ZEROFOX

2022

Q1 FINANCIAL SECTOR

Financial Quarterly Threat Landscape

ZEROFOX INTELLIGENCE

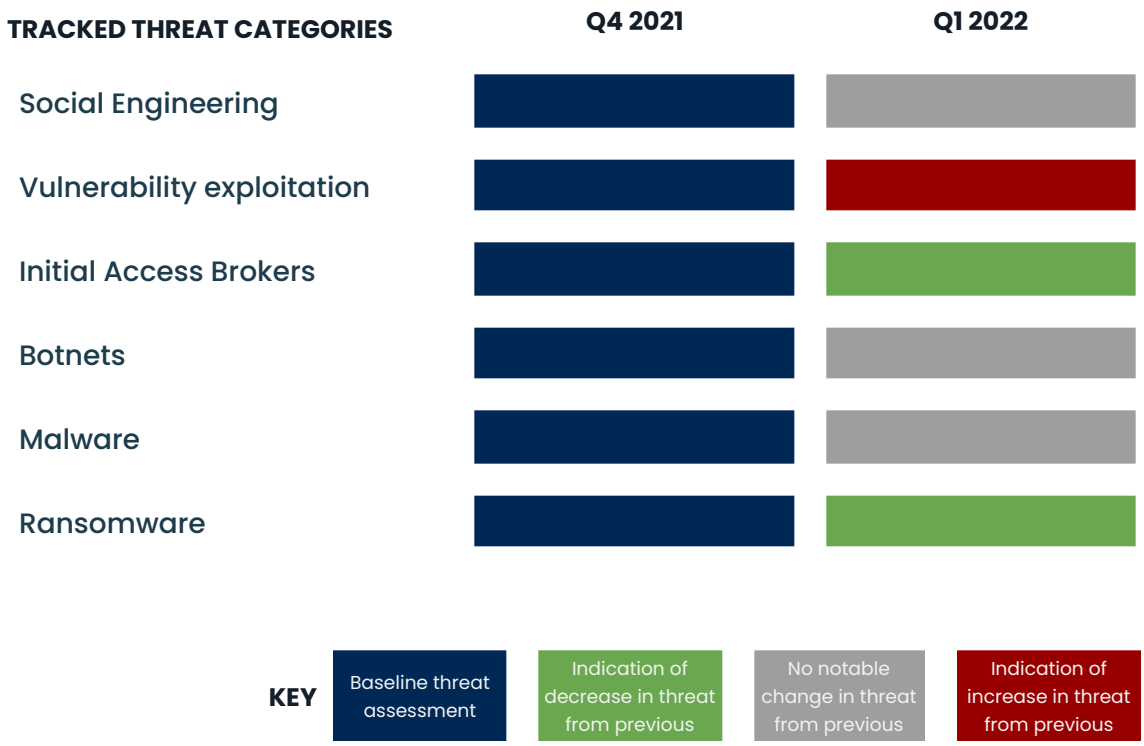
January 1 - March 31, 2022

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EDT) on April 8, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

EXECUTIVE SUMMARY

ZeroFox Intelligence assessed the developments to key cyber threats facing the financial sector from Q4 2021 through Q1 2022. Financial organizations faced a persistent threat from social engineering campaigns targeting them directly or impersonating them to entice customer engagement. Although the threat from Initial Access Brokers (IABs) may have decreased, the threat from vulnerability exploitation very likely increased. Botnet and malware deployment against targets in the financial sector remained high, including use of banking trojans against customers. Despite a drop in the number of ransomware and digital extortion attacks against financial sector organizations in Q1 2022, they remained some of the most significant threats to the sector.



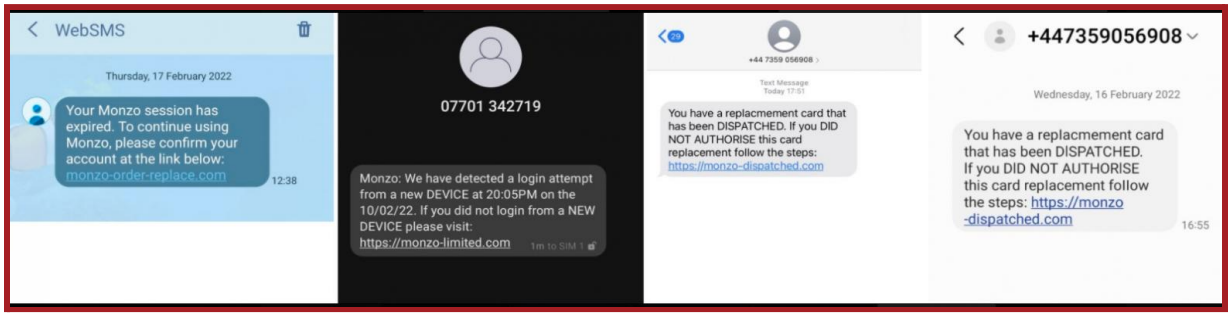
quarter quarter quarter

Key Findings

- Social engineering was one of the most frequently reported intrusion tactics leveraged against the financial sector in Q1 2022. However, threat actor tactics remained evolutionary rather than revolutionary, typically targeting employees and customers with rudimentary phishing emails and voice calls. ZeroFox Intelligence observed an increase specifically in conversation hijacking, which is a tactic used to make it more difficult for victims to identify nefarious activity.
- Phishing campaigns impersonating financial institutions continued to be prolific and given that financial sector organizations are seen as strategically significant by threat actors, this behavior is expected to continue.
- It is very likely that the threat to the financial sector from Common Vulnerabilities and Exposures (CVEs) and previously unknown software vulnerabilities (zero-days) increased in Q1 2022, particularly given the industry's ongoing reliance on remote working, cloud infrastructures, and commonly used software modules.
- Malware deployment across the landscape remained highly prevalent in Q1 2022 and ZeroFox Intelligence expects that to continue. Banking trojans remain a persistent threat to financial sector organizations and their customers.
- Despite a drop in the number of identified ransomware and digital extortion attacks against the financial sector in Q1 2022, ZeroFox Intelligence anticipates the threat will increase as desire to appear politically neutral during Russia's invasion of Ukraine dissipates.
- This quarter saw a notable increase from 'hack-and-leak' groups that claimed to be ransomware operations.

SOCIAL ENGINEERING

Social engineering was one of the most frequently reported intrusion tactics leveraged against the financial sector in Q1 2022, indicating human error remains a significant barrier to effective security practice. Threat actor tactics remained evolutionary rather than revolutionary, typically targeting employees and customers with rudimentary phishing emails and voice calls.[1][2][3][4] Social engineering will almost certainly remain a threat to the financial sector as campaigns are demonstrably effective and offer high return on investment.



Smishing messages to Monzo customers linking to phishing sites

Source: https://www.bleepingcomputer.com/news/security/new-phishing-campaign-targets-monzo-online-banking-customers/

Threat actors continued to use timely or topical lures in phishing campaigns, such as Russia's invasion of Ukraine which was leveraged in the distribution of the LoadEdge backdoor, Agent Tesla and Remcos, as well as activity attributed to nation states.[5][6][7][8][9] ZeroFox Intelligence anticipates continued leveraging of the invasion and subsequent humanitarian and economic crises for at least the duration of hostilities as a lure to entice user engagement, with financial sector organizations perceived by threat actors as lucrative and strategically important targets.

