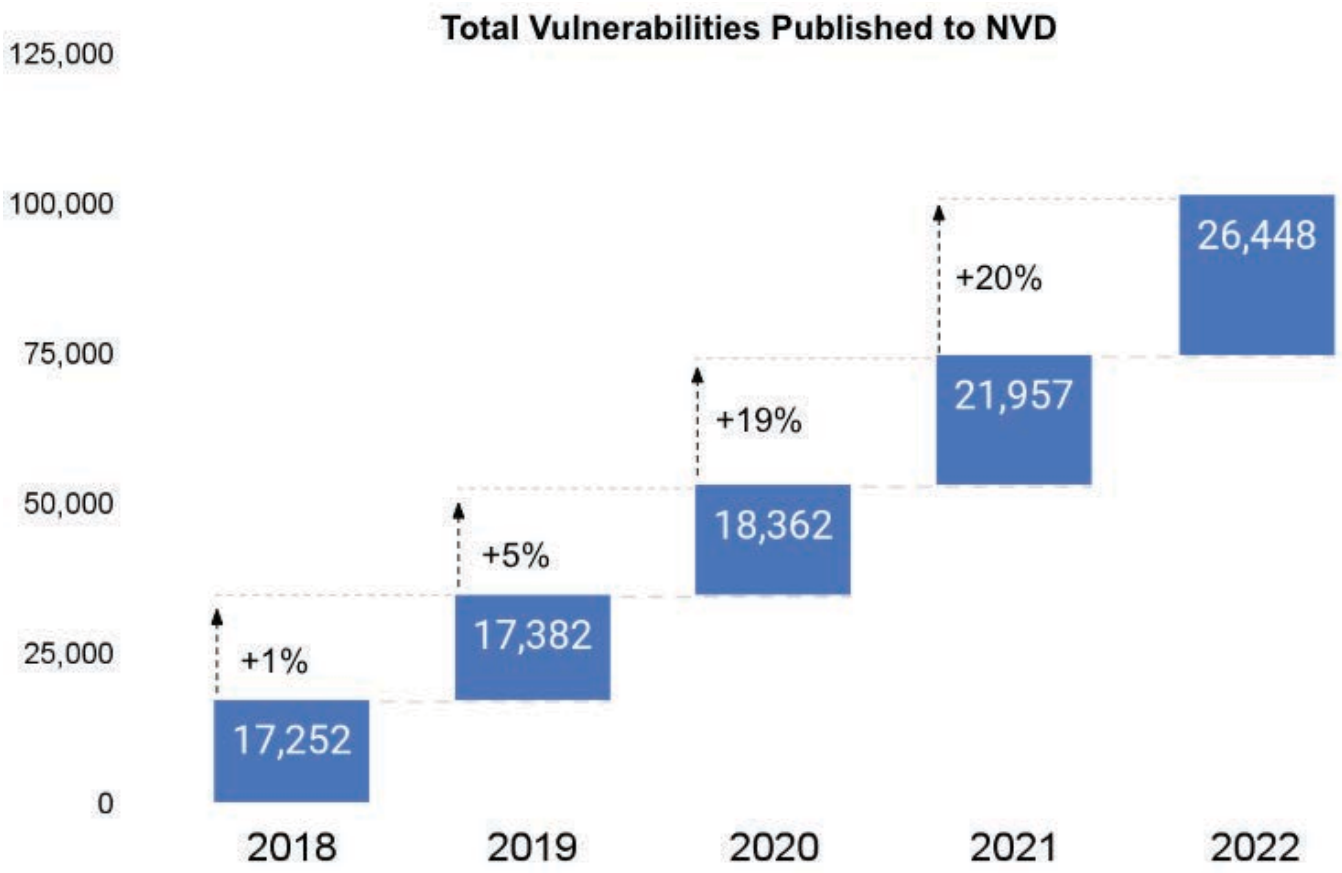

Figure 14: *Percent increase in annual total number of vulnerabilities published to the NVD from 2018 to 2022. Annual totals include any vulnerability with a release date that fell within a specified year, which may differ from the year listed within a CVE ID. (Source: NIST NVD)*

ProxyNotShell

CVE-2022-41082 and CVE-2022-41040, together known as "ProxyNotShell", were initially observed as being actively exploited in September 2022, before they had even been assigned CVE IDs. Reported to Microsoft through Trend Micro's Zero Day Initiative, the vulnerabilities, which affect Microsoft Exchange, could be chained and exploited to achieve remote code execution. It wasn't until November 2022 that Microsoft released patches for CVE-2022-41082 (an RCE vulnerability) and CVE-2022-41040 (a Server-Side Request Forgery vulnerability), after which security researchers had determined that the originally shared mitigations were easily bypassable.

Threat actors have exploited these vulnerabilities, which affect Microsoft Exchange 2013, 2016, and 2019 with a publicly accessed Outlook Web App (OWA), to deploy China Chopper and various strains of ransomware [1, 2, 3]. While these vulnerabilities do require authentication to exploit, once such authentication is obtained, the vulnerabilities can be exploited using low-complexity attacks.

Mark of the Web (MOTW)

The MOTW vulnerabilities (CVE-2022-41049 and CVE-2022-41091), which allow malware to bypass Microsoft's ability to detect files downloaded from the internet, went from a generally unclear but heavily warned-against threat in October 2022 to an infection vector for ransomware and botnets in November 2022. HP reported that criminals distributing the Magniber ransomware were exploiting CVE-2022-41091, and BleepingComputer reported on multiple episodes of exploitation, including one that spread Qbot malware. Given Qbot's links to follow-on ransomware attacks, its adoption of MOTW vulnerability exploitation should prompt network defenders to fix these vulnerabilities as soon as possible.

CVE-2022-26138

On July 29, 2022, CISA added a critical Confluence vulnerability, CVE-2022-26138, to its catalog of known exploited vulnerabilities (KEV) as a result of evidence of identified active exploitation. A remote, unauthenticated attacker with knowledge of a publicly disclosed, hard-coded password could exploit the vulnerability to log in to Confluence and view and compromise any pages that the Confluence users group has access to.

This zero-day Confluence vulnerability, originally disclosed in June 2022, has been exploited by numerous threat actors, including the AvosLocker Ransomware Gang, the operators of the Cerber 2021 Ransomware, Kinsing, and threat actors interested in carrying out illicit cryptocurrency mining activities.

Vulnerability Trend Overview

The disclosure and exploitation of vulnerabilities throughout 2022 followed 4 notable themes. First was the increased rate at which Apple and Google, among other major software vendors, released information about zero-day vulnerability exploitation. Second, these zero-day (and other high criticality) vulnerabilities were often quickly exploited by ransomware and Chinese state-sponsored threat actors. Third, the exploitation of the Log4j vulnerabilities, including Log4Shell, was ongoing across all quarters in 2022. And finally, Microsoft's back and forth over the automatic disablement of macros caused threat actors to adjust their campaigns to account for the potential loss of a once-reliable phishing technique.

Zero-Day Vulnerabilities Dominate All Quarters

Through 2022, newly disclosed vulnerabilities were often exploited to get malware onto victim systems in the first place. Many of these vulnerabilities affected Microsoft systems; and while vulnerabilities in Microsoft systems have long been among the most exploited, a trend between 2021 and 2022 was the increased rate at which other major software vendors — specifically, Apple and Google — released information about zero-day vulnerability exploitation:

- In March 2022, Apple and Google issued emergency updates for 3 zero-day vulnerabilities (CVE-2022-22674 and CVE-2022-22675 for Apple; CVE-2022-1096 for Google).
- In April 2022, Google released an emergency patch for CVE-2022-1364, which it confirmed was exploited in the wild.
- In May 2022, Apple flagged another security advisory for CVE-2022-22675 when it disclosed that it affected more systems than previously known.
- In July 2022, Google patched a high-severity zero-day vulnerability, CVE-2022-2294, which was first reported to them by Avast.
- In August 2022, both Google and Apple again released patches for 3 zero-day vulnerabilities affecting Chrome and iOS systems, respectively: CVE-2022-2856, CVE-2022-32893, and CVE-2022-32894.

