

Q2 2022

Quarterly Threat Landscape Report

ZeroFox Intelligence

April 1 – July 31, 2022

Table of Contents

Executive Summary	2
Key Findings	3
Quarterly Spotlight Russian Cyber Actors Scramble to Offset Fallout From Ukraine	4
Social Engineering	6
Vulnerability Exploitation	8
Initial Access Brokers	10
Botnets	12
Malware	15
Ransomware	18
Geopolitics	21
Outlook	23
Appendix- Traffic Light Protocol for Information Dissemination	24
Endnotes	25

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 July 8, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party link.



Executive Summary

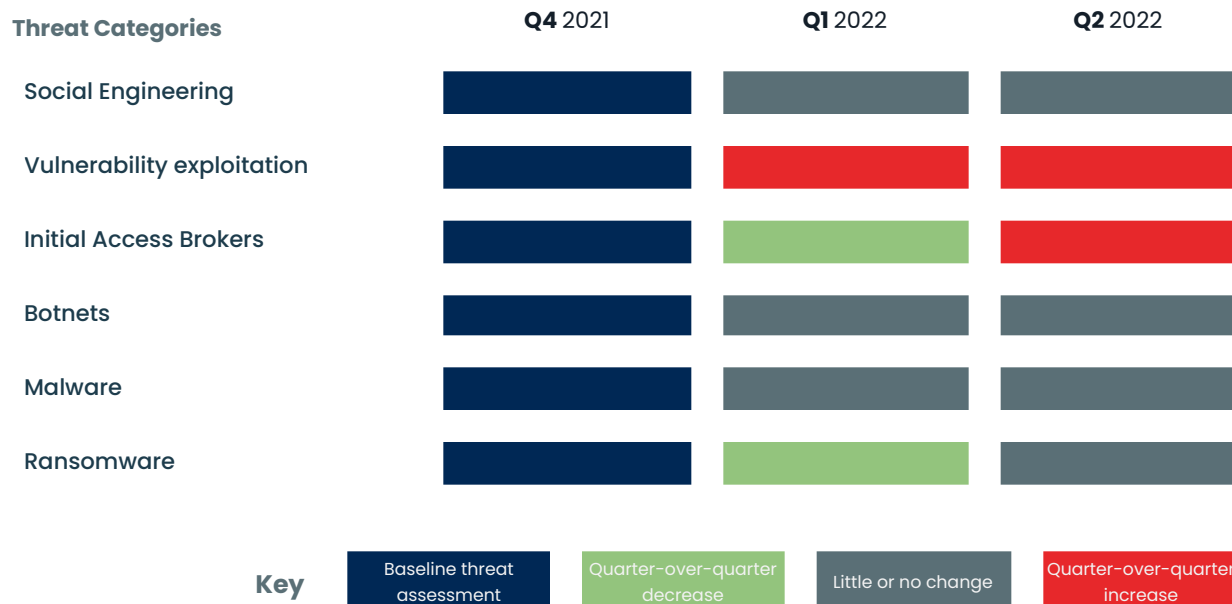
ZeroFox Intelligence collected and analyzed developments around key cyber threats during Q2 2022, and several trends stood out at the conclusion of the analysis. Notably, with the ongoing conflict in Ukraine, well-regarded threat actors continue to exchange ideas on how to maneuver within the new economic and political constraints. Immediate concerns continue to center around the fate of cryptocurrency funds and potential strategies to exchange them for fiat currency that can be spent. In addition, social engineering campaigns remained a persistent threat to organizations across the threat landscape this quarter, with threat actors very likely to continue targeting desirable employees in job-related scams—especially those in leadership positions who have elevated access levels, potentially leading to financial harm or corporate exposure.

The threat from vulnerability exploitation continued on an upward trajectory, most likely representing a new normal for the exploit landscape. ZeroFox Intelligence anticipates that threat actors will continue to leverage high-profile vulnerabilities in widely-used software—such as the Follina, Confluence, and F5 BIG IP applications—long after the security patches were released. Moreover, after a fall in activity in Q1 2022, the threat from Initial Access Brokers showed signs of resurgence. Threat actors may be pushed increasingly to more private means to sell illicit access, making the identification of activity more difficult. Botnet and malware deployment remained high, including from infostealers and banking trojans. To that end, high saturation of Malware-as-a-Service offerings will very likely continue to sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.

Despite a drop in the number of ransomware and digital extortion attacks in Q2 2022, the overall threat remained broadly consistent with the previous quarter—albeit with threat actors conducting more damaging attacks. The healthcare and retail industries in particular experienced a resurgence in targeting. ZeroFox Intelligence also observed that ransomware threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics. This may ultimately lead these actors to resort to more extreme pressure tactics in an attempt to cause greater operational downtime and reputational damage, which may have legal ramifications.

Lastly, the ongoing war in Ukraine continued to be the primary driver of geopolitical risk across the quarter and heavily influenced the cyber threat landscape. As the conflict in Ukraine continues on, issues like European Union/North Atlantic Treaty Organization membership and new sanctions on Russia are likely to trigger a Russian state response, which often coincides with Russian-backed groups targeting sensitive infrastructure.





Key Findings

- Russian-speaking cybercriminals demonstrated increasing concern regarding the ability to turn cryptocurrency into fiat currency, with specific unease related to the perception that cryptocurrency may be the only way to transfer financial support to Russia.
- Social engineering remained one of the most frequently reported intrusion tactics in Q2, with notable increases in the use of LNK shortcut files and fake Windows 11 upgrades to deliver malware and employment-related scams.
- The threat from Common Vulnerabilities and Exposures and previously-unknown software vulnerabilities likely increased in Q2 2022. Sustained quarters of high vulnerability disclosures provide more routes for threat actors to attack and place increased pressure on patch management processes.
- The Initial Access Broker marketplace showed signs of resurgence in Q2 2022 despite activity levels remaining lower than in 2021, likely reflecting continued limitations in supply. Threat actors may be pushed increasingly to more private means to sell illicit access.
- Despite the widespread media attention and Russia-aligned entities starting to target nations and entities that vocally opposed the war in Ukraine with botnet attacks, the threat from botnets in Q2 2022 appears to have remained unchanged.
- Malware deployment remained highly prevalent in Q2 2022, and ZeroFox Intelligence expects that to continue.
- Despite a drop in identified incidents, the threat from ransomware and digital extortion remained largely consistent with previous quarters. Threat actors changing extortion tactics may indicate difficulty in eliciting payments from victims.



| Quarterly Spotlight Russian Cyber Actors Scramble to Offset Fallout from Ukraine

In Russian-language Deep and Dark Web forums, well-regarded threat actors continue to exchange ideas on how to maneuver within the new economic and political constraints since the onset of the war in Ukraine. As a result, actors will likely rely on institutions in geopolitically indifferent or supportive countries. Immediate concerns continue to center around the fate of cryptocurrency funds and potential strategies to exchange them for fiat currency that can be spent. Causing further unease is the perception that only cryptocurrencies can be sent or wired to Russia for financial support.

One noteworthy and longstanding Russian-language Dark Web forum member on Exploit[.]in offered their unfiltered opinion on European Union (EU) sanctions and why they decided to move to Dubai: *"Who gives a f*** what they want. I went to Dubai where I can get cash for any crypto under the sun. Moreover, opening a bank account here is not a huge deal."* When challenged with potentially exorbitant fees charged to cash-out crypto, the unfazed actor responded, *"Well it seems to me that with the volatility of Bitcoin (BTC), who cares about the exchange fees at the moment. It's the pinnacle of greediness...just put all your money in a bank account in Dubai."*

This sentiment was echoed in a separate forum thread in which actors discussed the best way to send money to Russia—another signal that the ramifications of geopolitical decisions trickle down into the underground economy. Forum members that participated in the thread overwhelmingly agreed that cryptocurrency was the most reasonable way to send funds to Russia.

This community has at least one unresolved obstacle to overcome: the SWIFT (The Society for Worldwide Interbank Financial Telecommunication) ban will likely impact the ability to withdraw or send money to or from Russia's majority state-owned bank, Sberbank. Russian banks only issue Russian rubles, and, as the currency continues its decline, well-known threat actors are assessing how to offset any temporary financial losses and disruption to their revenue streams. One tactic being discussed to skirt Western sanctions and gain access to hard currency is laundering rubles through specific Russian and peer-to-peer (P2P) exchanges into U.S. dollar-backed stablecoins—cryptocurrencies that attempt to offer some pricing stability.