Social engineering campaigns appear to have remained one of the most prolific means of distributing malware, successfully leveraged to disseminate some of the most dangerous strains, including Medusa and Flubot, Bazarbackdoor, Emotet, JSSLoader, Agent Tesla, and Redline.[10][11][12][13][14] Payloads were typically delivered by malicious email attachments such as PowerPoint, Excel, CSV, and Zip files. Financial sector organizations should note the Q1 2022 TeaBot Remote Access Trojan phishing campaign that enticed user engagement by impersonating financial institutions.[15]

ZeroFox Intelligence observed an increase in conversation hijacking,[16] leveraged by multiple malware operators in Q1 2022, including IcedID and Qbot.[17][18] Other notable trends include phishing kits designed to intercept or bypass multi-factor authentication, and an upward trend in fake job offers made online.[19][20][21]

Forward Look:

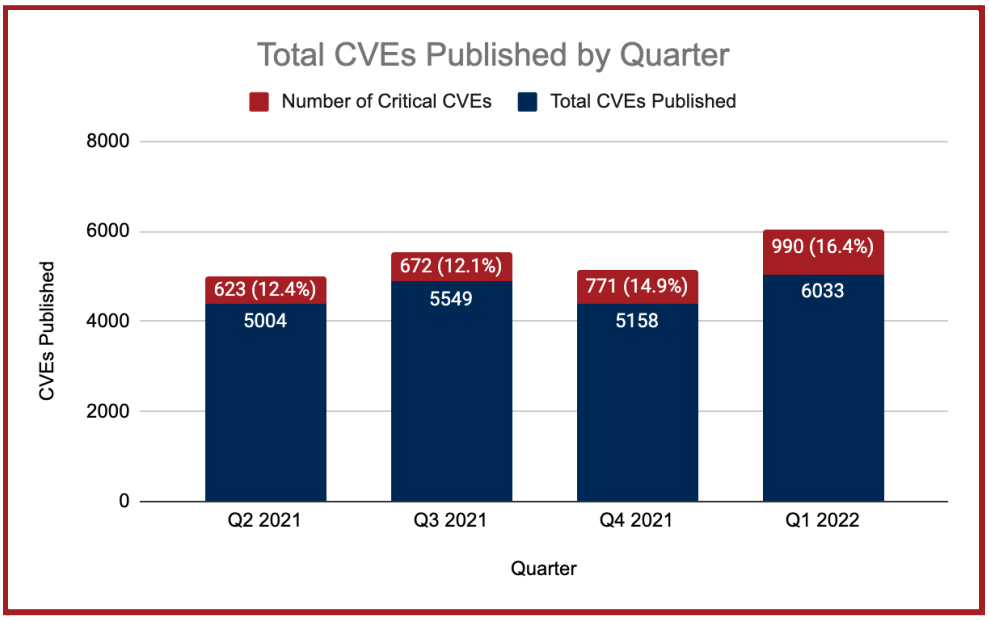
- ZeroFox Intelligence expects threat actors to continue leveraging the war in Ukraine and the subsequent humanitarian and economic crises to entice user interaction for at least the duration of the conflict.
- Given that threat actors view financial sector organizations as very valuable targets based on being very lucrative and strategic, targeting is expected to remain high.
- Conversation hijacking is likely to continue to be one of the most concerning growing social engineering threats.
- The impersonation of financial institutions in phishing campaigns offers a cover of legitimacy for threat actors that continue to deceive targets, and so as long as threat actors are able to use a guise of credibility with these phishing lures, leveraging financial institutions is likely to persist in phishing campaigns.

Recommendations:

- Include threats to third party operators in all assessments to capture the totality of the threat social engineering attacks present to financial sector organizations.
- Provide user training programs and regular company-wide notifications on phishing or social engineering tactics used to obtain critical information that can lead to attacks.
- Provide customers regular correspondence indicating legitimate communication in an effort to educate the customer base on how to identify phishing campaigns.
- Never download email attachments or click links from untrusted sources.
- Enable multi-factor authentication wherever possible.
- Verify suspicious correspondence via an alternative method of communication.

VULNERABILITY EXPLOITATION

It is very likely the threat to the financial sector from Common Vulnerabilities and Exposures (CVEs) and previously unknown software vulnerabilities (zero-days) increased in Q1 2022. The severity and pace of vulnerability disclosures reached unprecedented levels. The 6,033 security CVEs published—an average of more than 65 CVEs per day—are more than in any previous quarter, with a larger proportion than in any previous quarter receiving a Common Vulnerability Scoring System (CVSS) 3.X Critical rating.[22] [23] The frequency of zero-day disclosure also remained high in Q1 2022 affecting end-users in most industries. Google twice released emergency updates for Chrome vulnerabilities (CVE-2022-1096, CVE-2022-0609) under active exploitation, including by state-linked groups, and Apple published patches for two zero-days affecting Macs, iPhones, and iPads (CVE-2022-22674, CVE-2022-22675).[24] [25]



Data Source: https://nvd.nist[.]gov

Vulnerabilities in remote working and cloud infrastructures continued to dominate the exploit landscape, particularly those in network edge infrastructure such as routers and firewalls, commonly used software modules, and off-the-shelf packages.[26] [27] There was an apparent increase in reporting of vulnerabilities in Network Attached Storage devices.[28] [29] [30] [31] [32] These vulnerabilities created opportunities for threat actors to target financial sector organizations of various sizes and locations, often by enabling remote attackers to gain complete control over devices.

Delay or failure to install security updates continued to leave hardware and software vulnerable long after mitigations became available. Despite a patch release in December 2021, threat actors continued to exploit the Log4j remote code execution (RCE) vulnerability (CVE-2021-42278) in Q1 2022, including Deep Panda, TunnelVision, Prophet Spider, and B1txor20 operators.[33] [34] [35] [36] This enabled malicious actors to deploy rootkits, cryptominers, and botnets, as well as sell network access to third parties. ZeroFox Intelligence expects the "Spring4Shell" RCE zero-day (CVE-2022-22965) disclosed in March 2022 to follow this trend, with threat actors continuing to exploit unpatched software long after patches were released.[37]

Patching delays were compounded by the pace at which vulnerabilities were exploited after a proof-of-concept, in some cases as little as one day.[38] Professionalization of underground markets and media attention on vulnerabilities made it easier for threat actors to identify and exploit them. With threat actors actively monitoring for exploit disclosure, financial sector organizations must implement a timely patching program.

› Forward Look:

- Vulnerabilities in remote working, cloud infrastructures, and commonly used software modules will likely continue to dominate the exploit landscape.
- The Spring4Shell vulnerability will very likely be leveraged by threat actors long after the security patch was released.
- The pace at which these vulnerabilities are exploited will continue to accelerate as the ease for threat actors to exploit grows.