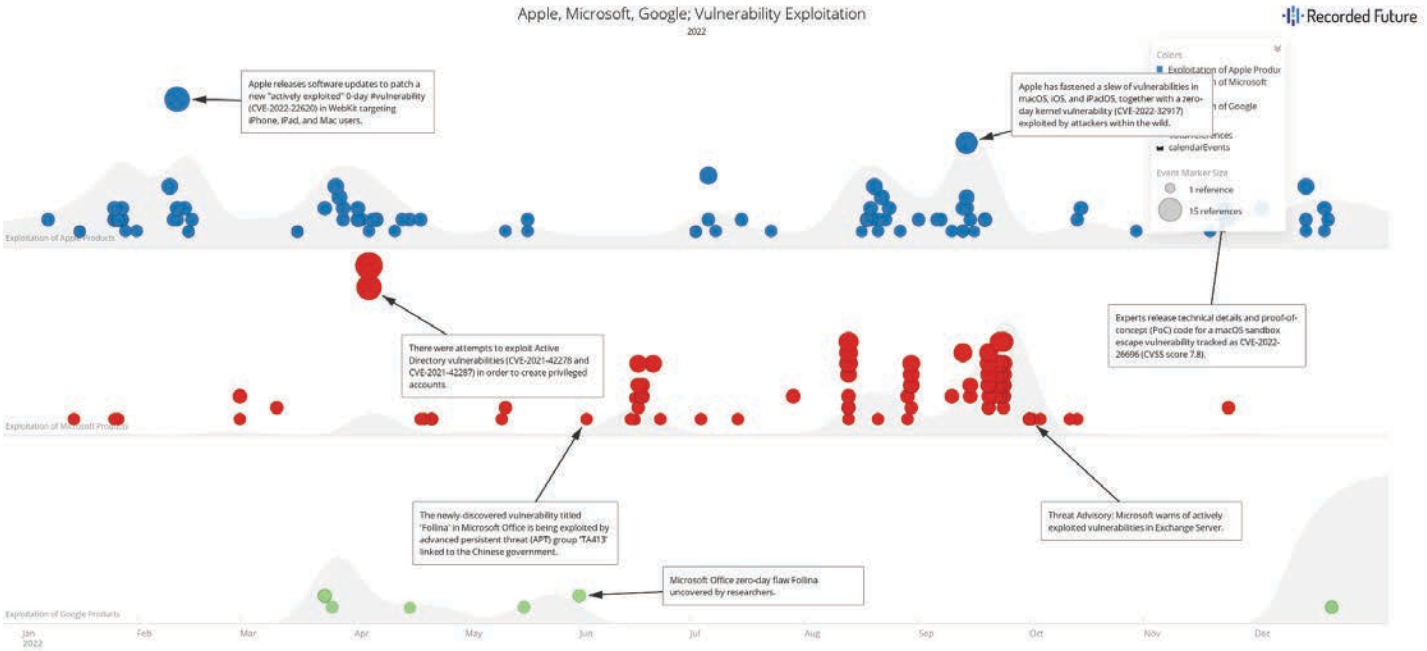

***Figure 15**: Timeline demonstrating ongoing exploitation of zero-day and high-criticality vulnerabilities affecting **Apple**, **Microsoft**, and **Google** products (Source: Recorded Future)*

- In September 2022, Apple patched CVE-2022-32917, a zero-day vulnerability affecting both macOS and iOS.
- In October 2022, Apple released a security update that addressed the ninth zero-day vulnerability that was identified as affecting iOS devices since the beginning of the year, specifically CVE-2022-42827.

For Apple especially, the regular news of zero-day exploitation mirrored ongoing reports of spyware affecting iPhone and Android devices, mainly from the Israeli spyware vendor NSO Group. The twin trends of these attacks were the severity of the vulnerabilities involved and the types of targets affected. Some of these attacks were "zero-click", meaning that victims need not even interact with a malicious message or exploit for attackers to compromise their device. In April 2022, for example, The Citizen Lab published a blog about a zero-click exploit, "HOMAGE", targeting iPhones belonging to Catalan politicians, journalists, and activists. That victimology lines up with the second trend: targets of NSO Group spyware in the last year (and before) tend to be dissidents or activists in countries including Armenia, Bahrain, Catalan, Côte d'Ivoire, Egypt, Greece, Indonesia, Madagascar, Saudi Arabia, Serbia, Spain, Thailand, and Uganda. Although these campaigns are highly targeted, the major risk associated with zero-click exploits is that, like the ETERNALBLUE exploits leaked in 2017, they will be stolen or misused in broader campaigns with massive attack-surface potential against mobile users.

Another Microsoft vulnerability used to target victims in broad campaigns was Follina (CVE-2022-30190), which represents the last of the major trends associated with vulnerability exploitation in the last year: a movement away from macros as a vector for exploiting Windows systems via malicious documents. In 2022, Microsoft announced that it would disable macros by default given their potential for exploitation. In the same month (April 2022) that Microsoft planned to enact this change, operators of the Emotet botnet discarded macro-based attacks, and within the next several months, attackers were seen exploiting Follina (in May) and DogWalk (CVE-2022-34713) (in August) in malicious documents that did not require macros.

Ransomware and Chinese Groups Capitalize on Critical Vulnerability Disclosures

Throughout 2022, ransomware gangs and more sophisticated threat actor groups, in some cases state sponsored, widely exploited zero-day vulnerabilities, tending to focus their exploitation activity on vulnerabilities that are widely reported on in association with, or sometimes in the run-up to, the release of patch information.

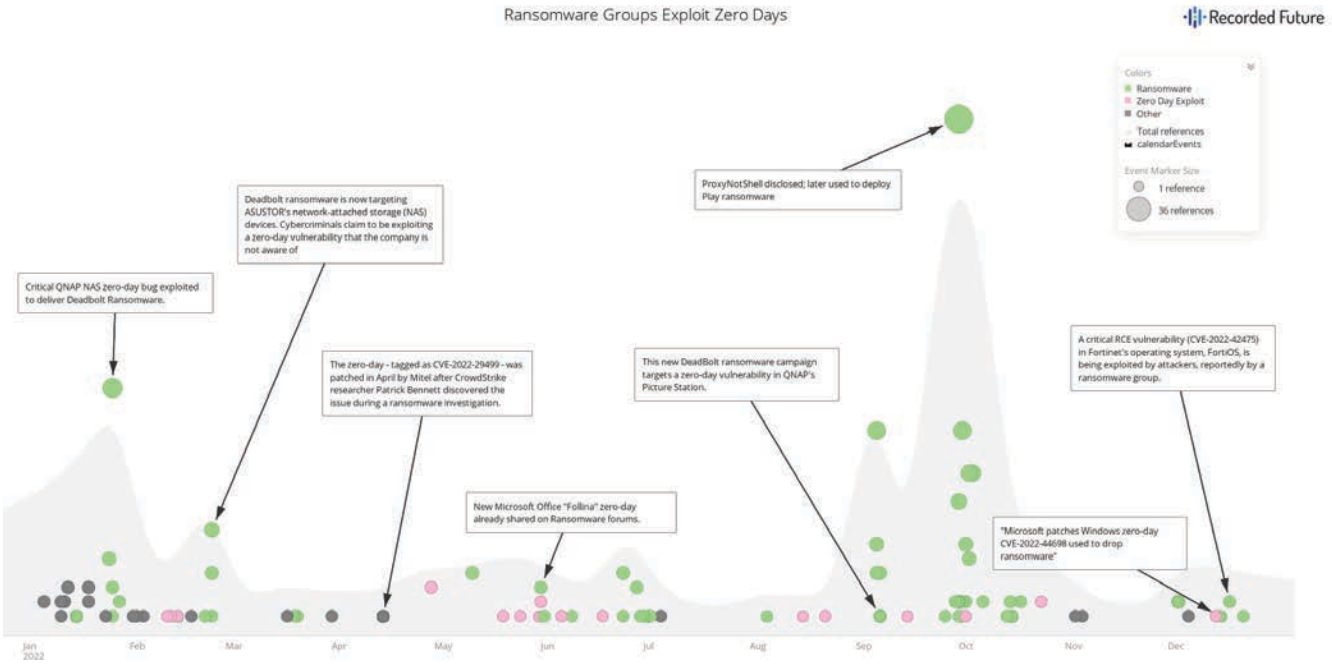

***Figure 16**: Timeline demonstrating the consistent exploitation of zero-day vulnerabilities by ransomware groups (Source: Recorded Future)*

Numerous ransomware campaigns exploited zero-day vulnerabilities in December 2022 alone. Security researchers observed the Magniber Ransomware Gang exploiting CVE-2022-44698, the MOTW zero-day vulnerability that affects the Windows SmartScreen security feature. The Cuba Ransomware operators capitalized on the disclosure of the zero-day vulnerability CVE-2022-24521, exploiting it post-disclosure to carry out ransomware attacks against critical infrastructure, as reported by a joint Cybersecurity Advisory (CSA) published in December 2022. And the Play Ransomware Group chained exploits for the ProxyNotShell vulnerabilities (CVE-2022-41040 and CVE-2022-41082) to exploit Outlook Web Access (OWA) and carry out ransomware attacks.