At the moment, there are few, if any, restrictions preventing private exchanges from converting assets from one currency to another. Actors are leveraging this fact to avoid attribution and move funds almost at will. The only calculated downside is the loss of funds from exchange fees, but this does not appear to concern most actors facing the possibility of losing access to Western financial institutions. Responding to a post about the exchange of Russian rubles to U.S. dollars,



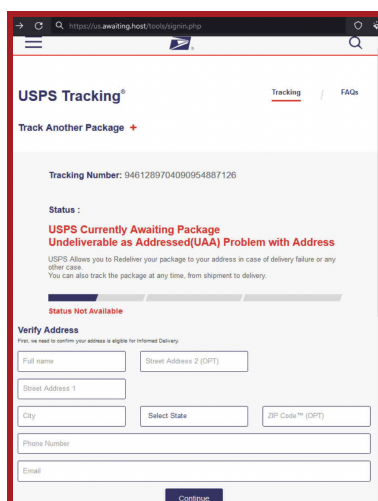
a longtime Russian-language Dark Web forum actor described converting Russian rubles to U.S. dollar-backed stablecoins using a trusted Russian-language exchange called bestchange. The actor cautioned that the exchange rate to convert rubles to dollars was so outrageous that it would be difficult to find someone trustworthy enough to do it.

As the fallout from Russia's invasion of Ukraine intensifies, cyber actors are prepared to pivot and adapt in near real-time to offset temporary disruptions to their financial gains. They will continue to seek methods that use stable financial institutions to minimize personal financial losses.

Once they safely exchange rubles for cryptocurrency, they will then look to convert digital currency into hard currency—most likely U.S. dollars—that can be offshored to non-Russian banks.

Social Engineering

Social engineering remained one of the most frequently reported intrusion tactics in Q2, and this will almost certainly remain the case for the foreseeable future. As long as campaigns prove effective and highly cost-efficient, threat actors have little incentive to change tactics. Threat actors successfully targeted employees, customers, and members of the public with phishing emails, smishing, and vishing.^{1 2 3 4 5} Campaigns targeted almost all industries, including—but not limited to—the financial, manufacturing, retail, healthcare, and public sectors.^{6 7 8 9 10 11 12}



Fake data entry form as part of a smishing campaign impersonating the U.S. Postal Service

Source: [hxxps://blog.malwarebytes\[.\]com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/](https://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/)

Threat actors continued to distribute malware via malicious email attachments in Q2 2022—such as Excel, ISO, PDF, and Word documents—and will almost certainly continue to do so.^{13 14 15 16} All incoming files received via email should be scanned to mitigate the risk associated with increased use of LNK shortcut files delivering malware like Emotet, IcedID, and BazarLoader.^{17 18 19 20} Security teams should be aware of new campaigns and associated Indicators of Compromise (IOCs) from



some of the most dangerous strains—including GammaLoad, BitRat, Qbot, Mantanbuchus, and Raccoon Stealer (as identified by ZeroFox Intelligence in June 2022)—and new strains, such as SVC, more_eggs, Meta, and DarkWatchman.^{[21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#)}

As anticipated in ZeroFox Intelligence’s Q1 2022 report, threat actors leveraged Russia’s war in Ukraine as lures in social engineering campaigns in Q2.^{[31](#) [32](#) [33](#) [34](#) [35](#)} ZeroFox Intelligence anticipates that threat actors will continue to use the war and associated crises—humanitarian and economic—as lures for at least the duration of hostilities.

Both state-linked and financially-motivated threat actors increasingly targeted hiring managers, job-seekers, and key personnel in employment-related scams in Q2 2022. These approaches facilitate financial loss, deployment of malware, credential theft, and obtaining privileged access.^{[36](#)}
^{[37](#) [38](#) [39](#)} Security teams should also note an increase in fake Windows 11 upgrades used to deploy malware, such as remote access trojans and infostealers.^{[40](#) [41](#) [42](#) [43](#)}

➤ Forward Look:

- Malicious email attachments will almost certainly remain a prominent method of disseminating malware, with threat actors adapting their approach to evade detection.
- Threat actors are very likely to continue targeting desirable employees in job-related scams—especially those in leadership positions with elevated access levels, which increases the risk of financial harm or corporate exposure.

➤ Recommendations:

- Provide regular communication online via corporate social media channels and websites to highlight what legitimate organization job postings look like and when they are posted in an effort to get ahead of fake job offers.
- Request an Attack Surface Assessment from ZeroFox Intelligence—including the totality of the threat social engineering attacks present—for actionable intelligence to mitigate risk.
- Provide user training programs and regular company-wide notifications on phishing and social engineering tactics used to obtain critical information that can lead to attacks.
- Utilize the ZeroFox Platform’s Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains, Botnet Infected Hosts, Compromised Account Credentials, and phishing-related Email Addresses and Phone Numbers.
- Raise awareness of LinkedIn scams targeting employees and actively scan for potential phishing domains used in recruitment scams.
- 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.

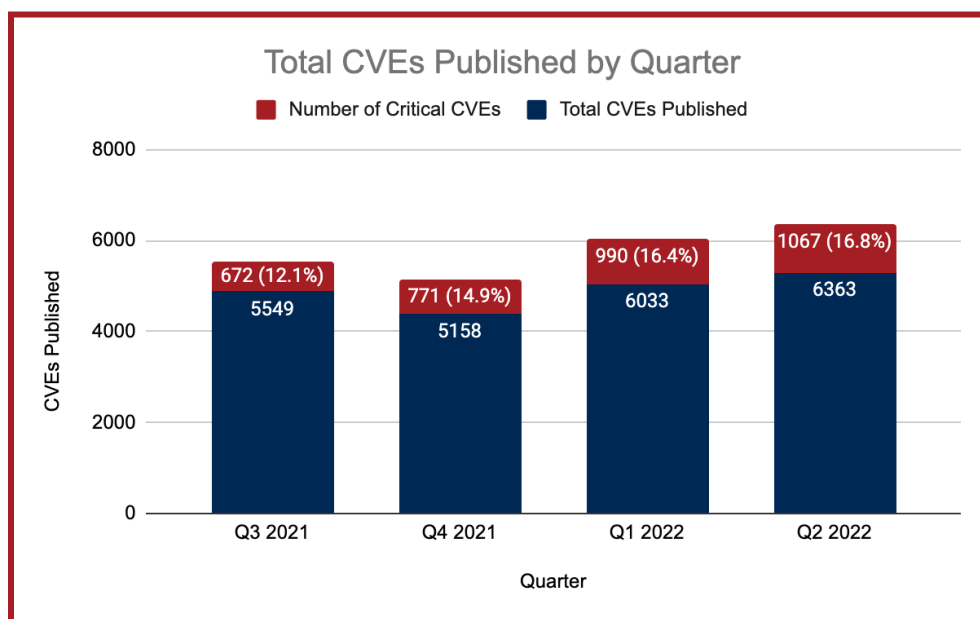


Vulnerability Exploitation

ZeroFox Intelligence assesses that the threat from Common Vulnerabilities and Exposures (CVEs) and previously-unknown software vulnerabilities (zero-days) likely increased in Q2 2022.

The severity and pace of vulnerability disclosure continued on an upward trajectory, averaging almost 70 CVEs disclosed per day. Nearly 17 percent of vulnerabilities disclosed received a Common Vulnerability Scoring System (CVSS) 3.X Critical rating. The frequency of zero-day disclosures also remained high, affecting end users in almost all industries.

Sustained quarters of high vulnerability disclosures are of considerable concern, as they provide more routes for threat actors to attack and place increased pressure on patch management processes. This is exacerbated by the increased integration of third-party software into enterprise technology stacks and the pace at which threat actors exploit newly-disclosed vulnerabilities. This upward trend may reflect more effective security research and efficient reporting but is more likely representative of a new normal for the scale of exploit disclosure.



Source: <https://nvd.nist.gov>

Vulnerabilities in the cloud and network perimeter infrastructure—including routers, firewalls, and commonly-used software modules—remained prevalent this quarter, enabling remote attackers to compromise enterprise networks of organizations of all sizes and locations. ZeroFox Intelligence is conducting ongoing monitoring following early indications of an increase in Small Office / Home Office (SOHO) network device exploitation.^{44 45 46} The importance of efficient patching programs is magnified by widespread reporting of vulnerabilities in commonly-used software, enabling threat actors to rapidly target vulnerable systems. This was evidenced by state-linked threat actors and



malware operators leveraging the Microsoft Windows Support Diagnostic Tool (MSDT) RCE vulnerability (CVE-2022-30190)—dubbed “Follina”—prior to a patch becoming available, as highlighted in a June 2022 ZeroFox Intelligence Flash.^{47 48 49 50 51 52} There was also rapid exploitation of the Confluence server zero-day vulnerability (CVE-2022-26134) and the F5 BIG-IP iControl REST endpoints vulnerability (CVE-2022-1388) to drop malicious payloads.^{53 54 55 56} As seen with Log4j (CVE-2021-42278) and Spring4Shell (CVE-2022-22965), it is very likely that high-profile vulnerabilities disclosed this quarter will continue to be exploited by threat actors despite the longstanding availability of patches.⁵⁷

➤ Forward Look:

- Vulnerabilities in the cloud and network perimeter infrastructure— including routers, firewalls, and commonly-used software modules—will likely continue to dominate the exploit landscape.
- Threat actors will continue to leverage high-profile vulnerabilities in widely-used software, such as the Follina, Confluence, and F5 BIG IP applications, long after the security patches were released.
- The scale and pace of exploit disclosures likely represent a new normal for the vulnerability landscape.