› Recommendations:

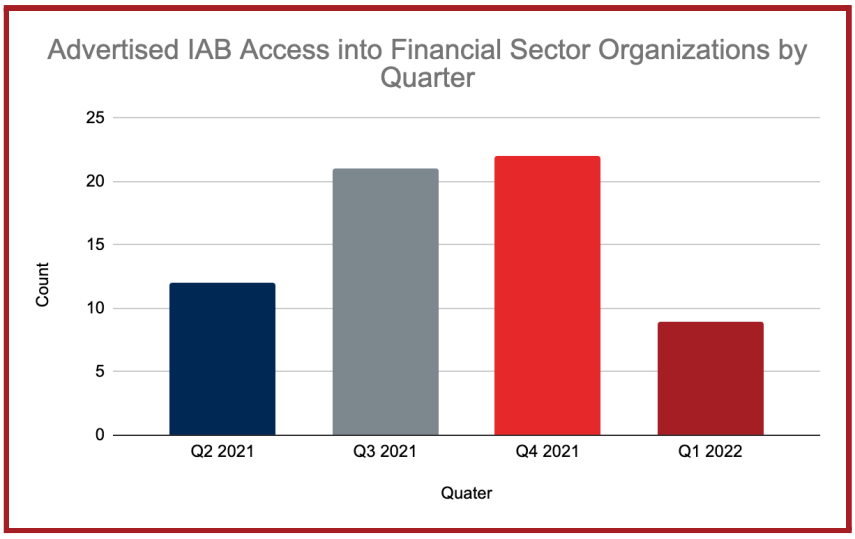
- Ensure a thorough understanding of the technology stack and patching schedule and, where possible, those of operating partners.
- Configure devices with the principle of zero-trust and least privilege.
- Periodically review edge device configurations and audit perimeter security.
- Regularly scan for software updates and implement them as quickly as practical.
- Enable multi-factor authentication wherever possible.
- Disable PowerShell wherever possible.

INITIAL ACCESS BROKERS

ZeroFox Intelligence assesses, with low-medium confidence, that the threat to financial sector organizations from Initial Access Brokers (IABs) reduced in Q1 2022. This assessment is based on illicit access sales that occurred in open marketplaces and covert communications channels we monitor, yet we recognize the scope of activity that may have fallen outside these collections channels. The number of posts selling access to compromised financial organizations' networks fell in Q1 2022; a trend seen in multiple sectors. This bucks the upward trend over the previous year of threat actors increasingly purchasing initial access for a plethora of follow-on malicious targeting, such as ransomware delivery.

The fall in activity likely reflects limitations to the supply from IABs rather than a lack of demand from buyers. This may be explained in part by Russia's invasion of Ukraine, with some IABs implicated in the conflict.[39] The war may have also driven some IABs to seek more private or direct communication methods to sell illicit access. Disruption to underground marketplaces such as Raid Forums in Q1 2022, where access sales have appeared regularly, may also be a driver. Threat actors shifted to an alternative marketplace following disruption, with Deep Web sites breached[.]co or Breached Forums taking Raid Forum's place.

Given the upward trajectory over the last year, and the likelihood that disruption to IABs' operations is only temporary, ZeroFox Intelligence anticipates that the threat to the financial sector from IABs will increase.



Data Source: ZeroFox Intelligence

Financial sector organizations almost certainly remained highly desirable targets in Q1 2022. While IABs and their customers pursued targets based on a wide range of criteria, including ethics, industry, location, and size, the financial sector is less likely than others to be shielded by

ideological aversions because the overwhelming motive for threat actors targeting it is financial gain. Given the potential for threat actors to move laterally across interconnected networks, financial sector organizations should be wary of IABs targeting them directly and indirectly via their operating partners.

Reporting disclosed several IAB campaigns in Q1 2022, including Prophet Spider leveraging Log4Shell vulnerabilities in unpatched VMware Horizon Servers, and the financially-motivated Exotic Lily, which has close ties to the Conti and Diavol ransomware gangs, launching a new phishing campaign.[40] [41] According to media reports, threat actors paid as much as USD 15,000 for access to computers belonging to employees of 21 energy companies.[42] While that price may appear substantial, it is a negligible cost when compared with the potential harm that can be inflicted.

ZeroFox Intelligence identified no significant change to advert content in Q1 2022. Threat actors typically continued to avoid specifying what type of access they were selling, instead listing the level of access, either user or admin, to entice buyers. Of the occasions when the type of access was disclosed, they usually related to VPN and Remote Desktop Protocol access.

› Forward Look:

- ZeroFox Intelligence anticipates an increasing threat to the financial sector from IABs, especially as the situation in Ukraine continues on and threat actors return to pursuing pre-conflict activities.
- In the absence of any takedown activity, Deep Web site breached[.]co or Breached Forums will continue as Raid Forum's replacement and a popular marketplace for IAB adverts.

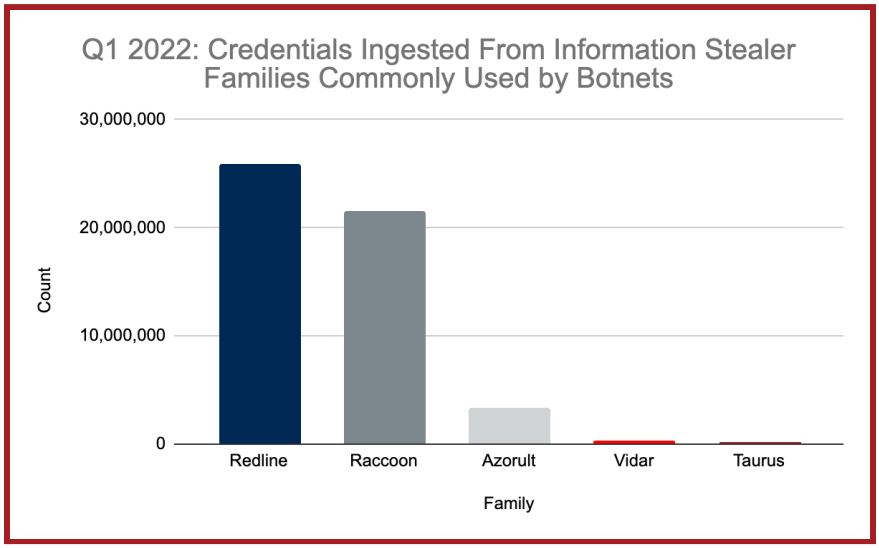
› Recommendations:

- Proactively monitor for potential network access sales to obtain critical early warning for an impending cyber attack, and help identify malicious actors, including insiders, meaning to harm your network.
- Configure devices with the principle of zero-trust and least privilege.
- Periodically review edge device configurations and audit perimeter security.
- Regularly scan for software updates and implement them as quickly as practical.
- Enable multi-factor authentication wherever possible.
- Disable PowerShell wherever possible.

BOTNETS

The threat to the financial sector from botnets in Q1 2022 remained largely consistent with previous quarters. However, the proliferation of highly capable botnets and the fallout from Russia's invasion of Ukraine makes it likely the threat posed to the financial sector will increase. ZeroFox Intelligence observed no significant change in botnet capabilities, with typical modifications including wormlike propagation and cryptojacking.[43] Infection by botnets facilitated the deployment of malware, including cryptominers and follow-on remote compromises with other malicious code.