Ransomware groups were not the only threat actors exploiting zero-day vulnerabilities throughout 2022. Chinese-nexus threat actors APT5 (UNC2630, MANGANESE) exploited various high-criticality and zero-day vulnerabilities, including a zero-day vulnerability affecting Citrix products, CVE-2022-27518, in December 2022. Earlier in the year, Microsoft disclosed that an unspecified China-linked threat actor exploited an Atlassian vulnerability (CVE-2022-26134) to gain access to an unnamed US-based organization and noted that the attack occurred 4 days before the flaw had been disclosed in June 2022.

Microsoft's disclosure was included within a larger report published by the media giant, which alleged that Chinese government-backed actors are taking advantage of China's vulnerability disclosure rules and regulations to exploit such vulnerabilities. In July 2021, the Cyberspace Administration of China (CAC) published stricter rules regarding how organizations within the country should disclose vulnerabilities to the government before sharing the information to organizations associated with the affected product. The Record indicated that there were concerns that the Chinese military would exploit any zero-day vulnerabilities they may discover, and Microsoft alleged that the regulations might further enable China-backed actors to weaponize those vulnerabilities. However, the US Department of Homeland Security's Cyber Safety Review Board said to the Chinese government that there was no evidence of China exploiting any of the discovered vulnerabilities for malicious purposes.

The Chinese government has maintained a consistently dismissive attitude toward cybersecurity companies that accuse it of sponsoring APT attacks; however, we have previously reported on how the Chinese National Vulnerability Database (CNNVD) altered the original publication dates in its public database for at least 267 vulnerabilities to hide evidence of its evaluation process and obfuscate which vulnerabilities the MSS may have been using in offensive cyber operations.

Regardless of the potential effects of China's vulnerability reporting requirements on the exploitation of zero-days in particular, well-resourced Chinese groups continue to exploit vulnerabilities in great number. While we cannot forecast the specific products that will be affected by critical or zero-day vulnerabilities throughout 2023, well-resourced groups, specifically ransomware and state-sponsored threat actors, will surely and quickly capitalize on vulnerability disclosures to carry out attacks involving the exploitation of products by prominent technology vendors.

The Shadow of Log4Shell

Existing within the Log4j logging library since 2013 (and privately disclosed to Apache in November 2021 by a security researcher), CVE-2021-44228, otherwise known as Log4Shell, significantly disrupted the cyber threat landscape when it was publicly disclosed on December 9, 2021. The vulnerability allows a remote actor to send a crafted HTTP packet to Apache servers running any Log4j versions older than 2.15.0. This vulnerability received considerable attention at the end of 2021 from cybersecurity researchers, defenders, and threat actors due to its ease of exploitation and the widespread use of Log4j across networks and applications. However, reports emerged through the end of 2022 about the active exploitation of the vulnerability.

While Apache released an emergency fix (2.15.0) for the vulnerability on December 9, 2021, researchers quickly identified a second vulnerability, tracked as CVE-2021-45046, within the patch, which did not disable message lookups and could allow denial-of-service (DoS). On December 14, 2021, a second patch (2.16.0) was released to mitigate the DoS flaw; however, on December 17, 2021, Apache released yet another patch (2.17.0) after discovering an additional DoS flaw, CVE-2021-45105, in 2.16.0.

Based on a review of prominent reports referencing Log4Shell during 2022, a large subset of exploitation activity centered around the exploitation of the vulnerability to target vulnerable VMware servers. A sample of such reports are highlighted below; a more detailed list of events can be found in Appendix B.

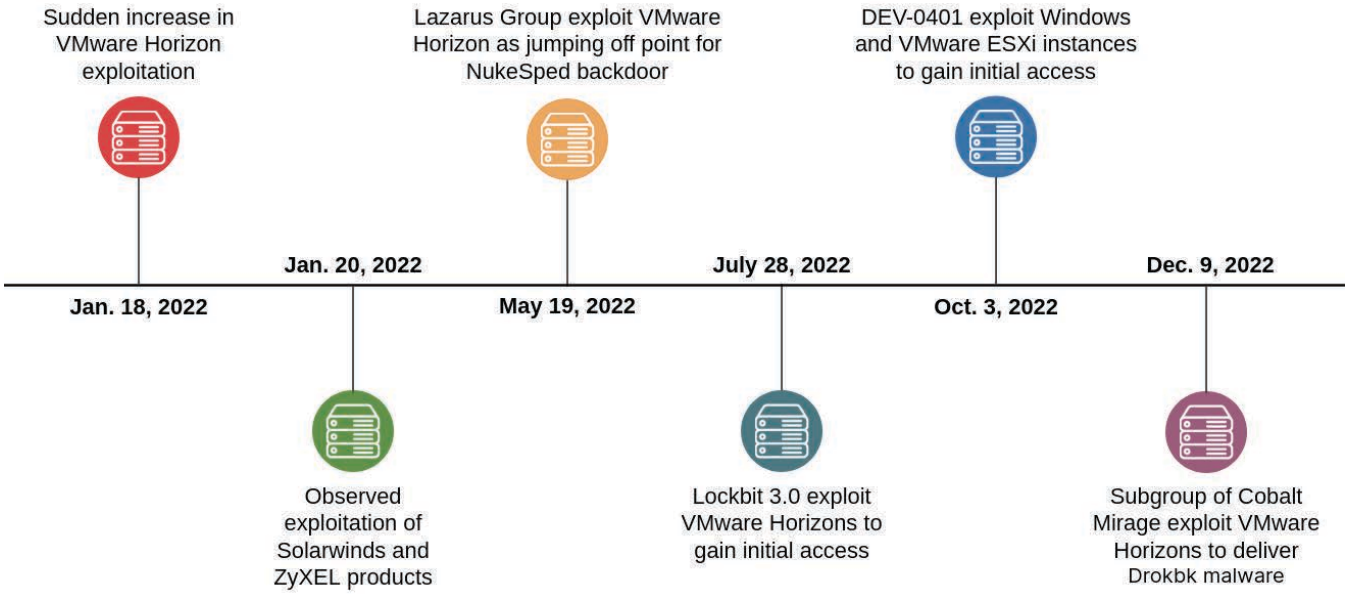

***Figure 17**: Timeline of Log4Shell exploitation targeting VMware systems (Source: Recorded Future)*

Threat actors have continued to exploit Log4Shell as recently as December 2022. Exploitation of an earlier set of vulnerabilities known as ProxyShell, which affect Microsoft Exchange, was also an ongoing threat from multiple threat actors. As we have identified in vulnerability research within the last several years, cybercriminals prefer to target a small set of known vulnerabilities that they can count on to be present on victim systems.

Microsoft's Decision-Making Regarding Disabling Macros by Default

VBA marcos, which are essentially snippets of code embedded within Microsoft Office documents, have historically been used by threat actors of all kinds to carry out phishing attacks. In response to such prolific exploitation, Microsoft released a statement in February 2022 that they would start blocking VBA macros by default later in the year, which they did in April 2022 (XLM macros, or those used in Microsoft Excel documents, have previously been blocked by default in Microsoft 365 tenants.)

However, Microsoft quietly began rolling back the automatic disablement in July 2022 and confirmed that the automatic blocking of macros was on hold on July 8, 2022. This statement was followed shortly by another in which Microsoft confirmed that they would in fact be automatically blocking macros by default later this year. (A statement updated by Microsoft in January 2023 confirms that this is still the plan.)

Despite Microsoft's back-and-forth, threat actors recognized the need to move away from the use of VBA macros in phishing attachments. In the same month (April 2022) that Microsoft initially planned to enact this change, operators of the Emotet botnet discarded macro-based attacks; and within the next several months, attackers exploited both Follina (in May 2022) and DogWalk (CVE-2022-34713) (in August 2022) in malicious documents that did not require macros.