➤ Recommendations:

- Utilize the ZeroFox Platform’s Intelligence Search interface to investigate vulnerabilities and associated exploits. Vulnerability data sourced from the NIST database is enriched by ZeroFox analysts to provide an attack surface risk score, potential impact, and remediation.
- Ensure a thorough understanding of the technology stack and patching schedule, as well as those of operating partners, where possible.
- 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.

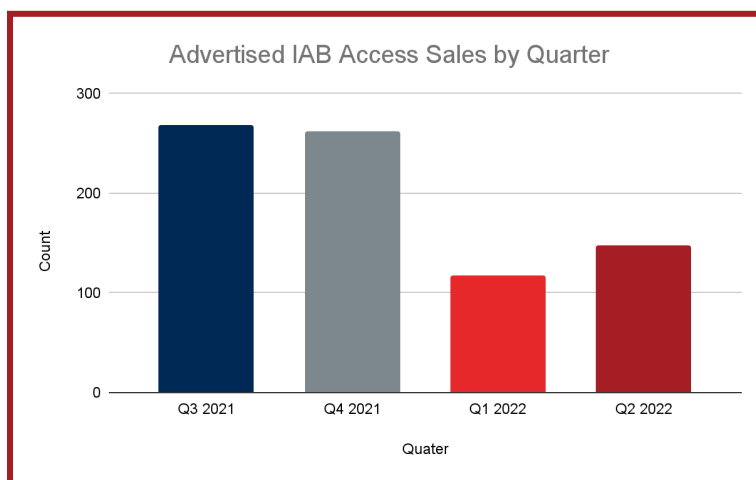


Initial Access Brokers

The Initial Access Broker (IAB) marketplace showed signs of resurgence in Q2 2022, with a particular focus on advertising access to entities participating in high-profile events in a bid to maximize their own brand awareness.⁵⁸ Although the threat to most industries remained broadly consistent with Q1 2022, ZeroFox Intelligence identified a greater number of access sales in some industries, including finance. When broken down by industry, the IAB landscape is more volatile than other cyber threats, with access sales typically trending against particular industries for a period of time before moving on and spiking against others.

Despite the resurgence, IAB activity levels remained lower than in 2021, likely reflecting continued limitations in supply rather than a reduction in demand from buyers. This is due to a confluence of factors, including:

- IABs being implicated in Russia's invasion of Ukraine, resulting in some IABs seeking more private or direct communication methods via which to sell illicit access.
- Continued disruption to underground marketplaces in Q2 2022, where access sales have appeared regularly.^{59 60 61 62}



Source: ZeroFox Intelligence

Most IABs continued to be driven by financial gain, with few ideological barriers for advertising access to victims. The criteria for targeting typically include company profile, industry, and location. Advertisement content in Q2 2022 remained broadly consistent with previous quarters and typically avoided specifying the type of access for sale, instead just listing the level of access available. Security teams should be wary of IABs targeting them directly and indirectly via their operating partners.



ZeroFox identified several notable IAB campaigns in Q2 2022, including a BreachForum user advertising a USD 100,000 bounty for data exfiltrated from a prominent cybersecurity firm and mentioning employees by name whose personal account credentials were being sought. While that price may appear substantial, it is negligible when compared with the potential harm that can be inflicted by gaining access to such data.

➤ Forward Look:

- ZeroFox Intelligence anticipates a continued resurgence in threats from IABs given strong demand from buyers and the likelihood that disruption to IAB operations is only temporary.
- Threat actors may be pushed increasingly to more private means to sell illicit access, making the identification of activity more difficult.

➤ Recommendations:

- Proactively utilize the unique data sets available within ZeroFox's Threat Intelligence Feeds to analyze and prepare appropriate security responses ahead of threat actor activity.
- Monitor for network access sales to gain critical early warnings of impending cyberattacks and identify malicious actors, including insiders, intending to harm your network.
- Employ ZeroFox Intelligence to conduct a Person of Interest Investigation into threat actors to establish a real-world identity, determine motivation, assess reputation, and inform the level of risk and appropriate course of action.
- 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

Organizations in most locations across the globe saw a negligible change in the threat from botnets in Q2 2022. Threat actors continued to develop their arsenal, but ZeroFox Intelligence observed no significant change in botnet capabilities that affected typical modifications, such as worm-like propagation. Botnets were leveraged by threat actors to conduct Distributed Denial of Service (DDoS) attacks; deploy malware, including crypto miners; and other malicious follow-on activity. Disruption to major botnets, including Cyclops Bink and RSocks, is unlikely to have a substantial long-term impact on the threat.^{63 64}

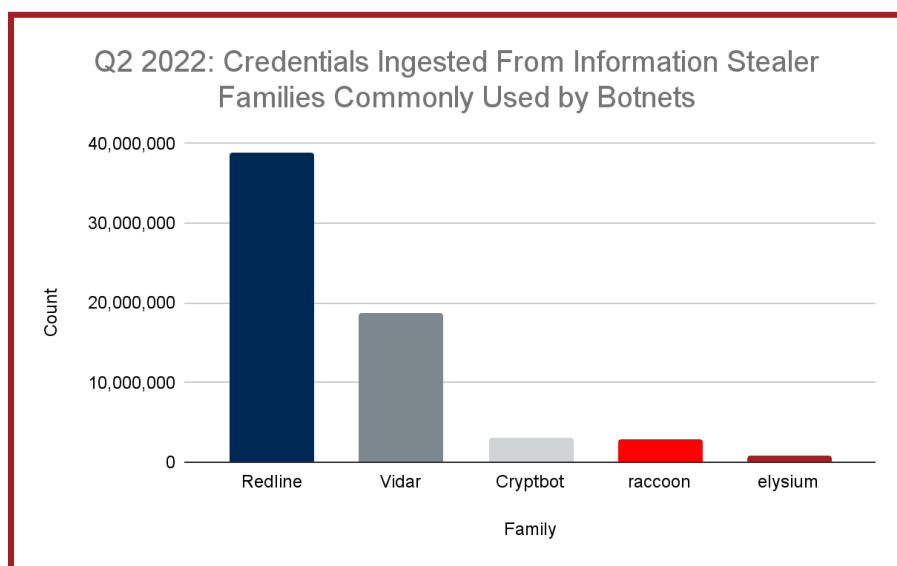
As anticipated in ZeroFox Intelligence's Q1 2022 report, Russia-aligned entities began targeting nations and organizations that vocally opposed the war in Ukraine with botnet attacks, such as



those launched by KillNet.⁶⁵ Botnets continued to be leveraged against Russian and Ukrainian telecoms, government, and energy targets.^{66 67 68} DDoS attacks have also been directed towards regional neighbors, potentially exacerbating geopolitical tensions as highlighted in a June 2022 ZeroFox Intelligence Brief.^{69 70 71 72} However, this did not happen at the scale or breadth expected. Much of the observed activity was conducted by typically less capable Russian state-aligned, rather than Russian state-backed, threat actors. ZeroFox speculates that this may be due to continued disruption to threat actors operating in the conflict region.

Botnets deploying information stealers continued to pose a significant threat to organizations, rapidly taking advantage of new exploits and upgrading detection evasion capabilities.^{73 74 75}

In Q2 2022, ZeroFox ingested more than 66 million credentials harvested by infostealer families commonly used by botnets, of which RedLine was the most active.⁷⁶ Expansion of the botnet market continued, with new botnets—including Fodcha, Panchan, and the Mirai-based Enemybot—emerging to target web servers, modems, routers, Internet-of-Things (IoT), and Android devices.