Botnets deploying information stealers continued to pose a threat to financial sector organizations. In Q1 2022, ZeroFox ingested more than 50 million credentials harvested by infostealer families commonly used by botnets, of which RedLine was the most active. Emerging botnets raised their profile, including B1txor20, which leveraged the Log4j vulnerability to infect target devices, and the ZeroFox Intelligence-identified Kraken that supported numerous backdoor capabilities.[44] [45] Financial sector organizations should note the continued resurgence of Emotet.[46] At its peak, it was one of the largest and most capable botnets ever seen, and while a long way from the scale it once achieved, Emotet could pose a significant threat to organizations of various sizes, sectors, and locations in the coming months.[47]



Data Source: ZeroFox Intelligence

Internet-of-things (IoT) botnets, such as Mirai, continued to pose a significant threat to business operations and customers, particularly from Distributed Denial of Service (DDoS) attacks. Routers, firewalls, and IoT devices were still frequently leveraged as proxies to either anonymize threat actor activity or to serve as DDoS amplification tools.[48] [49] [50] The scale of DDoS attacks in Q1 2022 continued on an upward trajectory and, given the demonstrable impact they have had, ZeroFox Intelligence expects that to continue.[51] [52]

Botnets leveraged during Russia's invasion of Ukraine have primarily been targeted at Ukraine, Russia, and the surrounding region. However, ZeroFox Intelligence expects an increasing global impact in coming months with a greater threat to financial sector organizations. Botnets were leveraged in the build up to, and immediate aftermath of, kinetic action, with threat actors aligned with each side launching sizable DDoS attacks, including against the Ukrainian financial sector.[53] [54] [55] [56] [57] [58] [59] Russia-affiliated entities are likely to increase targeting of nations and organizations that vocally opposed the war or withdrew business operations from Russia, including those in the financial sector. Similarly, financial sector organizations that continued operations in Russia are likely to be increasingly targeted by pro-Ukrainian threat actors.

› Forward Look:

- Russia's invasion of Ukraine made geopolitical neutrality difficult to maintain; financial sector organizations could be targeted by either side.
- Financial sector organizations should be aware of the continued resurgence of Emotet, which may pose a significant threat to organizations of all sizes, sectors and locations in the coming months.

› Recommendations:

- Proactive monitoring for botnet logs may give critical early warning for an impending cyber attack.
- Keep up to date on Emotet developments in order to be able to adjust security postures appropriately.
- Map network infrastructure and blacklist as appropriate.
- Make sure defensive systems are updated with the latest detections.
- Monitor botnet logs for stolen credentials.
- Enable multi-factor authentication whenever possible.
- Deploy a DDoS protection solution.
- Ensure that security updates are rolled out as quickly as possible once they are provided.

MALWARE

Malware deployment across the landscape remained highly prevalent in Q1 2022 and ZeroFox Intelligence expects that to continue given ease of acquisition and impact on end users. Although infection rates remained high, ZeroFox Intelligence observed no significant change in capability. "Malware-as-a-service" (MaaS) models, offered for as little as USD 20, kept barriers to entry low. Threat actors continued to develop their arsenal, often leveraging commodity tools or more than one type of malware in attack chains.[60]

Loaders continued to serve as an effective means to deploy second-stage payloads. Established loaders launched new distribution campaigns, including a GootLoader campaign targeting employees of accounting and law organizations.[61] New loaders emerged, including at least one threat actor leveraging Verblecon in attacks that failed to utilize the potent malware to its full potential.[62] The rising popularity of MaaS offerings make it increasingly likely that there will continue to be highly capable malware in the hands of less capable individuals.

NVIDIA (February 2022)

- After compromising U.S.-based computer chip maker NVIDIA, Lapsus$ published stolen data including two stolen code-signing certificates used by NVIDIA developers to sign drivers and executables.[63]
- In March 2022, threat actors were identified using the stolen certificates to sign malware and tools to enable malicious drivers to be loaded in Windows. These included Cobalt Strike beacons, Mimikatz, backdoors, and remote access trojans.
- It is a realistic possibility that financially-motivated threat actors will seek to learn from, and commercialize, this approach by exfiltrating code-signing certificates when possible to sell to third party malware operators, as a variation on the initial access broker market.

The infostealer market remained highly saturated, with the steady rise and fall of new strains, and infostealing modules often incorporated into broader trojan malware. ZeroFox Intelligence observed an increase in threat actors leveraging infostealers to target digital currency wallets in Q1 2022 including BHUNT, Cryptbot, WeSteal, RedLine, and the emergence of Mars Stealer.[64] [65]

Commodity trojan malware posed a high threat to financial sector organizations in Q1 2022, leveraged by those with financial and political motives.[66] [67] Remote Access Trojans (RATs) remained a persistent threat, with new campaigns this quarter to distribute BitRAT and JSSLoader, which were linked to the financially-motivated Russian FIN7 group.[68] [69]

Many of the most prevalent banking trojans—including variants of TrickBot, QBot, and IcedID—remained persistent threats to the financial sector. Trickbot was observed targeting customers of 60 mostly U.S.-based companies dating back to 2020, 50 of which provide financial services.[70] However, the landscape was more dynamic than this suggests. New banking trojans emerged, and older trojans launched new campaigns and/or expanded their scope of targets.[71] [72] [73] Organizations in the financial sector should also note the feature-rich Sharkbot which is now distributed via a fake Google Play Store application and is capable of siphoning credentials to initiate money transfers from compromised devices by circumventing multi-factor authentication mechanisms.[74]

Proliferation of mobile malware remained on an upward trajectory, both as a means to steal passwords, banking information, and other sensitive user information, and to intercept multi-factor authentication codes.

Reporting indicates that wiper malware observed being leveraged during Russia's invasion of Ukraine—including HermeticWiper, WhisperGate, IsaacWiper, CaddyWiper, AcidRain, and the LoadEdge backdoor—has been limited in its use to date to Ukraine and the immediate surrounding area.[75] [76] [77] [78] [79] Multiple Ukrainian financial institutions were targeted. If or when Russia's focus reverts to its other long-standing interests, variants of these strains will likely be deployed more broadly against organizations and governments in Western nations, those who vocally opposed Russia's actions, pro-European Union nations such as Finland, Georgia, and Moldova, and other nations in Russia's geographic proximity. Organizations operating in the financial and other critical sectors of these countries will likely face an increased threat.

› Forward Look:

- Financial organizations are likely to face an increased threat from malware deployed by Russia, state-linked, and pro-Russian threat actors.
- MaaS offerings are very likely to sustain low barriers to entry for threat actors and continue diversifying the tactics, techniques, and procedures (TTPs) typically seen within each malware strain.