According to Proofpoint, the use of macro-enabled documents in phishing campaigns declined by 66% between October 2021 and June 2022. This data aligns with an overall decrease in references in the Recorded Future Intelligence Cloud to cyber threat activity involving the exploitation of macros following a spike in references in August 2022 (possibly due to discussion of Microsoft's changing stance on disablement by default) and declining through the end of the year.

This shift demonstrates that certain threat actors can adjust their TTPs quickly to account for changes to security solutions and within standard device configurations, and we anticipate that they will continue to do so in 2023.

Closing Statistic: Top Vulnerabilities Referenced by Cybercriminals

The following table lists the vulnerabilities that received the most mentions on our special access forums collection from overall dark web sources. The list breaks down into a roughly even split between vulnerabilities first identified prior to 2022 (such as Log4Shell or Spectre) and those identified in 2022 (such as Follina or ProxyNotShell).

Rank	Vulnerability	Affected Vendor / Component	Risk Score
1	CVE-2022-40684	Fortinet FortiOS, FortiProxy, FortiSwitchManager	89
2	CVE-2021-44228 ("Log4Shell")	Apache Log4j2	99
3	CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 ("ProxyShell")	Microsoft Exchange Server	79
4	CVE-2020-1472 ("ZeroLogon")	Microsoft Netlogon protocol	99
5	CVE-2022-22963	Spring Cloud	89
6	CVE-2022-30190 ("Follina")	Microsoft Windows and Windows Server	99
7	CVE-2022-41040, CVE-2022-41082 ("ProxyNotShell")	Microsoft Exchange Server	64
8	CVE-2017-5753 ("Spectre")	Intel, AMD, and ARM processors	99
9	CVE-2021-42278	Microsoft Windows Server	89
10	CVE-2022-36804	Atlassian Bitbucket	89

Table 3: *Top vulnerabilities by reference count on special-access forum sources in 2022 (Source: Recorded Future)*

We suspect that there is a feedback loop that often determines what criminals will pay attention to in the vulnerability space: for example, researchers disclose a zero-day vulnerability like Log4Shell, which then triggers interest in exploitation from threat actors, which then triggers high levels of exploitation, which triggers further attention from researchers and threat actors in turn, and so on. It is likely that both security practitioners and criminals have limited time to dedicate to vulnerability prioritization, and thus both rely on highly publicized vulnerabilities to drive operations.

Section V: Ransomware and Data Extortion Intelligence

Ransomware was a true constant in the 2022 threat landscape. It found its targets opportunistically and did not discriminate against entities of any size, in any industry, or based in any country.

This dominance emboldened groups to test out implications to their services that went beyond conventional encryption or exfiltration of victim data, such as through the selling of ransomware-as-a-service (RaaS) kits or through the "triple extortion" campaigns perpetrated by the prolific LockBit ransomware gang. Triple-extortion campaigns add on the threat of disruptive DDoS attacks to the other 2 means of extortion in order to further pressure victims into paying ransom amounts. Even if not all such trials were successful (since triple extortion did not become as widespread as originally thought), ransomware's financial returns from victim payments have allowed threat actors to innovate their attacks in 2022 and into 2023. However, these returns also dropped by 60% in 2022, mainly due to 2 factors: first, increased guidance from governments on the risk of OFAC sanctions concerning ransomware payments; and second, what is likely an increased due diligence on cybersecurity standards from insurance companies when underwriting policies for ransomware attacks.

Background: Ransomware, Data Extortion, and Data Wipers

Many kinds of threat actors using various tactics operate in the truly large space that is often collectively referred to as "ransomware". Indeed, experts like Recorded Future's Allan Liska have acknowledged that defining ransomware is somewhat of a moving target.

For the purposes of this report, "ransomware" will refer to malware that seizes a victim's information asset and demands some kind of action to return the asset; threat actors may encrypt the information and threaten to destroy it. Similar to ransomware, data extortion implies threat actors exfiltrating victim data to extort money from the victim to return the files. In both of these cases, a threat actor will likely notify the victim directly that they have seized their asset, and there may be a negotiation process between the victim and the threat actor. In the case that these negotiations fail, threat actors may escalate the situation with double-extortion, or a "name and shame" technique in which threat actors will post a ransom note to their public data leak sites. By openly calling out the victim, the threat actor seeks to pressure the compromised organization to pay the ransom.

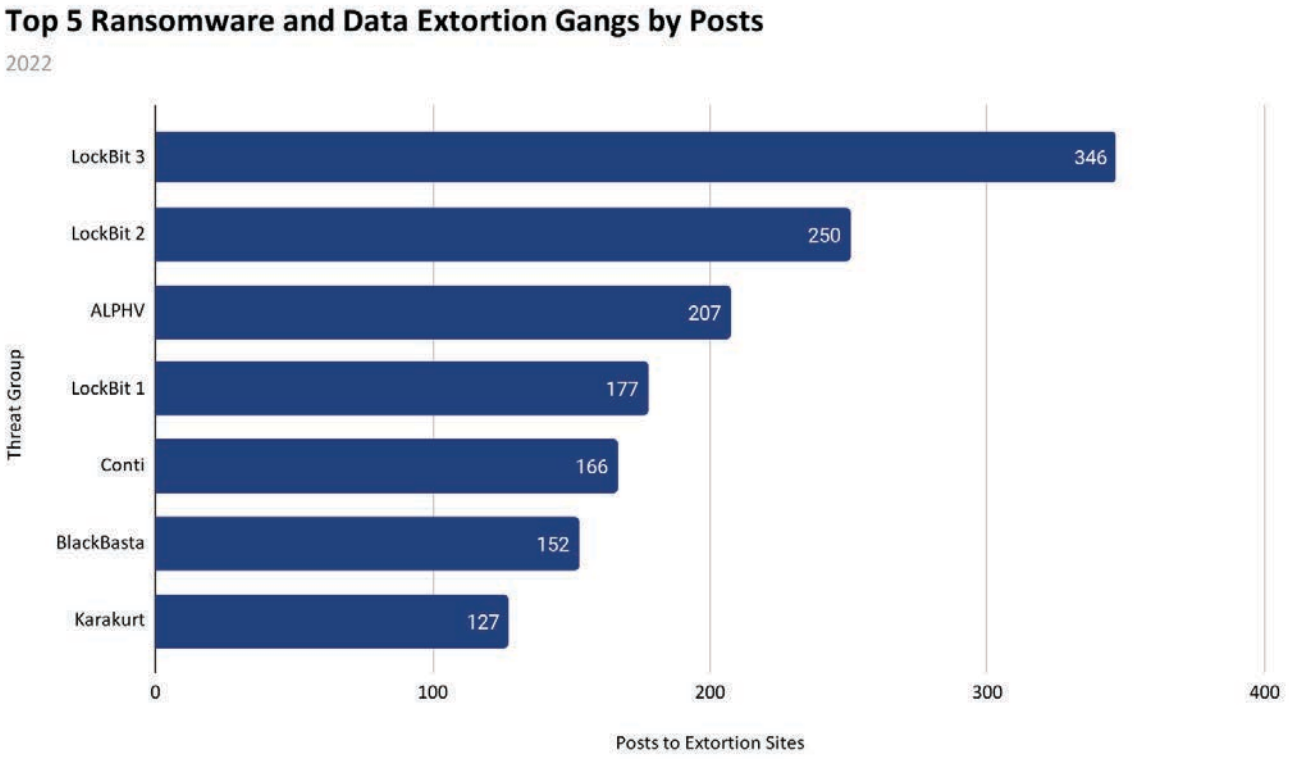

Figure 18: *The top 5 most active ransomware and data extortion groups by events reflected in public ransomware notes (Source: Recorded Future)*

Ransomware actors are also predominantly financially motivated actors who target victims opportunistically, given that most attacks center around a ransom payment to release the captured information asset. However, we did observe several instances throughout 2022 of ideologically motivated threat actors deploying data wipers to seize malware. Unlike ransomware, these data wipers either overwrite or destroy data to ensure that the victim cannot recover it.

The 5 Most Active Ransomware Groups of 2022

Even if ransomware itself was a constant throughout 2022, the top threat actor groups that perpetrated it often fluctuated and, in some cases, even disbanded. We identified the 5 most active ransomware gangs and data extortion groups in 2022 according to the volume of available ransom notes and information collected by Recorded Future data.