Source: ZeroFox Intelligence

IoT botnets remained a threat to business operations, particularly via DDoS attacks. The scale of DDoS attacks in Q2 2022 continued on an upward trajectory, including two of the largest incidents ever recorded.^{77 78} Given the demonstrable impact, ZeroFox Intelligence expects that to continue. Amplification attacks—including using TCP Middlebox Reflection to reflect and amplify TCP traffic to victims' machines—also pose a significant threat to financial institutions.⁷⁹



Despite receiving much media attention, KillNet's activities had little impact on the cybersecurity landscape.⁸⁰ Although the group claimed responsibility for DDoS attacks on multiple industries across Europe and rendered websites inoperable, KillNet typically had limited sustained impact. KillNet was very likely acting on behalf of, rather than directed by, Moscow. KillNet's actions align with Russia's known history of leveraging cybercriminal groups to advance foreign policy goals while maintaining plausible deniability. This can be achieved directly via state-linked groups or indirectly via cybercriminals acting on behalf of the state.

As flagged in last quarter's ZeroFox Intelligence report, security teams should be wary of Emotet's continuing resurgence, increasing distribution, leveraging of new distribution methods, and deploying of a stealer module this quarter.^{81 82 83 84} At its peak, Emotet was one of the largest and most capable botnets and could again pose a significant threat to organizations of various sizes, sectors, and locations in the coming months.

➤ Forward Look:

- Botnets leveraged by Russia-aligned entities have the potential to exacerbate geopolitical tensions, particularly if more capable threat actors engage in the activity.
- Security teams 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:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains, Botnet Infected Hosts, Compromised Account Credentials, and phishing-related Email Addresses and Phone Numbers.
- Map network infrastructure and blacklist as appropriate.
- Ensure 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.



Malware

The threat from malware deployment across the landscape remained high in Q2 2022; it is unlikely to reduce given the ease of acquisition and the impact on victims, but ZeroFox Intelligence observed no significant change in capabilities. Malware-as-a-service (MaaS) models maintained low barriers to entry, with the launch of new services and other offerings selling for as little as USD 6 for a two-month subscription.^{85 86} Dissemination of malware via fake apps on application marketplaces appeared to rise, increasing the potential risk for those that use personal devices professionally.^{87 88 89}

Loaders continued to be leveraged by threat actors, including ransomware gangs and hacking collectives, to deploy second-stage payloads.^{90 91 92} The emergence and rapid rise of the Bumblebee malware loader—attributed to Conti as a replacement for BazarLoader—indicates how capable threat actors can pivot their approach and rebrand.⁹³ There was also a reported increase in the use of the Matanbuchus loader.⁹⁴ Threat actors continue to deploy new versions of long-established loaders, such as ArguePatch Loader and IceXLoader, as well as launching new strains.^{95 96 97}

Infostealers remained highly prevalent in Q2 2022 and were often used in conjunction with other malware or incorporated into broader trojans. Leveraged against a variety of targets, infostealers most notably targeted cryptocurrency exchanges and the automotive industry.^{98 99} Infostealers continued to emerge at a high rate in Q2 and included FFdroider, Lightning Stealer, Saintstealer, Prynt Stealer, META, and a new version of Raccoon Stealer.^{100 101 102 103 104} These threats increase the pressure on enterprise security teams to ensure threat detection tools remain up to date.

Commodity trojan malware remained a persistent threat to most sectors in Q2 2022, though ZeroFox Intelligence observed no significant change in capability. The Remote Access Trojan (RAT) landscape continued to evolve, with new strains emerging, widespread proliferation, and ease of acquisition for threat actors with financial or political motives.^{105 106 107 108} Despite the notable takedown of the widely-used Flubot operation, the threat is unlikely to change significantly in the coming quarter due to quickly emerging additional strains.

Prevalent banking trojans such as QBot and IcedID remained persistent threats in Q2 because operators regularly and rapidly updated the malware's capabilities, as seen with QBot leveraging the Follina vulnerability to hit targets. The threat is underpinned by the high rate of new banking trojans emerging and older trojans launching new campaigns.^{109 110 111}



Mobile banking trojans are reportedly moving towards more on-device fraud, rather than account takeover, to better-obfuscate fraudulent transactions.¹¹² Android banking trojans that support this capability include Alien, Anatsa, Hydra, Octo, and SharkBot.

The threat posed by skimmers remained largely consistent with last quarter, as threat actors continued to successfully siphon payment details from unwitting victims in Q2 2022. It is unlikely the threat will reduce in the near term, though it may change in nature. While threat actors continued to successfully deploy skimmers against ATM networks—and warnings were issued about the danger skimmers pose to online stores—the most capable threat actors are attacking fewer targets but employing more advanced techniques to obfuscate malicious code.^{113 114 115}

Although spyware received significant media attention in Q2 2022, there was likely little change to the threat posed. The greatest threat to the majority of organizations comes from fraudulent apps distributing spyware, or spyware modules within broader malware packages, to steal sensitive information.¹¹⁶ However, Q2 highlighted the threat spyware poses to high-profile individuals in all sectors and the importance of good security practices in mitigating any attempted attacks.^{117 118 119 120 121}

➤ Forward Look:

- A high volume of MaaS offerings will very likely sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.
- Threat actors operating the most effective trojans will almost certainly continue to rapidly update capabilities to take advantage of vulnerabilities in widely-used software, placing increased importance on having a comprehensive and efficient patching program.

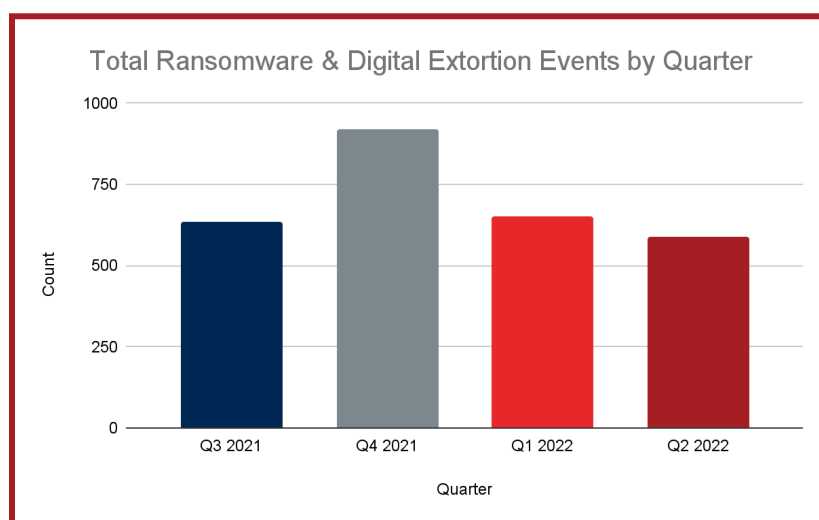
➤ Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Regularly back up critical data, including offline password-protected backup copies.
- Update defensive systems with the latest detections.
- Ensure proper network segmentation.
- Blacklist network infrastructure as appropriate.
- Conduct threat hunting activity with available signatures.



Ransomware

The threat from ransomware and digital extortion likely remained broadly consistent in Q2 2022, though the nature of the threat changed significantly. Despite a drop in identified incidents, threat actors demonstrated greater capability than in prior attacks in Q1 2022. High-profile attacks targeted the finance, manufacturing, retail, healthcare, and public sectors.^{122 123 124 125 126 127 128 129 130 131} ZeroFox Intelligence has identified changes to extortion tactics in Q2, which may indicate that threat actors are struggling to elicit payments from victims. Ransomware and digital extortion remained two of the greatest threats in Q2 2022, and ZeroFox Intelligence anticipates that threat will most likely increase.



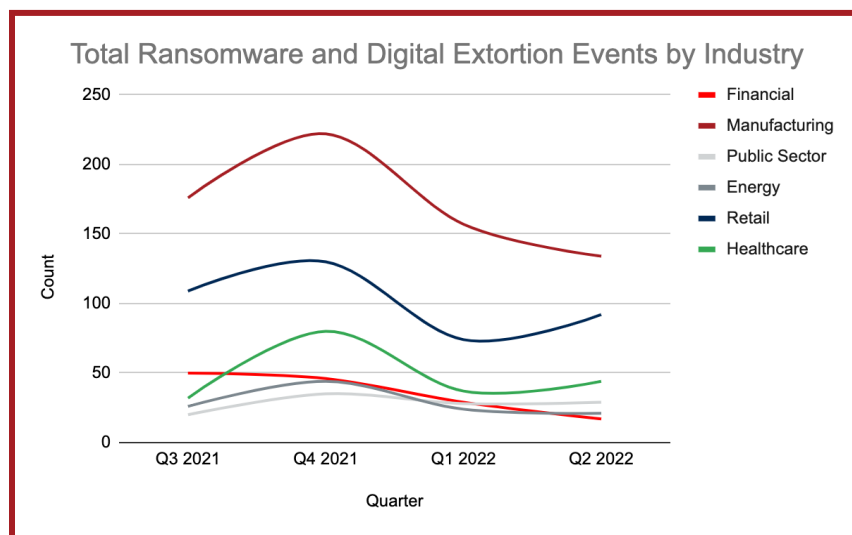
Source: ZeroFox Intelligence

LockBit remained the primary digital extortion threat, claiming the most victims in almost all industries in Q2 2022. The collective launched an updated strain and established a bug bounty program.¹³² The Hive and BlackCat (aka ALPHV) ransomware gangs also remained active this quarter, and ZeroFox Intelligence anticipates that REvil, ClOp, and Cuba—which all resumed operations in Q2 2022—will also increase their activity in the coming months.^{133 134 135}