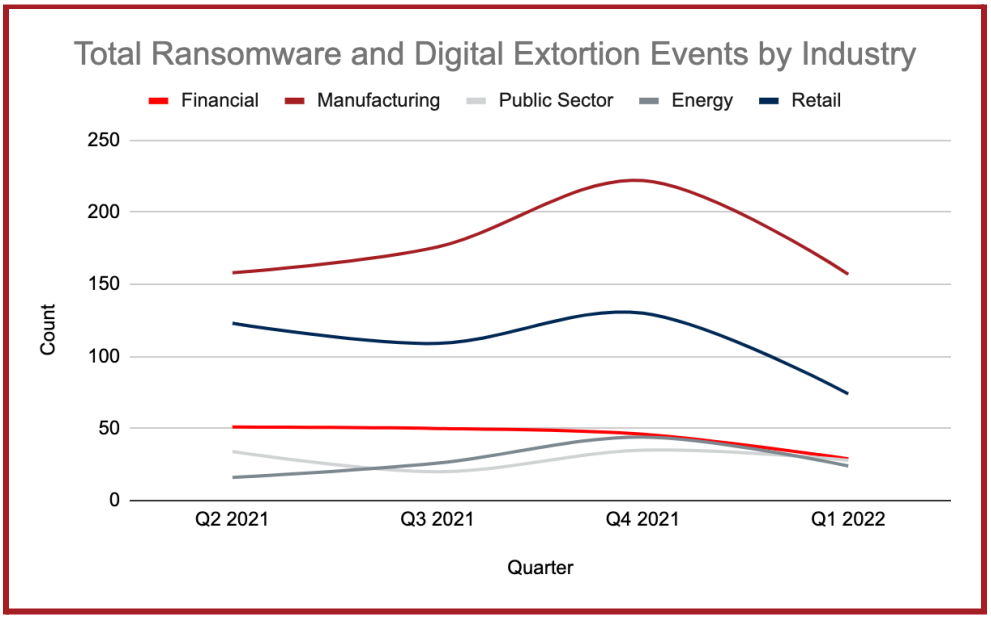
› Recommendations:

- Review obligations in different jurisdictions with regards to disclosure of breaches, particularly with the U.S. passing the Strengthening American Cybersecurity Act (the "Act") into law in March 2022.
- Adopt appropriate app security programs to defend against
- Regularly backup critical data, including keeping password-protected backup copies offline.
- Make sure defensive systems are updated with the latest detections.
- Ensure proper network segmentation.

- Blacklist network infrastructure as appropriate.
- Conduct threat hunting activity with available signatures.

RANSOMWARE

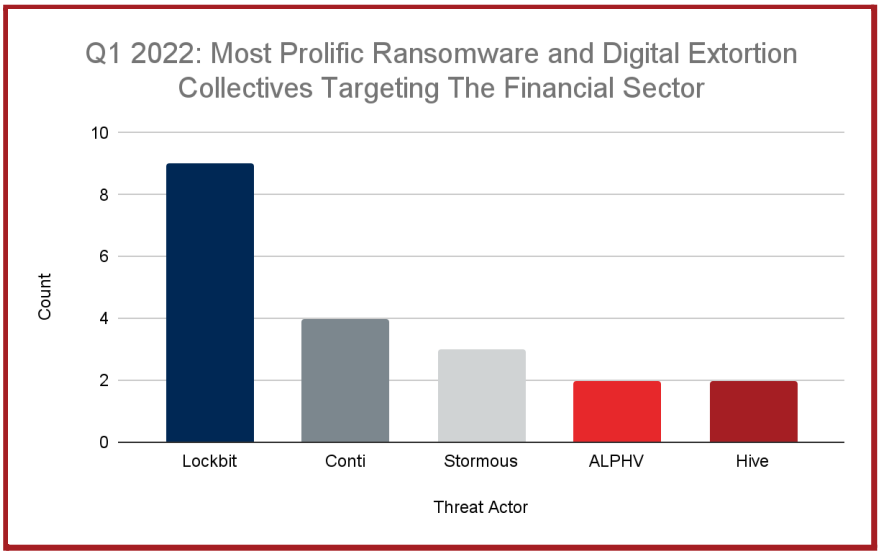
Ransomware and digital extortion remained two of the greatest threats to the financial sector despite a drop in identified incidents in Q1 2022. Russia's invasion of Ukraine may have contributed to a temporary suppression of the threat, with ransomware collectives seeking to avoid overtly, or inadvertently, aligning themselves politically. However, the impact of the invasion must not be overstated.
The frequency and scale of extortion incidents reached unprecedented levels in 2021, and the financial sector faced a high volume of attacks in Q1 2022; remaining one of the most frequently targeted industries. ZeroFox Intelligence anticipates that ransomware and digital extortion groups will increase their activity, with organizations in the financial sector perceived as a lucrative target for attack.



Data Source: ZeroFox Intelligence

The most prolific ransomware operators in previous quarters continued to be highly active in Q1 2022. LockBit and Conti continued operations against financial sector organizations, despite Conti having chat logs, infrastructure, and source code leaked online after publicly announcing support for the Russian government. Hive and BlackByte ransomware gangs were also active this quarter, and a plethora of new strains were identified, including Night Sky, White Rabbit, Entropy, and LokiLocker.[80][81][82][83] Additionally, law enforcement disruption of extortion gangs continued this quarter, including the arrest, extradition, and sentencing of operatives, as well as the release of decryptors.[84][85][86][87][88][89] However, disruptive activity taken against ransomware groups is unlikely to result in their abandoning this lucrative business. Instead, threat actors are likely to relaunch or rebrand under a different name, as has

been evident in multiple cases, such as Black Cat/AlphV reportedly confirming it is composed of former Blackmatter/Darkside members.[90] [91]



Data Source: ZeroFox Intelligence

ZeroFox Intelligence identified an increase in activity in Q1 2022 from '"hack-and-leak" collectives—often erroneously labeled as ransomware groups—which were responsible for multiple high profile attacks. Attributed groups included Lapsus$ and Stormous; the latter having been one of the most prolific threat actors targeting the financial sector this quarter.[92] [93] Despite groups exfiltrating sensitive data to be leveraged in ransom demands, ZeroFox Intelligence identified no evidence in these cases that malware was deployed or files encrypted. These groups may consider exfiltrating and threatening to leak sensitive data to be of greater concern to victims than file encryption and disruptions to business operations. The success of this tactic depends on the ability for groups to achieve their aims either politically or financially. If victims are able to mitigate the effects of leaked data without paying ransoms, we anticipate encryption as a pressure tactic to reemerge as the dominant activity.

› Forward Look:

- Ransomware operators are likely to target financial organizations as retaliation for perceived stances taken during the war in Ukraine.
- Disruptive activity is very likely to only temporarily suppress the threat before threat actors relaunch activities or rebrand under a different group name.

› Recommendations:

- Review obligations in different jurisdictions with regards to disclosure of breaches, particularly with the U.S. passing the Strengthening American Cybersecurity Act (the "Act") into law in March 2022.
- Regularly backup critical data, including keeping password-protected backup copies offline.

- Prevent the lateral movement of ransomware, which is a tactic frequently used by Conti ransomware, which is one of the top ransomware strains targeting the financial sector.
- Make sure defensive systems are updated with the latest detections.
- Ensure proper network segmentation.
- Blacklist network infrastructure as appropriate.
- Conduct threat hunting activity with available signatures.