While the number of victims posted online by ransomware groups is only a percentage of all the organizations they target, we still believe it offers sufficient insights to understand targeting patterns and overall levels of activity.

LockBit was by far the most active group of 2022, with a consolidated amount of recorded events that superseded those of its 4 other competitors put together. This was also reflected in LockBit's extortion process, which tended to demonstrate a unique administrative organization — especially after the launch of LockBit 3.0. Indeed, LockBit's extortion notes provided the most detailed information about its victims. Consider the amount of information in a ransom note from LockBit to one of its victims in the construction sector. The post outlines the amount of data stolen (29 GB), the date when the data was uploaded (June 29), the deadline (July 11), the ransom amount ($200,000) and even the amount required to extend the deadline by 24 hours ($1,000). Compare this to information from groups like BlackBasta, whose public posts provide little metadata on their attacks.

Ransomware-as-a-service (RaaS) kits were consistently popular throughout 2022, especially those sold by groups like LockBit and Conti. RaaS, a business model that allows threat actors to purchase a group's ransomware for their own use (and to subsequently become affiliates of the group), helped lower the barriers to entry into ransomware attacks. However, more access to ransomware also meant that actors who were not versed in certain norms around cybercrime could conduct attacks. In late December 2022, the LockBit ransomware gang publicly apologized and released a free decrypter after it launched a cyberattack on the Hospital for Sick Children (also known as "SickKids"), a Canadian healthcare center, and noted that the affiliate responsible for the intrusion was no longer part of LockBit Gang. LockBit Gang's policy for their ransomware operations

specifies that its affiliates are prohibited from targeting medical organizations, as damaged files and compromised medical equipment or systems may lead to death.

LockBit

LockBit ransomware was on its third variant, LockBit 3.0, by the end of 2022. A notable trend identified within Lockbit's activity this year was its quasi-adoption of a new extortion model. While the advertised triple-extortion model was only identified as being purportedly used once, its updated extortion model, which allows for the purchase of stolen data while attacks are ongoing, highlights the group's ability to adopt new tactics to increase attack monetization.

ALPHV

ALPHV, also known as "BlackCat", is a group that uses ALPHV ransomware, with preliminary activity recorded as early as December 2021. On April 19, 2022, the FBI released indicators of compromise (IOCs) for the ALPHV ransomware group, which has compromised at least 60 organizations worldwide as of March 2022 and was the first ransomware group to use ransomware with the Rust programming language (the majority of ransomware is written in C# and C++). This linguistic ability allows the group to go after targets on major operating systems such as MacOS, Linux, and Windows.

Conti (Defunct)

Conti ransomware was operated by the Conti ransomware group before disbanding its operations in May 2022. Despite its cutoff of activity mid-year, the group managed to be one of the most active of 2022, partly due to its use of the RaaS model to distribute malware. The group also confirmed suspicions of its ties to Russian intelligence through leaked group communications. Its members have since either split into other groups (such as BlackBasta, detailed below) or moved to provide their expertise to existing groups such as Hive and ALPHV.

BlackBasta

BlackBasta ransomware first surfaced in April 2022, when researchers reported that the ransomware gang was conducting double-extortion ransomware campaigns, stealing corporate data and documents before encrypting files on victim machines. Its creation right before Conti's disbandment makes it likely that BlackBasta was 1 of the primary groups that Conti members left to join. The BlackBasta Gang continued to publish information on the Basta News Tor site about victims who did not pay their ransom; for example, it did this for Canada's largest packaged meat producer, Maple Leaf Foods Inc., in November 2022.

Karakurt

Because Karakurt exclusively employs data extortion tactics, it is discussed in the **The Rise of Data Extortion** subsection of this report.

Ransomware Metrics

Ransomware's Universal Reach

The top host countries in 2022 for entities affected by ransomware were the US, the UK, Germany, Canada, and France, which demonstrated a steady pattern of attacks affecting companies in the Global North. Figure 19 below illustrates ransomware attacks by country over the past year.

It is important to understand why threat actors have preferred companies primarily located in Europe and North America. Consider the example of LockBit, who stated that "insurance in this area is developed in the United States of America and the EU, and it is here that most of the world's richest companies are concentrated". Here, Lockbit's spokesperson is referring to cybersecurity insurance that companies purchase to mitigate some of the risk posed by ransomware attacks. Both points of this statement indicate that threat actors are likely to prefer targets they believe have more resources to engage with threat actors.

This indicates that these same threat actors are forced to accept the risk that comes with targeting companies hosted in countries that are perceived as wealthier and more developed, with stronger defense and government institutions. This is likely because they see the chance of law enforcement action from national governments and their institutions as both longer-term and lower when compared to the immediate financial gains from ransomware activity. These threat actors are likely prepared for some degree of eventuality of being discovered by these same, highly resourced governments, such was the case with Mikhail Vasiliev, a Russian-Canadian national recently charged with involvement in the LockBit gang.

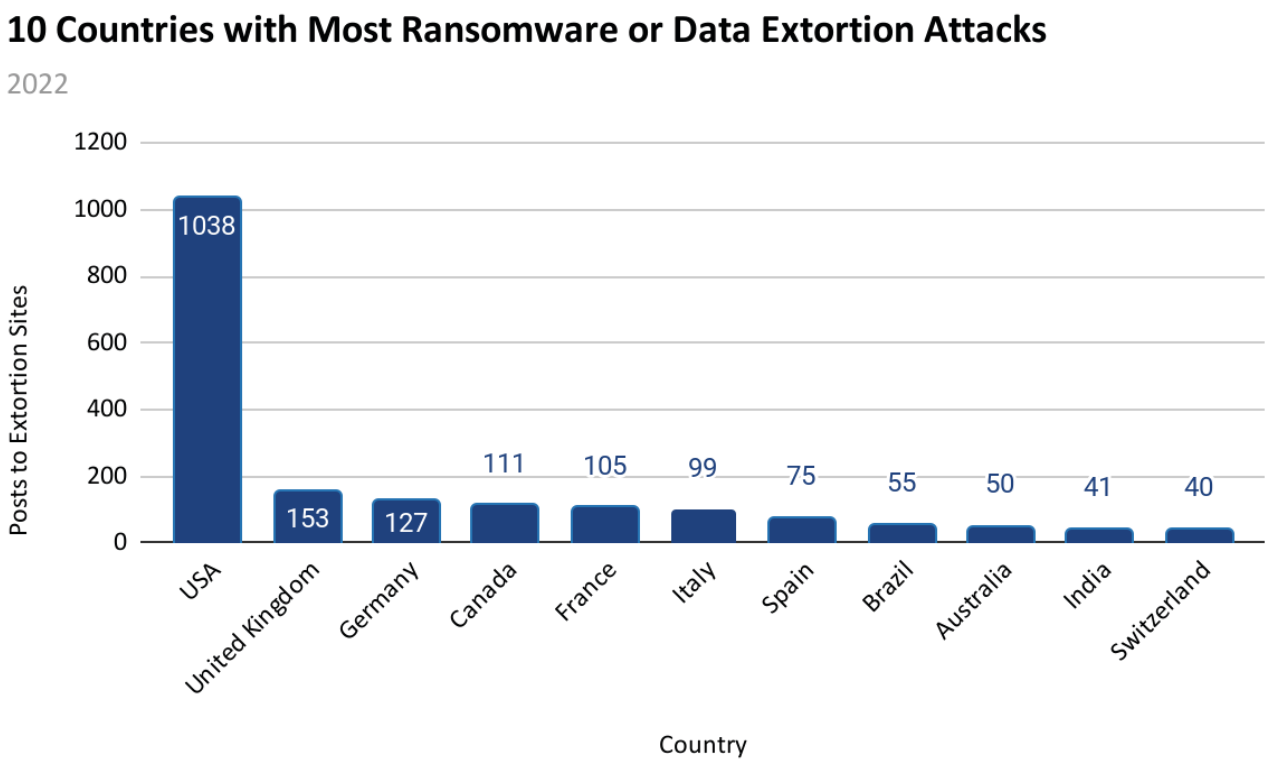

Figure 19: *The 10 countries with the most ransomware and data extortion attacks in 2022, by posts to extortion sites (Source: Recorded Future)*

Countdown to "All Available Data Published"

Methodology Note*: We analyzed a sample of 5% of ransom notes from each of the 5 most active actors that contained relevant timeline information (see the* ***The 5 Most Active Ransomware Groups of 2022*** *subsection).*

To understand the timelines that ransomware and extortion groups set for victims, we surveyed a subset of ransomware threat digests. Most of the information contained in these notes was about extortion timelines. 60 days was the longest amount of time between ransomware operators posting public ransom notes and the set deadline for victim payment, for an attack against an automotive and manufacturing company by the Conti gang in March 2022. The shortest amount of time was 14 hours, as observed in 2 attacks that used LockBit ransomware; the average amount of time was approximately 10 days.