The threat from Conti operatives very likely dispersed, rather than reduced, by the end of Q2 2022. After shutting down its operation, Conti members have very likely splintered and begun operating within other collectives.¹³⁶ Despite denials from the group, analysis has linked its operatives with Hive, and Karakurt has been named as Conti's data extortion arm.^{137 138 139} Prior to ceasing operations, Conti claimed responsibility for high-profile attacks, including one on Costa Rica's government—and possibly its healthcare system—that resulted in a state of emergency.^{140 141 142 143}



Security teams should be wary of new ransomware strains, and their associated IOCs, launched this quarter—the most concerning of which is the Black Basta operation. This ransomware-as-a-service operation hit more than 50 victims, partnered with the Qbot malware operation, and is alleged to have ties to Conti members.^{144 145 146 147} Other new strains include BlueSky, Cheers, DarkAngels, GoodWill, and Yashma.^{148 149 150 151 152} The financial threat actor FIN7 has also begun ransomware operations, as has the Industrial Sky extortion marketplace.^{153 154}



Source: ZeroFox Intelligence

Threat actors continued to develop their tactics during the exploitation stage, while operators continued to push speed boundaries to deploy payloads—with some executing very quickly and others lying undetected in networks for significant periods of time.¹⁵⁵ This quarter also saw ransomware being used as a decoy in an attack to obfuscate threat actors' real objectives; this tactic was utilized by several ransomware groups, most recently with LockBit 2.0.¹⁵⁶

Changes to threat actor tactics in the post-exploitation stage may indicate that ransomware gangs are finding it increasingly difficult to elicit payments from victims. This quarter saw threat actors hacking corporate websites to display ransom notes to increase pressure on victims.¹⁵⁷ LockBit began testing a new process in which they gradually reduce the ransom demand, hoping victims that initially refuse to pay may decide it is financially prudent to recover stolen data at a lower price. LockBit also went to great lengths to distance itself from the U.S.-sanctioned Evil Corp, likely concerned about lost revenue.¹⁵⁸



➤ Forward Look:

- If ransomware operators struggle to elicit payments from victims, they will likely resort to more extreme pressure tactics that threaten to cause greater operational downtime and reputational damage—which may have legal ramifications.

➤ Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Review breach disclosure obligations in different jurisdictions, particularly with the United States passing the Strengthening American Cybersecurity Act into law in March 2022.¹⁵⁹
- Regularly back up 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.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

| Geopolitics

As anticipated in ZeroFox Intelligence's Q1 2022 report, Russia and its war in Ukraine were the primary drivers of geopolitical risk across industries this quarter.¹⁶⁰ In Q1, Russia's war in Ukraine worsened existing inflation, energy, and cost-of-living issues. In Q2, Russia demonstrated an eagerness to deliberately worsen these crises by strategically limiting energy supplies and using threat actors to target Western allies of Ukraine. Meanwhile, the malicious activities of other traditional sources of geopolitical tension, like China and Iran, are minor in comparison. The slow progress of Russian forces and eastern Ukraine's landscape means a military victory for either side is unlikely in the short term. The complexity in resolving the war makes it very likely it will drag on for years, remaining a primary source of geopolitical risk across industries.

The most obvious sector impacted is energy. Energy shortfalls and reorienting supply chains away from Russia were always part of the Western response to Russia's war in Ukraine. However, Russia began retaliating against Western sanctions in Q2 by cutting off gas supplies to Europe. As Ukraine advanced its EU membership bid, gas supplies were suddenly reduced to countries like Germany and Italy.¹⁶¹ Finland had its supplies cut off entirely after it formally applied to join the North Atlantic Treaty Organization (NATO). In total, 10 EU nations had gas supplies cut for geopolitical reasons in Q2.¹⁶²



This contributes to spiking prices and worsening inflation, which impacts all sectors. Russia aims to use the cost-of-living issues to weaken the West's resolve to support Ukraine, and there is a high probability Russia will cut off Europe entirely from Russian energy supplies in the future.

Cybercriminal groups, likely operating on behalf of the Russian state, launched attacks against government websites and critical infrastructure over opposition to the war in Q2. As speculation rose that Finland would apply to join the NATO alliance, Finland reported multiple government websites and services had been targeted by denial-of-service (DoS) attacks.¹⁶³ When Lithuania attempted to enforce EU sanctions on the Russian enclave of Kaliningrad, Russia publicly threatened retaliation—including non-political maneuvers such as low-level military engagements, disruptions of deliveries of non-sanctioned commodities like oil and gas, and even cyberattacks.

In the short term, businesses with physical operations or sales in EU states, particularly those with close geographic or cultural ties with Russia, should be prepared for an increase in low-level cyber threat activity. The attacks will likely be carried out by criminal groups, like the pro-Russian hacker group Killnet, to allow Russia to maintain plausible deniability.¹⁶⁴ The targets could be sectors most vulnerable to the current supply chain and cost-of-living issues, like energy, agriculture, telecommunications, or transportation. Government websites will also likely be targeted. There may also be influence operations aimed at distorting the narrative around issues like EU/NATO membership or overall support for Ukraine. This threat trend is very likely to continue going forward and will make the business environment difficult. Additionally, the wide-ranging impacts of Russia's war in Ukraine are very likely to trigger a wave of economic crises across emerging markets before 2023 related to debt levels and the rising prices of food and energy. However, the largest geopolitical risk across industries will be Russia's use of energy supplies to influence political behavior.

➤ **Forward Look:**

- As Russia's war with Ukraine drags on, Russian-backed groups will likely seek to weaken Western resolve by exacerbating issues ranging from inflation to energy prices.
- Issues like EU/NATO membership and new sanctions on Russia are likely to trigger a Russian state response, which often involves Russian-backed groups targeting sensitive infrastructure.
- A wave of economic defaults before 2023—triggered by the war—has the potential for straining business operations. The energy crisis, particularly for natural gas, will worsen.

➤ **Recommendations:**

- Configure ZeroFox geopolitical monitoring and alerting for areas of interest.



- Continue to seek alternative supplies of food and energy commodities.
- Increase protections for entities operating in nations that have been openly antagonistic to the war in Ukraine, as Russia is most likely to target operations in those countries.
- Prepare organizations operating in highly-indebted countries for more social unrest.
- Engage the ZeroFox Intelligence Team to conduct an in-depth Regional Threat Landscape report on critical geographic regions of interest that provides an extensive review of risks and threats and highlights potential impacts on business operations and continuity.

Outlook

Russia's invasion of Ukraine will likely continue to heavily influence the cyber threat landscape for at least the duration of the conflict. The conflict and the resulting humanitarian and economic crises will almost certainly continue to be leveraged by threat actors in social engineering lures. Vulnerabilities in cloud infrastructures, perimeter security devices, and commonly-used software modules will likely continue to dominate the exploit landscape. As seen already in Q2 2022, ZeroFox Intelligence anticipates pro-Russian threat actors and state-linked entities will likely increasingly target countries and organizations with malware—including wipers, ransomware, and botnets—in retaliation for perceived stances taken during the war. If ransomware operators struggle to elicit payments from victims, they will likely resort to more extreme pressure tactics, threatening to cause greater operational downtime and reputational damage, which may have legal ramifications.



Appendix

Traffic Light Protocol for Information Dissemination

Red

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.

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.

Amber

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.

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

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.

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.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP: **WHITE** information without restriction, subject to copyright controls.