GEOPOLITICS

Russia established itself as the primary geopolitical concern in Q1 2022 for the financial sector, replacing China. China, as the world's second largest economy and dominant trading partner with most nations on earth, continues to present the biggest potential geopolitical threat to financial services. However, during Russia's prolonged military buildup in 2021, China actively sought to reassure financial services and diminished other economy-damaging behaviors as the geopolitical threat landscape shifted to Russia. The unified Western response when the conflict did happen in Q1 and lack of an obvious diplomatic resolution to the war means Russia will very likely continue to be the world's primary driver of geopolitical risk for the financial sector.

Russia's outsized role in commodity production and strategic location between Europe, Asia, and North Africa make up for its small economic output, accounting for roughly 2 percent of global GDP. Effective Western sanctions following Russia's war in Ukraine forced most Western financial firms that operate in Russia or sell to the Russian market to withdraw. The outcome of Russia's war in Ukraine threatens Russia's entire USD 1 trillion balance sheet, of which USD 300 billion is in international money markets.[94]

The secondary effects of the war like the financial impact of high energy, food, and other commodity prices also impact the financial sector. In Q1 2022 this led to social unrest in markets like Spain, Peru, and Pakistan where financial services likely maintain a footprint, but also central bank intervention in the form of interest rate hikes that impact the cost of doing business internationally. The International Monetary Fund (IMF) took the unusual step of downgrading its financial forecast for 2022 after just one quarter. This came with an accompanying increase in projected inflation.[95] The biggest Q1 instigator of inflationary protests, more drastic interest rate hikes, and economic slowdowns was Russia's invasion of Ukraine.

Source: https://blogs.imf.org/2022/04/19/war-dims-global-economic-outlook-as-inflation-accelerates/

The financial sector must also contend with heightened cybersecurity threats and the accompanying spending for defenses triggered by Russia's war in Ukraine. This could extend to Russian threat actors targeting Western financial services in response to sanctions imposed over the war in Ukraine or those most vulnerable to the financial downturn. This could include financial services in emerging markets or those with large holdings in foreign debt or volatile commodities.

Russia's invasion of Ukraine created a dynamic where geopolitical neutrality has been difficult to maintain. Nations are increasingly pressured to side either with the West - namely the U.S., United Kingdom, European Union, and Ukraine - or the dominant powers of the East - Russia and China. India, in particular, experienced growing pressure in Q1 that ZeroFox Intelligence expects to continue throughout the Russia/Ukraine conflict due to the nation's deep connections to each side of that schism. For the financial sector, this complicates maintaining global operations or investments when doing so risks incurring the wrath of threat actors who may perceive business in a country to be a sign of support for a nation they see as their political enemy.

In previous quarters, the U.S. and China were engaged in a damaging trade war, and China used its trade dominance to punish nations and private enterprises critical of their human rights record. The 2020 Hong Kong National Security Law (HKNSL) also threatens the safe middle ground financial services have used to maintain market access to mainland China without increased government intervention. During the entire four year U.S.-China trade war, around USD 550 billion was lost in import tariffs.[96] Despite harsh COVID-19 lockdowns and China imposing HKNSL on the financial hub of Hong Kong, most financial services maintained operations in China.

China spent Q1 of 2022 reiterating to financial services firms in particular that they would not risk their economic relationship with the West to back Russia. Following reports that China would do just that, on March 14 China's stock market suffered its worst day since the 2008 financial crisis with the Hang Seng China Enterprises Index dropping 7.2 percent, and the Hang Sang Tech Index dropping 11 percent. On March 16, 2022, Chinese stocks regained most of their losses, and the Hang Seng China Enterprises Index was up 12.5 percent in its best session since October 2008.[97] This came after U.S. intelligence reports that China did not countenance Russia's request for military aid and a significant financial policy statement from China vowing neutrality and stability regarding international finance. This underscores China's policy regarding Russia. While it may share many of Russia's adversarial positions with regards to the U.S., Zerofox Intelligence estimates China is not prepared to risk the important financial relationship it has with the U.S. and the West at this moment.

The financial sector is globalized, but many organizations were forced to abandon the Russian market as a result of Western sanctions and public pressure. Due to China's far greater importance as a financial market when compared to Russia, ZeroFox Intelligence finds it unlikely that a similar exodus from China - or sanctions similar to those imposed on Russia - will occur. However, in the weeks following Russia's invasion of Ukraine, multinationals and foreign investors reportedly withdrew billions from China or reduced operations in what may signal at least some shifting of priorities over geopolitical concerns.[98]

› Forward Look:

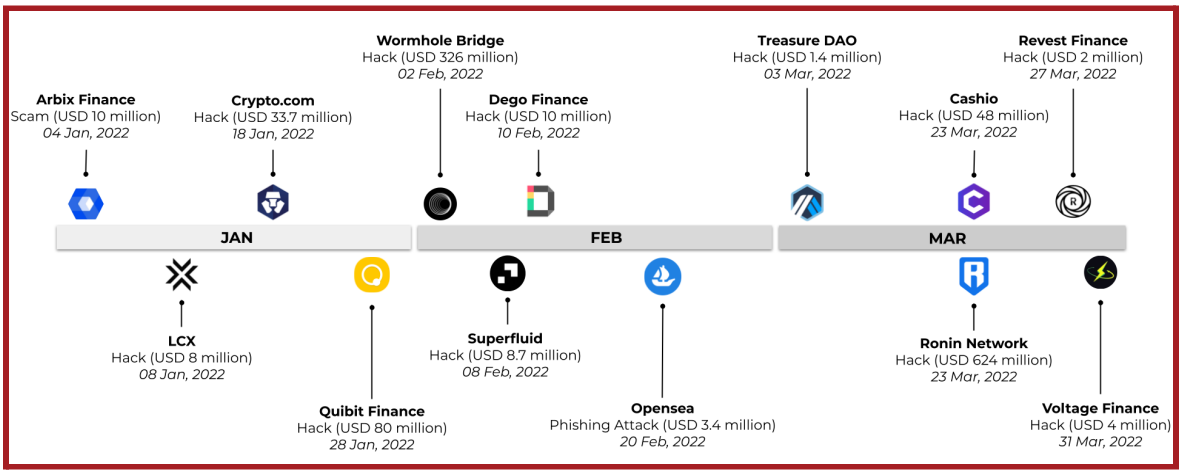
- States or companies that have pulled services from Russia or taken a pro-Western position should expect pushback that could include influence operations; particularly against Eastern or Northern European states considering NATO/EU membership.
- Harsh COVID-19 lockdowns in China are likely to have down-the-line supply chain impacts which will impact production and availability of goods.

› Recommendations:

- Organizations should map and assess their current supply chains, as well as assign potential risks to each portion, in order to determine impacts if those portions are disrupted. In addition, organizations should develop alternative supply chain plans to accommodate disruptions.
- Any continuing operations in Russia and/or China should be closely monitored for geopolitical as well as COVID-19 impacts.