Despite the wealth of timing data available, not all timelines are publicly disclosed by threat actors. This is mainly for 2 reasons. The first is simply that different threat actors vary in their organization and consistency, and therefore, their extortion advertisements on their websites vary as well. As an example, LockBit provided the most detailed timelines for notice and deadlines on its extortion website — a level of organization indicative of how well-resourced the threat group is. The second, more nefarious reason is that threat actors often sell victims' information to other threat actors, as demonstrated in the screenshot contained in this reference. This lends itself to further, more serious damage to victims' data. A higher bidder may have bought employee information, for example, to test stolen payment data in order to conduct fraudulent purchases.

The Relative Definition of "a Lot of Data"

Methodology Note: *We analyzed a sample of 5% of ransom notes from each of the 5 most active actors that contained relevant information on seized data amounts.*

The largest amount of data released for a recorded victim this year was 40 TB, which was the amount purportedly stolen by LockBit in November 2022 from the major automotive parts manufacturer Continental AG (which was held for ransom for "just 40 million dollars"). The smallest amount of data for a victim in this sector was just 7.9 MB, purportedly stolen by LockBit; the average amount was approximately 500 GB. For comparison, the Ashley Madison data breach that occurred in 2015, which was considered "massive" at the time, only involved about 60 GB of data.

The amounts of data taken can vary greatly and are relative to the size of the affected organization. While 990 MB may not be a lot of information for a top car manufacturer, it is more significant for small or medium-sized companies. And the size of the stolen data is not necessarily a good indicator of a breach's severity. It is more useful to consider the kinds of information that have been collected, which also depends on whether threat actors purposely selected the kinds of information to hold for ransom or simply seized random amounts.

The Rise of Data Extortion

A growing number of cybercriminal groups in 2022 specialized in data extortion without using ransomware payloads, relying instead on identifying confidential information of high value and inflicting public embarrassment via social media to coerce victims. In addition to the loss of brand reputation and operational downtime, these groups also seek to create potential competitive disadvantages by publishing or monetizing proprietary IP like source code.

There are pros and cons to this approach. One advantage is the decreased reliance on ransomware payloads for launching a successful attack. Ransomware affiliates who penetrate target networks always suffer the risk of encryption failing, which has been a source of criticism by affiliates in certain RaaS programs like Lockbit, when Lockbit was found to be renaming instead of encrypting files on network drives. Ransomware payloads also have a higher chance of being detected by security software, as encryption is a "noisy" process from a defender's perspective. However, the tradeoff is that threat actors need to dwell on victim infrastructure without being detected for long enough to identify and exfiltrate sensitive data, which raises the bar in terms of required skill.

Given their reliance on exfiltrating confidential data of high value, some extortion groups adopted a targeting rationale that differs significantly from that of traditional ransomware groups. While ransomware gangs typically target organizations opportunistically, data extortion groups like LAPSUS$ typically focus on compromising large organizations with valuable data, as demonstrated by the group's compromise of major tech firms including Uber, Microsoft, Nvidia, Okta, Globant, Samsung, Ubisoft, Rockstar Games, and T-Mobile, all in 2022 alone. The following source code repositories, which were leaked or sold by LAPSUS$, could have been used by cybercriminals to develop exploits or by competitors to develop competing products, leading to either further risk or competitive disadvantage.

- **February 2022**: LAPSUS$ stole over 1 TB of source code and company data from Nvidia, including source code for the company's proprietary Deep Learning Super Sampling (DLSS) technology.
- **March 2022**: LAPSUS$ uploaded 190 GB of source code for Samsung's Galaxy and TrustZone products, including source code for access control and authentication features, to torrent websites.
- **March 2022**: LAPSUS$ uploaded over 46 GB of source code for over 250 Microsoft projects from a compromised Microsoft Azure Devops Server, including the source code for Bing, Bing Maps, and Cortana.
- **April 2022**: LAPSUS$ stole over 30,000 repositories of source code from a T-Mobile Bitbucket server. The contents of the source code were not confirmed.
- **September 2022**: A LAPSUS$-affiliated threat actor reportedly sold the source code for Grand Theft Auto (GTA) V, Rockstar Games's latest video game in its leading franchise. According to Rockstar Games's parent company, 2K Games, the threat actor also stole source code for GTA VI.

Ransomware groups have also understood this tradeoff in risk, and have likely sought to diversify their tactics in response. For instance, Karakurt is a prolific threat actor that emerged in the past year and is believed to be a subgroup of Conti. According to a CISA advisory released on June 1, 2022, Karakurt is believed to have benefited from Conti's supply chain of victims obtained from affiliates and IABs to target victims swiftly and frequently, relying on data theft, rather than encryption via Conti ransomware, to extort victims. Insikt Group has tracked more than 150 victims uploaded to Karakurt's victim website since December 2021.

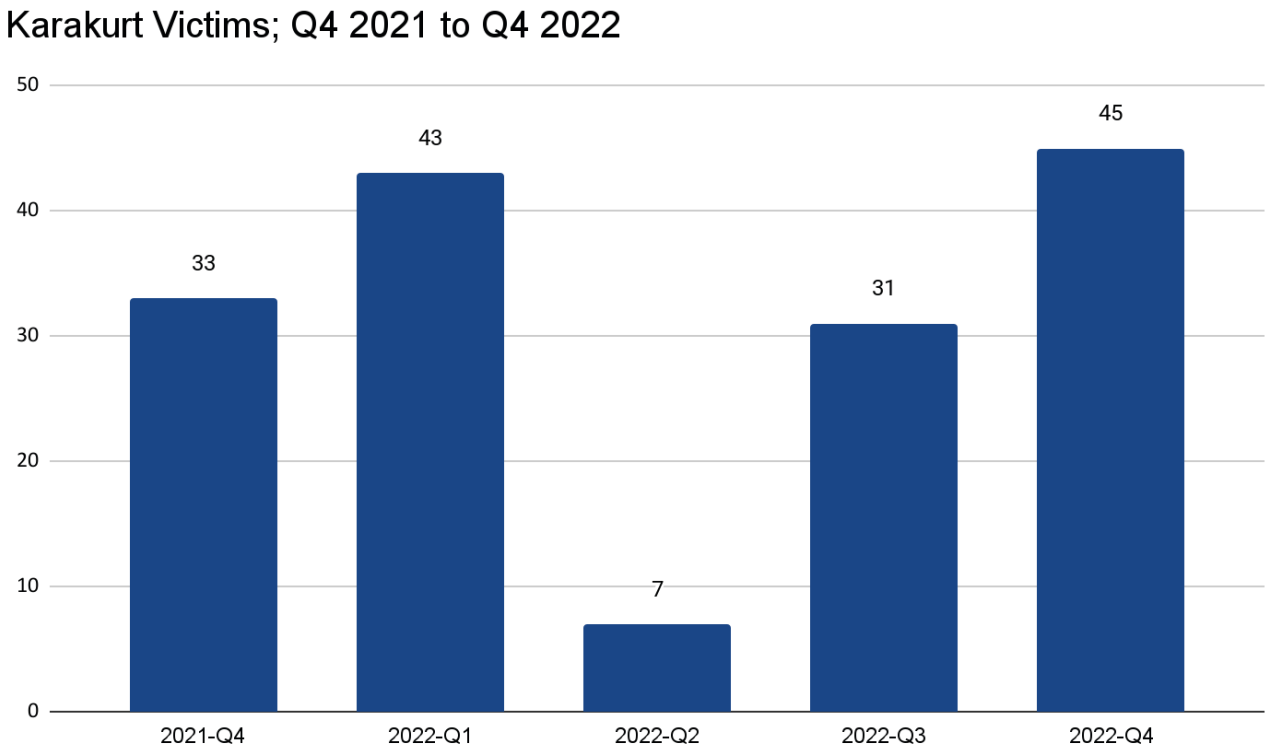

Figure 20: *Number of victims posted to Karakurt's extortion website since Q4 2021 (Source: Recorded Future)*

Another common feature among data extortion groups that differs from traditional ransomware groups is the attention paid to generating publicity around victims. For instance, while Karakurt operated a clearweb website and a (now-suspended) social media account to publish victims, LAPSUS$ publicly claimed responsibility for victims on a Telegram channel with over 50,000 subscribers, where they ran polls to select victims and made public calls to recruit malicious insiders. LAPSUS$ has also formulated unusual extortion demands, such as asking graphics card manufacturer Nvidia to open-source video drivers in order for users to remove hash rate limits imposed by the manufacturer to deter cryptocurrency mining using Nvidia cards.