Endnotes

1. [hXXps://www.bleepingcomputer.com/news/security/google-smtp-relay-service-abused-for-sending-phishing-emails/](https://www.bleepingcomputer.com/news/security/google-smtp-relay-service-abused-for-sending-phishing-emails/)
2. [hXXps://cyberintelmag.com/malware-viruses/flubot-android-malware-aims-finland-in-fresh-sms-attacks/](https://cyberintelmag.com/malware-viruses/flubot-android-malware-aims-finland-in-fresh-sms-attacks/)
3. [hXXps://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/](https://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/)
4. [hXXps://www.bleepingcomputer.com/news/security/hackers-steal-whatsapp-accounts-using-call-forwarding-trick/](https://www.bleepingcomputer.com/news/security/hackers-steal-whatsapp-accounts-using-call-forwarding-trick/)
5. [hXXps://www.techradar.com/uk/news/that-voicemail-message-could-be-a-microsoft-365-phishing-scam](https://www.techradar.com/uk/news/that-voicemail-message-could-be-a-microsoft-365-phishing-scam)
6. [hXXps://www.hackread.com/crooks-spoofing-credit-unions-steal-login-credentials/](https://www.hackread.com/crooks-spoofing-credit-unions-steal-login-credentials/)
7. [hXXps://www.cpomagazine.com/cyber-security/ferrari-website-hacked-used-to-push-nft-scam-that-built-on-official-announcement/](https://www.cpomagazine.com/cyber-security/ferrari-website-hacked-used-to-push-nft-scam-that-built-on-official-announcement/)
8. [hXXps://www.zdnet.com/article/fake-android-shopping-apps-steal-bank-account-logins-2fa-codes/](https://www.zdnet.com/article/fake-android-shopping-apps-steal-bank-account-logins-2fa-codes/)
9. [hXXps://www.itworldcanada.com/post/microsoft-365-credentials-targeted-in-phony-voicemail-campaign](https://www.itworldcanada.com/post/microsoft-365-credentials-targeted-in-phony-voicemail-campaign)
10. [hXXps://blog.malwarebytes.com/scams/2022/04/steer-clear-of-this-sms-tax-refund-phish/](https://blog.malwarebytes.com/scams/2022/04/steer-clear-of-this-sms-tax-refund-phish/)
11. [hXXps://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/](https://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/)
12. [hXXps://www.scmagazine.com/brief/email-security/diplomatic-organizations-attacked-in-apt29-phishing-campaigns](https://www.scmagazine.com/brief/email-security/diplomatic-organizations-attacked-in-apt29-phishing-campaigns)
13. [hXXps://thehackernews.com/2022/05/ukrainian-cert-warns-citizens-of-new.html](https://thehackernews.com/2022/05/ukrainian-cert-warns-citizens-of-new.html)
14. [hXXps://latesthackingnews.com/2022/07/06/astralocker-2-0-ransomware-spreads-via-phishing-campaigns-including-malicious-microsoft-word-files/](https://latesthackingnews.com/2022/07/06/astralocker-2-0-ransomware-spreads-via-phishing-campaigns-including-malicious-microsoft-word-files/)
15. [hXXps://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/](https://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/)
16. [hXXps://blog.malwarebytes.com/scams/2022/05/chromeloder-targets-chrome-browser-users-with-malicious-iso-files/](https://blog.malwarebytes.com/scams/2022/05/chromeloder-targets-chrome-browser-users-with-malicious-iso-files/)
17. [hXXps://www.bleepingcomputer.com/news/security/malicious-windows-lnk-attacks-made-easy-with-new-quantum-builder/](https://www.bleepingcomputer.com/news/security/malicious-windows-lnk-attacks-made-easy-with-new-quantum-builder/)
18. [hXXps://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/](https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/)
19. [hXXps://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html](https://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html)
20. [hXXps://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/](https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/)
21. ZeroFox Intelligence, Raccoon Stealer Version 2.0, B-2022-06-30a
22. [hXXps://securityaffairs.co/wordpress/131296/apt/cert-ua-warns-armageddon-apt.html](https://securityaffairs.co/wordpress/131296/apt/cert-ua-warns-armageddon-apt.html)
23. [hXXps://www.techradar.com/uk/news/qbot-malware-found-smuggled-inside-windows-installer-packages](https://www.techradar.com/uk/news/qbot-malware-found-smuggled-inside-windows-installer-packages)
24. [hXXps://threatpost.com/snake-keylogger-pdfs/179703/](https://threatpost.com/snake-keylogger-pdfs/179703/)
25. [hXXps://www.thetechoutlook.com/news/technology/security/devices-with-cobalt-strike-are-infected-by-new-phishing-attack/](https://www.thetechoutlook.com/news/technology/security/devices-with-cobalt-strike-are-infected-by-new-phishing-attack/)
26. [hXXps://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/](https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/)
27. [hXXps://thehackernews.com/2022/06/researchers-warn-of-spam-campaign.html](https://thehackernews.com/2022/06/researchers-warn-of-spam-campaign.html)
28. [hXXps://thehackernews.com/2022/04/hackers-sneak-moreeggs-malware-into.html](https://thehackernews.com/2022/04/hackers-sneak-moreeggs-malware-into.html)
29. [hXXps://www.scmagazine.com/brief/malware/malspam-campaign-spreads-novel-meta-info-stealer](https://www.scmagazine.com/brief/malware/malspam-campaign-spreads-novel-meta-info-stealer)
30. [hXXps://www.bleepingcomputer.com/news/security/russian-govt-impersonators-target-telcos-in-phishing-attacks/](https://www.bleepingcomputer.com/news/security/russian-govt-impersonators-target-telcos-in-phishing-attacks/)
31. ZeroFox Intelligence, Q1 Financial Sector: Financial Quarterly Threat Landscape, S-2022-05-06a
32. [hXXps://thehackernews.com/2022/05/ukrainian-cert-warns-citizens-of-new.html](https://thehackernews.com/2022/05/ukrainian-cert-warns-citizens-of-new.html)
33. [hXXps://www.infosecurity-magazine.com/news/global-apt-ukraine-war-phishing/](https://www.infosecurity-magazine.com/news/global-apt-ukraine-war-phishing/)
34. [hXXps://www.bleepingcomputer.com/news/security/ukraine-russian-armageddon-phishing-targets-eu-govt-agencies/](https://www.bleepingcomputer.com/news/security/ukraine-russian-armageddon-phishing-targets-eu-govt-agencies/)
35. [hXXps://www.ic3.gov/Media/Y2022/PSA220531](https://www.ic3.gov/Media/Y2022/PSA220531)
36. [hXXps://thehackernews.com/2022/04/hackers-sneak-moreeggs-malware-into.html](https://thehackernews.com/2022/04/hackers-sneak-moreeggs-malware-into.html)
37. [hXXps://cyware.com/news/lazarus-apt-uses-tradertraitor-malware-to-target-cryptocurrency-organizations-b4c1eb47](https://cyware.com/news/lazarus-apt-uses-tradertraitor-malware-to-target-cryptocurrency-organizations-b4c1eb47)
38. [hXXps://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/](https://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/)
39. [hXXps://www.theguardian.com/world/2022/may/17/dont-accidentally-hire-a-north-korean-hacker-fbi-warn](https://www.theguardian.com/world/2022/may/17/dont-accidentally-hire-a-north-korean-hacker-fbi-warn)
40. [hXXps://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information](https://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information)
41. [hXXps://cyware.com/news/inno-stealer-fake-windows-11-upgrade-spreads-infostealer-74a72e5d](https://cyware.com/news/inno-stealer-fake-windows-11-upgrade-spreads-infostealer-74a72e5d)
42. [hXXps://www.zdnet.com/article/fake-domains-offer-windows-11-installers-but-deliver-malware-instead/](https://www.zdnet.com/article/fake-domains-offer-windows-11-installers-but-deliver-malware-instead/)
43. [hXXps://www.bleepingcomputer.com/news/security/hackers-target-russian-govt-with-fake-windows-updates-pushing-rats/](https://www.bleepingcomputer.com/news/security/hackers-target-russian-govt-with-fake-windows-updates-pushing-rats/)
44. [hXXps://www.securityweek.com/soho-routers-north-america-and-europe-targeted-zuorat-malware](https://www.securityweek.com/soho-routers-north-america-and-europe-targeted-zuorat-malware)
45. [hXXps://riskybiznews.com/p/risky-biz-news-microsoft-accused](https://riskybiznews.com/p/risky-biz-news-microsoft-accused)
46. [hXXps://cyware.com/news/cisa-warns-against-russian-hackers-exploiting-a-critical-bug-a0aa7lee](https://cyware.com/news/cisa-warns-against-russian-hackers-exploiting-a-critical-bug-a0aa7lee)
47. ZeroFox Intelligence, Follina Vulnerability, F-2022-06-01a
48. [hXXps://www.darkreading.com/vulnerabilities-threats/icymi-cyber-pro-hopelessness-follina-atlassian](https://www.darkreading.com/vulnerabilities-threats/icymi-cyber-pro-hopelessness-follina-atlassian)
49. [hXXps://techcrunch.com/2022/06/01/china-backed-hackers-are-exploiting-unpatched-microsoft-zero-day/](https://techcrunch.com/2022/06/01/china-backed-hackers-are-exploiting-unpatched-microsoft-zero-day/)
50. [hXXps://securityaffairs.co/wordpress/131992/apt/nation-state-actors-follina-exploits.html](https://securityaffairs.co/wordpress/131992/apt/nation-state-actors-follina-exploits.html)
51. [hXXps://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/](https://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/)
52. [hXXps://www.computing.co.uk/news/4050886/threat-actors-actively-exploiting-windows-follina-zero-day-deliver-qbot-malware](https://www.computing.co.uk/news/4050886/threat-actors-actively-exploiting-windows-follina-zero-day-deliver-qbot-malware)
53. [hXXps://riskybiznews.com/p/risky-biz-news-google-shuts-down](https://riskybiznews.com/p/risky-biz-news-google-shuts-down)