QUARTERLY SPOTLIGHT - BLOCKCHAIN THREATS

Blockchain attacks in Q1 2022 continued on an upward trajectory in the form of hacks, scams, and social engineering campaigns. Q1 2022 highlighted the frequency and scale of such attacks, with reports indicating at least 80 malicious incidents occurred across different blockchains—an increase from 33 the previous year—particularly on decentralized finance (DeFi) exchanges and platforms. These attacks resulted in an estimated USD 1.3 billion stolen in assets.[99] Previous quarters have seen a surge in the adoption of digital assets—such as cryptocurrency and non-fungible tokens (NFTs)—from businesses and consumers globally, reportedly rising almost 900 percent in 2021.[100] There has been a corresponding rise in threat actor activity, seeking to conduct crypto theft by exploiting poor user security and vulnerabilities within blockchain mechanisms such as smart contracts.



High-profile malicious blockchain incidents in Q1 2022

Source: https://rekt.news/leaderboard/

DeFi—a collective term for financial products and services built on the blockchain—has been increasingly targeted by threat actors. In fact, 97 percent of all crypto theft in Q1 2022 was reportedly taken from DeFi exchanges and platforms, up from 72 percent the previous year.[101] This was likely due to a rise in user adoption, and the spike in the total value locked (TVL), which measures the overall value and growth rate of DeFi; this increased by 1200 percent in late 2021 to over USD 240 billion.[102] The nascent and competitive nature of the DeFi market means projects may overlook appropriate security measures in favor of first-mover advantage. Threat actors have exploited DeFi via security breaches and vulnerable code within smart contracts—self-executing blockchain programs that run when predetermined conditions are met—for unprecedented financial gain.

The rising value of DeFi has attracted financially-motivated threat actors of all capabilities, including Advanced Persistent Threats (APTs). On March 23, 2022, Ronin Network—also known as Ronin Bridge—was exploited for USD 625 million, becoming the largest crypto hack to date. North Korea-linked Lazarus Group has been credited with this attack, which leveraged social engineering to compromise Ronin Network's validator key scheme; a system designed to increase security by requiring multiple signatures to authorize withdrawal transactions.[103] This activity is consistent with Lazarus Group's targeting of the crypto market, including a string of attacks on exchanges since at least 2017.[104] ZeroFox Intelligence anticipates further high-profile DeFi attacks throughout 2022 due to a combination of the profit potential and the ongoing discovery of vulnerabilities among exchanges and platforms.

Social engineering attacks directed towards the crypto market persisted throughout Q1 2022, as threat actors continued to leverage malicious emails and links on social media platforms to target digital assets. One noteworthy phishing campaign took advantage of a contract migration on Opensea—one of the largest NFT marketplaces. By replicating official emails, threat actors tricked users into visiting fake websites and signing malicious transactions crafted to look like a legitimate OpenSea request, leading to the theft of hundreds of high-profile NFTs worth USD 2 million collectively.[105] Threat actors have continued to distribute infostealing malware—that specifically targets credentials linked to crypto wallets—to steal digital assets. Well-known strands, such as Cryptbot and Redline remain the most prevalent.[106] However, ZeroFox Intelligence also observed an increase in newly developed strains throughout Q1 2022, including BHUNT, Blackguard, Mars, META, and ZingoStealer.

OUTLOOK

ZeroFox Intelligence anticipates Russia's invasion of Ukraine will continue to heavily influence the cyber threat landscape facing the financial sector for at least the duration of the conflict. Threat actors are very likely to continue leveraging the conflict and the subsequent humanitarian and economic crises as lures in social engineering scams. There is likely to be an increased threat from malware deployed by Russia, state-linked and pro-Russian threat actors, and ransomware operators likely to target financial organizations as retaliation for perceived stances taken during the war.

Vulnerabilities in remote working, cloud infrastructures, mobile banking, and commonly used software modules will likely continue to dominate the exploit landscape, including the Spring4Shell vulnerability which is expected to be leveraged by threat actors long after the patch was released. ZeroFox Intelligence anticipates an increase in threats from IABs, ransomware, and digital extortion collectives, with disruption to operations by law enforcement very likely to only temporarily suppress these threats.

APPENDIX : Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use TLP:** RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use TLP:** AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share TLP:** RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share TLP:** AMBER information with members of their own organization and only as widely as necessary to act on that information.

	Green	White
WHEN SHOULD IT BE USED?	**Sources may use TLP:** GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use TLP:** WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share TLP:** GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share TLP:** WHITE information without restriction, subject to copyright controls.

ENDNOTES

1. https://www.armorblox.com/blog/the-email-bait-and-phish-instagram-phishing-attack/
2. https://www.bleepingcomputer.com/news/security/citibank-phishing-baits-customers-with-fake-suspension-alerts/
3. https://www.bleepingcomputer.com/news/security/new-phishing-campaign-targets-monzo-online-banking-customers/
4. https://www.bleepingcomputer.com/news/security/morgan-stanley-client-accounts-breached-in-social-engineering-attacks/
5. https://www.zdnet.com/article/ukraine-warns-of-invisimole-attacks-tied-to-state-sponsored-russian-hackers/
6. https://anvilogic.com/threat-reports/agent-tesla-and-remcos-rats-phishing-emails/
7. https://www.zdnet.com/article/google-multiple-hacking-groups-are-using-the-war-in-ukraine-as-a-lure-in-phishing-attempts/
8. https://www.reuters.com/world/europe/ukraine-says-its-military-is-being-targeted-by-belarusian-hackers-2022-02-25/
9. https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/
10. https://threatpost.com/medusa-malware-flubot-android-distribution/178258/
11. https://www.bleepingcomputer.com/news/security/malicious-csv-text-files-used-to-install-bazarbackdoor-malware/
12. https://threatpost.com/emotet-spreading-malicious-excel-files/178444/
13. https://www.bleepingcomputer.com/news/security/malicious-microsoft-excel-add-ins-used-to-deliver-rat-malware/
14. https://www.bleepingcomputer.com/news/security/new-redline-malware-version-spread-as-fake-omicron-stat-counter/
15. https://www.zdnet.com/article/teabot-android-banking-trojan-continues-its-global-conquest-with-new-upgrades/
16. Conversation hijacking abuses end user trust in the legitimacy of interactions and can make it more difficult for victims to identify nefarious activity.
17. https://thehackernews.com/2022/03/hackers-hijack-email-reply-chains-on.html
18. https://news.sophos.com/en-us/2022/03/10/qakbot-injects-itself-into-the-middle-of-your-conversations/
19. https://www.infosecurity-magazine.com/news/growing-number-of-phish-kits/
20. https://www.ic3.gov/Media/Y2022/PSA220201
21. https://www.zdnet.com/article/linkedin-phishing-scams-increase-232-since-feb-1-report/
22. https://nvd.nist.gov/vuln
23. This is the highest severity rating assigned in the framework, accounting for software vulnerabilities that score 9.0-10 out of 10.
24. https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-used-in-attacks/
25. https://www.bleepingcomputer.com/news/security/apple-emergency-update-fixes-zero-days-used-to-hack-iphones-macs/
26. https://www.theregister.com/2022/03/24/developers_using_microsoft_azure_targeted/
27. https://thehackernews.com/2022/03/critical-sonicos-vulnerability-affects.html
28. https://thehackernews.com/2022/03/critical-bugs-in-terramaster-tos-could.html
29. https://thehackernews.com/2022/03/dirty-pipe-linux-flaw-affects-wide.html
30. https://www.zdnet.com/article/asustor-warns-users-of-deadbolt-ransomware-attacks/
31. https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/
32. https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-bugs-in-smb-routers-exploits-available/
33. https://www.zdnet.com/article/chinese-hackers-deep-panda-return-with-log4shell-exploits-new-fire-chili-rootkit/
34. https://www.bleepingcomputer.com/news/security/iranian-hackers-target-vmware-horizon-servers-with-log4j-exploits/
35. https://thehackernews.com/2022/01/initial-access-broker-involved-in.html
36. https://www.bleepingcomputer.com/news/security/new-linux-botnet-exploits-log4j-uses-dns-tunneling-for-comms/
37. ZeroFox Flash Report: Spring4Shell, April 1, 2022
38. https://www.bleepingcomputer.com/news/security/public-redis-exploit-used-by-malware-gang-to-grow-botnet/
39. https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/
40. https://thehackernews.com/2022/01/initial-access-broker-involved-in.html
41. https://thehackernews.com/2022/03/google-uncovers-initial-access-broker.html
42. https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine
43. https://thehackernews.com/2022/03/dirtymoe-botnet-gains-new-exploits-in.html
44. https://www.bleepingcomputer.com/news/security/new-linux-botnet-exploits-log4j-uses-dns-tunneling-for-comms/
45. ZeroFox Advisory: Meet Kraken: A New Golang Botnet in Development, February 10, 2022
46. https://threatpost.com/emotet-spreading-malicious-excel-files/178444/
47.www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
48. https://thehackernews.com/2022/04/beastmode-ddos-botnet-exploiting-new.html
49. https://www.zdnet.com/article/cyclops-blink-botnet-launches-assault-against-asus-routers/
50. https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html
51. https://thehackernews.com/2022/03/imperva-thwarts-25-million-rps-ransom.html
52. https://www.theregister.com/2022/03/10/mitel_amplification_ddos_attack/
53. https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/