Despite the law catching up with LAPSUS$ with 2 of its members reportedly arrested, we assess that other emerging threats are likely to note these groups' success (even if it is fleeting) and adopt data extortion models in 2023. The sheer size and scale of data extortion victims in 2022 will likely send a signal to other threat actors that ransomware payloads are not necessary for extortion to work, and that not using them can help minimize the risk of detection and operational security failures, pushing more threat actors toward this business model. Such a shift in method presents a greater risk to major tech companies and other organizations who seek to protect intellectual property like proprietary source code, as the risk of competitive disadvantage compounds with brand impairment and operational downtime while remediating an intrusion.

Opportunity Versus Intent of Threat Actors

The use of Recorded Future data helps build an understanding of the combination of opportunity and intent among threat actors. To chart this information, we analyzed threat lead data across sectors, which consists of advertisements for system access by threat actors, ransomware extortion site digests, and more. We subsequently identified a total of 3,000 threat leads in 2022, including a total of 2,579 targeted entities in 289 threat leads detailing ransomware attacks. While overall threat leads for 2022 predominantly referenced advertisements for organizations in the finance, government, and retail sectors, ransomware events predominantly affected manufacturing, professional services, and government organizations, as shown in Figure 20.

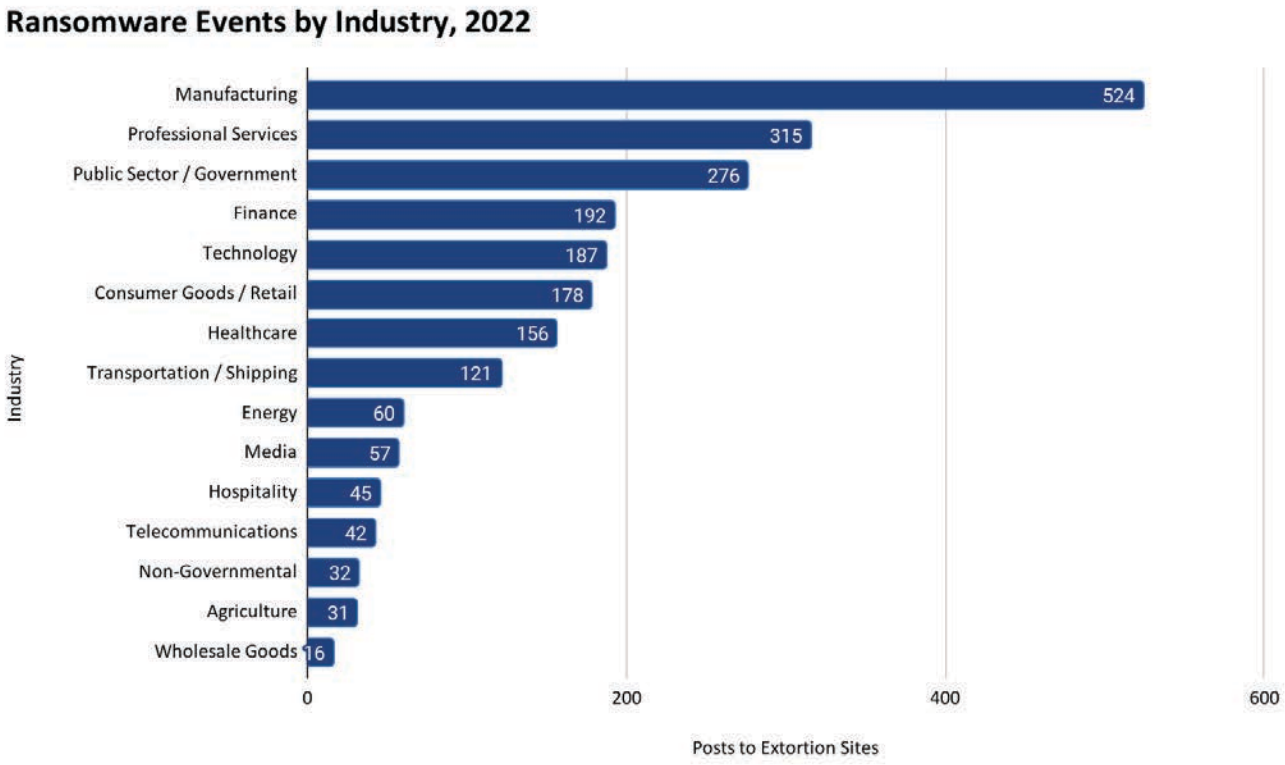

Figure 20: *Ransomware attacks in 2022 by industry and sub-sectors, by posts to extortion sites (Source: Recorded Future)*

For comparison, while 1,080 threat leads in 2021 similarly referenced entities in the financial and government sectors, they also frequently mentioned software companies. Of the total notes for 2021, 316 ransomware threat notes indicated that manufacturing, construction, and information technology were the sectors most affected by ransomware and data extortion actors.

The manufacturing sector's high representation among 2022 threat lead numbers indicates 1 of 2 trends: either the sector may be more attractive to threat actors, or the sector is more vulnerable to opportunistic attacks. This higher number of attacks also extends to manufacturer suppliers that form the complex "just-in-time" supply-chain model. For example, although Toyota itself was not publicly known to be directly breached by a ransomware actor in the past year, many of its suppliers were. Additionally, when Kojima Industries, Toyota's electronics and plastic supplier, suffered a breach in February 2022, the car manufacturer was forced to halt production.

Looking Ahead: Ransomware and Regulation

The motivations of threat actors to perpetrate ransomware or data extortion activities is unlikely to decrease in 2023. However, in an attempt to stem the steady stream of ransomware attacks, some countries are considering banning ransomware payments to stop incentivizing threat actors. In light of numerous recent attacks (including ransomware incidents) in late 2022, Australia stated that it was considering whether companies should be allowed to pay ransoms to attackers. In the next 12 months, it will be important to monitor whether such policy changes become a reality and, furthermore, a pattern among different national regulators. Companies should subsequently watch these developments to ensure that they are in line with national regulations in the event of a breach.

Other countries, like the US, have chosen to go on the offensive against ransomware groups. This includes concentrated efforts on everything from seizing ransom payments from threat actors (like the Department of Justice announcing it had seized the "majority" of the ransom payment from the May 2021 Colonial Pipeline ransomware attack) to the January 2023 announcement that the FBI had seized control of the Hive ransomware extortion site. The Hive ransomware group was the sixth-most active ransomware group in 2022 according to the volume of its ransomware notes from Recorded Future data.

The Australian proposal and the US Department of Justice payment seizures represent alternative endings to demands for ransom payment as governments attempt to increase costs for threat actors and erode their incentives. It does not mean, however, that breached companies should rely on governments being able to seize back cryptocurrency payments, or to shut down extortion or leak websites, in their incident response planning.

To avoid ransom payment situations altogether, the past year of ransomware attacks demonstrates the importance of preemptive mitigation against such attacks. While this includes maintaining updated, offline backups of company data that are regularly tested, threat actors may try to disable recovery functions like backups. As such, segmenting networks will help contain serious damage from a ransomware attack. Mitigation also includes proactive searching for malware such as through Recorded Future's Hunting Packages. A continuous security process should ensure that policies and business continuity plans are periodically reviewed and updated as necessary.

Section VI: Outlook

The targeting of open-source or proprietary software packages posed a significant problem in 2022 and will likely continue and perhaps worsen in 2023. Countless organizations rely upon these packages for day-to-day software development and maintenance of source code, and their security is often taken for granted. As companies not traditionally categorized as technology organizations undergo digital transformation, the use of these packages increases. By targeting these dependencies, threat actors can capitalize on the one-to-many structure of supply-chain attacks. These types of attacks will likely continue throughout the upcoming months.