54. [hXXps://www.zdnet.com/article/microsoft-warning-this-malware-that-targets-linux-just-got-a-big-update/](https://www.zdnet.com/article/microsoft-warning-this-malware-that-targets-linux-just-got-a-big-update/)
55. [hXXps://threatpost.com/exploit-f5-big-ip-bug/179563/#:~:text=Share%20this%20article%3A,vulnerability%20was%20publicly%20made%20available.](https://threatpost.com/exploit-f5-big-ip-bug/179563/#:~:text=Share%20this%20article%3A,vulnerability%20was%20publicly%20made%20available.)
56. [hXXps://www.computing.co.uk/news/4050482/iot-enemybot-vmware-f5-big-ip](https://www.computing.co.uk/news/4050482/iot-enemybot-vmware-f5-big-ip)
57. [hXXps://securityaffairs.co/wordpress/129998/hacking/mirai-based-botnet-spring4shell.html](https://securityaffairs.co/wordpress/129998/hacking/mirai-based-botnet-spring4shell.html)
58. This assessment is based on illicit access sales that occurred in open marketplaces and covert communications channels that ZeroFox Intelligence monitors, yet the scope of activity that may have fallen outside these collections channels is also recognized.
59. [hXXps://arstechnica.com/tech-policy/2022/06/feds-seize-ssndob-marketplace-that-listed-personal-data-of-24-million-people/](https://arstechnica.com/tech-policy/2022/06/feds-seize-ssndob-marketplace-that-listed-personal-data-of-24-million-people/)
60. [hXXps://portswigger.net/daily-swig/authorities-seize-hydra-servers-in-bust-against-darknet-cybercrime-marketplace](https://portswigger.net/daily-swig/authorities-seize-hydra-servers-in-bust-against-darknet-cybercrime-marketplace)
61. [hXXps://www.bbc.co.uk/news/technology-61082144](https://www.bbc.co.uk/news/technology-61082144)
62. [hXXps://www.bleepingcomputer.com/news/security/darknet-market-versus-shuts-down-after-hacker-leaks-security-flaw/](https://www.bleepingcomputer.com/news/security/darknet-market-versus-shuts-down-after-hacker-leaks-security-flaw/)
63. [hXXps://www.zdnet.com/article/doj-takes-down-russian-botnet-that-targeted-watchguard-and-asus-routers/](https://www.zdnet.com/article/doj-takes-down-russian-botnet-that-targeted-watchguard-and-asus-routers/)
64. [hXXps://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation](https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation)
65. ZeroFox Intelligence, Q1 Financial Sector: Financial Quarterly Threat Landscape, S-2022-05-06a
66. [hXXps://www.bleepingcomputer.com/news/security/ukraine-targeted-by-ddos-attacks-from-compromised-wordpress-sites/](https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-ddos-attacks-from-compromised-wordpress-sites/)
67. [hXXps://www.infosecurity-magazine.com/news/ukrainians-ddos-russian-vodka/](https://www.infosecurity-magazine.com/news/ukrainians-ddos-russian-vodka/)
68. [hXXps://www.secureblink.com/cyber-security-news/sberbank-targeted-by-a-staggering-wave-of-d-do-s-attacks-that-was-earlier-mitigated](https://www.secureblink.com/cyber-security-news/sberbank-targeted-by-a-staggering-wave-of-d-do-s-attacks-that-was-earlier-mitigated)
69. ZeroFox Intelligence, Treading on the Boundaries: How Pro-Russian Threat Actors are Exacerbating NATO Geopolitical Tensions, B-2022-06-23a
70. [hXXps://www.reuters.com/world/europe/norway-targeted-by-cyber-attack-security-agency-2022-06-29/](https://www.reuters.com/world/europe/norway-targeted-by-cyber-attack-security-agency-2022-06-29/)
71. [hXXps://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/](https://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/)
72. [hXXps://www.securityweek.com/lithuania-says-hit-cyberattack-russia-probably-blame](https://www.securityweek.com/lithuania-says-hit-cyberattack-russia-probably-blame)
73. [hXXps://www.bleepingcomputer.com/news/security/beastmode-botnet-boosts-ddos-power-with-new-router-exploits/](https://www.bleepingcomputer.com/news/security/beastmode-botnet-boosts-ddos-power-with-new-router-exploits/)
74. [hXXps://securityaffairs.co/wordpress/130112/security/cisa-watchguard-flaw-known-exploited-vulnerabilities-catalog.html](https://securityaffairs.co/wordpress/130112/security/cisa-watchguard-flaw-known-exploited-vulnerabilities-catalog.html)
75. [hXXps://thehackernews.com/2022/06/new-xloader-botnet-version-using.html](https://thehackernews.com/2022/06/new-xloader-botnet-version-using.html)
76. ZeroFox Intelligence expanded its collections capability in Q2 2022, which very likely accounts for the disparity in credentials ingested between Q1 2022 and Q2 2022 (rather than an increase in threats).
77. [hXXps://www.securityweek.com/cloudflare-customer-targeted-record-hXXps-ddos-attack](https://www.securityweek.com/cloudflare-customer-targeted-record-hXXps-ddos-attack)
78. [hXXps://blog.cloudflare.com/26m-rps-ddos/](https://blog.cloudflare.com/26m-rps-ddos/)
79. ZeroFox Intelligence Internal Collections, Jun 24, 2022
80. ZeroFox Intelligence, Treading on the Boundaries: How Pro-Russian Threat Actors are Exacerbating NATO Geopolitical Tensions, B-2022-06-23a
81. [hXXps://cyberintelmag.com/attacks-data-breaches/emotet-botnet-upgraded-to-64-bit-modules-activity-increases/](https://cyberintelmag.com/attacks-data-breaches/emotet-botnet-upgraded-to-64-bit-modules-activity-increases/)
82. [hXXps://www.scmagazine.com/analysis/malware/updated-emotet-banking-trojan-more-effective-proliferates-through-excel-macro](https://www.scmagazine.com/analysis/malware/updated-emotet-banking-trojan-more-effective-proliferates-through-excel-macro)
83. [hXXps://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/](https://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/)
84. [hXXps://latesthackingnews.com/2022/06/13/emotet-malware-evolves-to-steal-data-from-chrome-browser/](https://latesthackingnews.com/2022/06/13/emotet-malware-evolves-to-steal-data-from-chrome-browser/)
85. [hXXps://threatpost.com/telegram-spread-eternity-maas/179623/](https://threatpost.com/telegram-spread-eternity-maas/179623/)
86. [hXXps://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html](https://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html)
87. [hXXps://www.pcmag.com/news/this-android-malware-can-hijack-phone-calls-to-customer-support](https://www.pcmag.com/news/this-android-malware-can-hijack-phone-calls-to-customer-support)
88. [hXXps://thehackernews.com/2022/04/sharkbot-banking-trojan-resurfaces-on.html](https://thehackernews.com/2022/04/sharkbot-banking-trojan-resurfaces-on.html)
89. [hXXps://cyberintelmag.com/malware-viruses/another-group-of-android-apps-infected-with-joker-trojan-has-resurfaced-on-google-play/](https://cyberintelmag.com/malware-viruses/another-group-of-android-apps-infected-with-joker-trojan-has-resurfaced-on-google-play/)
90. [hXXps://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter](https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter)
91. [hXXps://www.zdnet.com/article/this-new-malware-is-now-at-the-heart-of-the-ransomware-ecosystem/](https://www.zdnet.com/article/this-new-malware-is-now-at-the-heart-of-the-ransomware-ecosystem/)
92. [hXXps://www.bleepingcomputer.com/news/security/chinese-hackers-target-script-kiddies-with-info-stealer-trojan/](https://www.bleepingcomputer.com/news/security/chinese-hackers-target-script-kiddies-with-info-stealer-trojan/)
93. [hXXps://www.scmagazine.com/brief/ransomware/more-cyberattacks-using-novel-bumblebee-malware](https://www.scmagazine.com/brief/ransomware/more-cyberattacks-using-novel-bumblebee-malware)
94. [hXXps://socprime.com/blog/matanbuchus-malware-detection-new-malspam-campaign-distributes-malware-loader-and-cobalt-strike/](https://socprime.com/blog/matanbuchus-malware-detection-new-malspam-campaign-distributes-malware-loader-and-cobalt-strike/)
95. [hXXps://theglobalinside.com/new-netdooka-malware-spreads-through-poisoned-search-results/](https://theglobalinside.com/new-netdooka-malware-spreads-through-poisoned-search-results/)
96. [hXXps://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/](https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/)
97. [hXXps://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim](https://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim)
98. [hXXps://cyware.com/news/inno-stealer-fake-windows-11-upgrade-spreads-infostealer-74a72e5d](https://cyware.com/news/inno-stealer-fake-windows-11-upgrade-spreads-infostealer-74a72e5d)
99. [hXXps://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/](https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/)