54. https://www.bleepingcomputer.com/news/security/malware-disguised-as-security-tool-targets-ukraines-it-army/
55. https://securityaffairs.co/wordpress/128051/hacking/ukraine-military-agencies-banks-hit-by-ddos-attacks-defacements.html
56. https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/
57. https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/
58. https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense
59. https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/
60. https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
61. https://thehackernews.com/2022/01/gootloader-hackers-targeting-employees.html
62. https://www.bleepingcomputer.com/news/security/verblecon-malware-loader-used-in-stealthy-crypto-mining-attacks/
63. https://twitter.com/BillDemirkapi/status/1499437244830175236?s=20&t=_EUUVs3s9yR8tsuA8auYOw
64. https://thehackernews.com/2022/01/new-bhunt-password-stealer-malware.html
65. https://www.bleepingcomputer.com/news/security/mars-stealer-malware-pushed-via-openoffice-ads-on-google/
66. https://thehackernews.com/2022/03/iranian-hackers-targeting-turkey-and.html
67. www.csoonline.com/article/3649209/iranian-apt-group-uses-previously-undocumented-trojan-for-destructive-access-to-organizations.html
68. https://www.bleepingcomputer.com/news/security/bitrat-malware-now-spreading-as-a-windows-10-license-activator/
69. https://www.bleepingcomputer.com/news/security/malicious-microsoft-excel-add-ins-used-to-deliver-rat-malware/
70. www.zdnet.com/article/trickbot-abuses-top-brands-including-bank-of-america-wells-fargo-in-attacks-against-customers/
71. https://securityaffairs.co/wordpress/128975/malware/hidden-c2-lampion-trojan-release-212.html
72. https://securityintelligence.com/posts/ramnit-banking-trojan-stealing-card-data/
73. https://www.zdnet.com/article/teabot-android-banking-trojan-continues-its-global-conquest-with-new-upgrades/
74. https://thehackernews.com/2022/03/sharkbot-banking-malware-spreading-via.html
75. https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
76. https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/
77. https://cyware.com/news/new-wipers-and-fake-av-updates-target-ukraine-f0f077d1
78. www.techtimes.com/articles/273755/20220331/viasat-hit-russia-s-wiper-malware-called-acidrain-affecting-european.htm
79. https://www.zdnet.com/article/ukraine-warns-of-invisimole-attacks-tied-to-state-sponsored-russian-hackers/
80. https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/
81. https://www.bleepingcomputer.com/news/security/new-white-rabbit-ransomware-linked-to-fin8-hacking-group/
82. https://www.bleepingcomputer.com/news/security/entropy-ransomware-linked-to-evil-corps-dridex-malware/
83. https://blogs.blackberry.com/en/2022/03/lokilocker-ransomware
84. https://www.zdnet.com/article/uk-police-arrest-seven-individuals-suspected-of-being-hacking-group-members/
85. https://www.zdnet.com/article/alleged-hacker-behind-kaseya-ransomware-attack-extradited-arraigned-in-texas/
86. www.justice.gov/opa/pr/former-canadian-government-employee-extradited-united-states-face-charges-dozens-ransomware
87. https://threatpost.com/decryptor-keys-maze-egregor-sekhmet-ransomwares/178363/
88. https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/
89. https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html
90. https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/
91. https://www.cybersecuritydive.com/news/ransomware-ryuk-conti-revil-2021/608845/
92. ZeroFox Profile: Profile of Lapsus$, March 22, 2022
93. ZeroFox Flash Report: Increased Stormous Ransomware Claims Made Against Previous Victims, February 18 2022
94. https://www.bain.com/insights/the-financial-system-consequences-of-the-russia-ukraine-war/
95. www.project-syndicate.org/commentary/imf-world-outlook-revision-growth-models-failing-by-mohamed-a-el-erian-2022-04
96.economictimes.indiatimes.com/news/international/business/chinas-trade-war-with-us-resulted-in-loss-of-usd-550-billion-report/articleshow/90025687.cms
97. https://www.bloomberg.com/news/articles/2022-03-16/xi-spurs-frantic-stock-buying-with-lifeline-for-china-markets
98. https://www.scmp.com/business/markets/article/3172201/ukraine-war-risk-sanctions-puts-china-stocks-valuation
99. https://atlasvpn.com/blog/blockchain-hackers-stole-nearly-700-million-in-q1-2022
100. https://www.coindesk.com/business/2021/10/07/new-chainalysis-report-reveals-whos-leading-the-world-in-crypto-adoption/
101. https://blog.chainalysis.com/reports/2022-defi-hacks/
102. https://finbold.com/total-value-locked-in-defi-surges-over-1200-in-2021-to-surpass-240-billion/
103.fbi.gov/news/pressrel/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea
104. https://www.computerweekly.com/news/450433324/North-Korean-hackers-tied-to-cryptocurrency-attacks-in-South-Korea
105. https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft
106. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/