The number of managed services offerings on dark web marketplaces and forums increased sharply in 2022. These services lower the barrier to entry for less-sophisticated threat actors, allowing more individuals to carry out cyberattacks of low and moderate sophistication. We expect interconnected marketplaces to grow throughout 2023, with increasingly sophisticated offerings moving toward managed models. Additionally, with machine-learning tools becoming increasingly publicly accessible, higher-quality PhaaS models and social engineering campaigns are highly likely to increase drastically. While the quantity and quality of cyberattacks are likely to go up, threat actors will likely keep relying on familiar attack methods like ransomware and phishing, enabling defenders to implement countermeasures with potentially significant results.

One such countermeasure was Microsoft's disablement of macros by default. As evidenced by the success of this countermeasure in drastically decreasing the deployment of phishing attachments using macros, we expect continued adoption of systemic one-to-many security solutions throughout 2023, such as the increased use of memory-safe programming languages and continued adoption of "phishing-resistant" MFA. Though these countermeasures can be effective, threat actors have demonstrated their ability to pivot operations in the face of newly developed or implemented security protections, underscoring the need for a defense-in-depth security strategy that is regularly updated in response to changes in the threat landscape.

The increasing volume of information stolen by infostealer malware highlights not only the ongoing dominance of such malware strains but also the criminal appetite for this kind of information. Authentication information obtained by infostealers is often used by threat actors to bypass conventional authentication and MFA protections. As such, infostealers' exfiltration of authentication information underscores that organizations will need to focus on alternative authentication protections, such as those that involve MFA in addition to advanced user behavior analytic monitoring.

In the vulnerability threat landscape, 2022 was unique in that the disclosure of zero-day vulnerabilities affecting the products of large technology organizations, such as Apple, Google, and Microsoft, came rapidly throughout the latter half of the year. Given such tech giants' resources and market need for creating secure products, these numbers reveal a criminal and nation-state landscape that is increasingly technologically savvy. However, the ongoing successful exploitation of previously reported vulnerabilities like Log4Shell (now already over a year old) underscores that many threat actors do not need to invest heavily in zero-day research; they simply need to be faster than a large proportion of businesses that do not or cannot patch for critical vulnerabilities within several months after disclosure. It is almost certain that threat actors will exploit zero-day vulnerabilities in widely used products through 2023; based on the trend line over the past 5 years, there will likely be more zero-day vulnerabilities in 2023 than 2022.

Finally, ransomware remains an evergreen threat, and 2023 is unlikely to see a complete shift in the criminal calculus behind extortion attacks. As long as any intrusion can be monetized, regardless of industry, company size, or geography, ransomware will remain a highly profitable form of opportunistic cyber threat activity. However, the decrease in average ransom payments in 2022 is an important emerging factor, showing that these campaigns have become less effective and these threat actor groups, entrenched but highly adaptable, will need to shift their tactics to maintain high ransoms. Such shifts have already begun. Throughout the year, ransomware and extortion groups have adjusted tactics at both the technical level (through new forms of initial access) and the operational level (such as by moving from double to triple extortion). Moreover, based on the number of ransomware offerings or individual threat groups, any disbandment or realignment of high-profile groups has to be seen in light of the total landscape before it is identified as evidence of a waning form of threat activity. We predict that in 2023, extortion groups are unlikely to fade from the threat landscape. Moreover, if ransomware payments continue to decline, some operators are very likely to engage in increasingly aggressive and destructive tactics to pressure their victims.

Appendix A: Notable Events Related to Russia's War in Ukraine

- **February 3, 2022**: Palo Alto Networks researchers uncovered the operations of a Russia-linked threat actor, "Gamaredon Group", also known as Primitive Bear, which targeted an undisclosed Western government entity in Ukraine.
- **February 12, 2022:** CISA urged all US businesses to mitigate the effects of potential cyberattacks as a result of the ongoing war.
- **February 23, 2022**: Multiple Ukrainian government websites and banks were targeted in a DDoS operation. Simultaneously, security firms ESET and Symantec indicated that entities in Ukraine were also targeted by a wiper malware, "HermeticWiper", which was reportedly "installed on hundreds of machines" in Ukraine.
- **March 19, 2022:** A cyberattack that led to a compromise of the mailbox of Michał Dworczyk, the chief of staff of Polish Prime Minister Mateusz Morawiecki, was attributed to the Belarusian cyber-espionage group "UNC1151", which is linked to the multi-layered Ghostwriter operation. The mailbox is believed to have contained 60,000 emails, including sensitive data from VIPs.
- **March 30, 2022:** Russian APT Gamaredon launched phishing attacks against accounts of NATO and Eastern European militaries in addition to existing campaigns against American NGOs, a Ukrainian defense contractor, and a Balkan military target.
- **June 6, 2022:** Russian threat actors targeted the phones of Ukrainian officials.
- **July 19, 2022**: Google's Threat Analysis Group (TAG) published an update on the continued cyber threat activity in Europe that involves the Russian-linked threat groups Turla, APT28, Sandworm, UAC-0098, Ghostwriter, Callisto, and Lorec53. The report includes an update that Turla, a threat group attributed to the Russian Federal Security Service (FSB), hosted malicious "CyberAzov" applications on a domain that emulated the far-right Ukrainian Azov Regiment.
- **July 21, 2022:** 2 radio stations owned by one of Ukraine's largest broadcasters, TAVR Media, were hacked to spread fake messages that Ukrainian president Volodymyr Zelensky was hospitalized and in critical condition.
- **August 2, 2022:** Ukraine's secret service announced it had dismantled an organized group that created a vast bot farm designed to discredit Ukraine's leadership and destabilize the country.
- **August 15, 2022**: The Microsoft Threat Intelligence Center (MSTIC) released a report about an ongoing phishing and credential theft campaign by Seaborgium, a highly persistent Russia-based, potentially nation-state threat actor. Seaborgium's campaigns target NATO countries and other countries in the Baltics, the Nordics, and Eastern Europe.
- **November 25, 2022:** Up to 12 million customers were without power in Ukraine after Russian air strikes hit critical infrastructure.
- **December 6, 2022:** Russia's VTB Bank was hit by a large DDoS attack, which may have been perpetrated by pro-Ukraine cyber forces targeting Russia's financial system.

Appendix B: Log4Shell Exploitation Targeting VMware Systems

- **January 18, 2022**: Rapid7 researchers reported an active exploitation of Log4Shell aimed at unpatched VMware Horizon servers. Based on Rapid7's telemetry, they observed a sudden increase in VMware Horizon exploitation beginning January 14, 2022.
- **January 20, 2022**: Recorded Future's The Record shared details regarding recent attacks by cybercriminals exploiting the Log4Shell vulnerability to target SolarWinds and ZyXEL products that use the Log4j library inside their software. Microsoft identified the activity after discovering unnamed threat actors abusing Log4Shell in combination with CVE-2021-35247 (an input validation vulnerability affecting the Serv-U web login screen) to bypass input validation on the login process using non-standard characters and then exploiting Log4Shell to take over Serv-U servers.
- **May 19, 2022**: AhnLab researchers detailed the ongoing exploitation of vulnerable VMWare Horizon servers by the Lazarus Group, a financially motivated North Korean threat actor. The name Lazarus Group serves as an umbrella for several subgroups that have conducted extensive operations since as early as 2009. Since April 2022, Lazarus Group has reportedly been exploiting Log4Shell in vulnerable VMWare Horizon servers to deploy the NukeSped backdoor to ultimately install infostealer malware.
- **July 28, 2022**: SentinelOne described a LockBit 3.0 campaign in which LockBit operators exploited the Log4Shell vulnerability on unpatched VMware Horizon servers to gain initial access to compromised systems.
- **October 3, 2022**: DEV-0401 is linked to the operators of the Cheerscrypt Ransomware and to general exploitation of the Log4Shell vulnerability to target Windows and VMware ESXi instances, according to a blogpost by Sygnia.
- **December 9, 2022**: Secureworks reported on Drokbk malware using GitHub as a dead drop resolver to identify its command-and-control (C2) server and run additional commands or payloads. The Drokbk malware is operated by Cluster B. Drokbk, a subgroup of the Iranian government-sponsored Cobalt Mirage threat group, which exploited 2 Log4j vulnerabilities in an unpatched VMwareHorizon, tracked as CVE-2021-44228 and CVE-2021-45046, to deliver the Drokbk malware via a ZIP archive file hosted on an open-source file transfer service.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.