100. [hXXps://cybersecuritynews\[.\]com/ffdroider-stealer-malware/](https://cybersecuritynews[.]com/ffdroider-stealer-malware/)
101. [hXXps://cyware\[.\]com/news/lightning-stealer-new-info-stealer-spotted-in-the-wild-74244757](https://cyware[.]com/news/lightning-stealer-new-info-stealer-spotted-in-the-wild-74244757)
102. [hXXps://thehackernews\[.\]com/2022/05/experts-detail-saintstealer-and-prynt.html](https://thehackernews[.]com/2022/05/experts-detail-saintstealer-and-prynt.html)
103. [hXXps://www.thetechoutlook\[.\]com/news/technology/new-meta-information-stealer-distributed-in-malspam-campaign/](https://www.thetechoutlook[.]com/news/technology/new-meta-information-stealer-distributed-in-malspam-campaign/)
104. ZeroFox Intelligence, Raccoon Stealer Version 2.0, B-2022-06-30a
105. [hXXps://www.bleepingcomputer\[.\]com/news/security/gallium-hackers-backdoor-finance-govt-orgs-using-new-pingpull-malware/](https://www.bleepingcomputer[.]com/news/security/gallium-hackers-backdoor-finance-govt-orgs-using-new-pingpull-malware/)
106. [hXXps://threatpost\[.\]com/nerbian-rat-advanced-trick/179600/](https://threatpost[.]com/nerbian-rat-advanced-trick/179600/)
107. [hXXps://blog.malwarebytes\[.\]com/threat-analysis/2022/06/asyncrat-surpasses-dridex-trickbot-and-emetet-to-become-dominant-mail-threat/](https://blog.malwarebytes[.]com/threat-analysis/2022/06/asyncrat-surpasses-dridex-trickbot-and-emetet-to-become-dominant-mail-threat/)
108. [hXXps://thehackernews\[.\]com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html](https://thehackernews[.]com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html)
109. [hXXps://www.bleepingcomputer\[.\]com/news/security/android-wiping-brata-malware-is-evolving-into-a-persistent-threat/](https://www.bleepingcomputer[.]com/news/security/android-wiping-brata-malware-is-evolving-into-a-persistent-threat/)
110. [hXXps://securityaffairs\[.\]co/wordpress/131705/malware/ermac-2-0-android-banking-trojan.html](https://securityaffairs[.]co/wordpress/131705/malware/ermac-2-0-android-banking-trojan.html)
111. [hXXps://cyberintelmag\[.\]com/malware-viruses/android-malware-called-revive-poses-as-2fa-app-for-spains-bbva-bank/](https://cyberintelmag[.]com/malware-viruses/android-malware-called-revive-poses-as-2fa-app-for-spains-bbva-bank/)
112. [hXXps://thehackernews\[.\]com/2022/05/latest-mobile-malware-report-suggests.html](https://thehackernews[.]com/2022/05/latest-mobile-malware-report-suggests.html)
113. [hXXps://cybersecuritynews\[.\]com/debit-card-stealing-skimmers/#:~:text=Bank%20of%20the%20West%20has,was%20identified%20by%20the%20bank.](https://cybersecuritynews[.]com/debit-card-stealing-skimmers/#:~:text=Bank%20of%20the%20West%20has,was%20identified%20by%20the%20bank.)
114. [hXXps://www.ic3\[.\]gov/Media/News/2022/220516.pdf](https://www.ic3[.]gov/Media/News/2022/220516.pdf)
115. [hXXps://www.bleepingcomputer\[.\]com/news/security/microsoft-credit-card-stealers-are-getting-much-stealthier/](https://www.bleepingcomputer[.]com/news/security/microsoft-credit-card-stealers-are-getting-much-stealthier/)
116. [hXXps://thehackernews\[.\]com/2022/05/over-200-apps-on-play-store-caught.html](https://thehackernews[.]com/2022/05/over-200-apps-on-play-store-caught.html)
117. [hXXps://www.theregister\[.\]com/2022/04/11/nso_spyware_eu/](https://www.theregister[.]com/2022/04/11/nso_spyware_eu/)
118. [hXXps://www.infosecurity-magazine\[.\]com/news/pegasus-spyware-uk-prime-minister/](https://www.infosecurity-magazine[.]com/news/pegasus-spyware-uk-prime-minister/)
119. [hXXps://www.euronews\[.\]com/next/2022/05/02/pegasus-spyware-spain-s-prime-minister-and-defence-minister-s-phones-infected-by-spying-so](https://www.euronews[.]com/next/2022/05/02/pegasus-spyware-spain-s-prime-minister-and-defence-minister-s-phones-infected-by-spying-so)
120. [hXXps://www.techradar\[.\]com/news/zero-click-iphone-exploit-abused-to-launch-nso-spyware-attacks](https://www.techradar[.]com/news/zero-click-iphone-exploit-abused-to-launch-nso-spyware-attacks)
121. [hXXps://www.bleepingcomputer\[.\]com/news/security/spyware-vendor-works-with-isps-to-infect-ios-and-android-users/](https://www.bleepingcomputer[.]com/news/security/spyware-vendor-works-with-isps-to-infect-ios-and-android-users/)
122. [hXXps://twitter\[.\]com/BankofZambia/status/1525048404337893376](https://twitter[.]com/BankofZambia/status/1525048404337893376)
123. [hXXps://www.thetechoutlook\[.\]com/news/technology/security/tb-kawashima-the-japanese-automotive-supplier-is-targeted-by-the-lockbit-ransomware-attack/](https://www.thetechoutlook[.]com/news/technology/security/tb-kawashima-the-japanese-automotive-supplier-is-targeted-by-the-lockbit-ransomware-attack/)
124. [hXXps://www.reuters\[.\]com/technology/japanese-automotive-hose-maker-nichirin-hit-by-ransomware-attack-2022-06-22/](https://www.reuters[.]com/technology/japanese-automotive-hose-maker-nichirin-hit-by-ransomware-attack-2022-06-22/)
125. [hXXps://techcrunch\[.\]com/2022/06/02/foxconn-ransomware-attack-mexico-factory/](https://techcrunch[.]com/2022/06/02/foxconn-ransomware-attack-mexico-factory/)
126. [hXXps://portswigger\[.\]net/daily-swig/ransomware-attack-on-montrose-environmental-group-disrupts-lab-testing-services](https://portswigger[.]net/daily-swig/ransomware-attack-on-montrose-environmental-group-disrupts-lab-testing-services)
127. [hXXps://www.bleepingcomputer\[.\]com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/](https://www.bleepingcomputer[.]com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/)
128. [hXXps://www.securityweek\[.\]com/healthcare-technology-provider-omnicell-discloses-ransomware-attack](https://www.securityweek[.]com/healthcare-technology-provider-omnicell-discloses-ransomware-attack)
129. [hXXps://www.teiss\[.\]co.uk/news/brazilian-retail-giant-fast-shops-cloud-databases-breached-by-a-ransomware-group-10325](https://www.teiss[.]co.uk/news/brazilian-retail-giant-fast-shops-cloud-databases-breached-by-a-ransomware-group-10325)
130. [https://www.bankinfosecurity\[.\]com/black-basta-claims-responsibility-for-agco-attack-a-19146](https://www.bankinfosecurity[.]com/black-basta-claims-responsibility-for-agco-attack-a-19146)
131. [hXXps://threatpost\[.\]com/ransomware-deathblow-college/179574/](https://threatpost[.]com/ransomware-deathblow-college/179574/)
132. [hXXps://www.bleepingcomputer\[.\]com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/](https://www.bleepingcomputer[.]com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/)
133. [hXXps://www.itworldcanada\[.\]com/post/clop-ransomware-returns-21-victims-suffer-cyberattack](https://www.itworldcanada[.]com/post/clop-ransomware-returns-21-victims-suffer-cyberattack)
134. [hXXps://www.bleepingcomputer\[.\]com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/](https://www.bleepingcomputer[.]com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/)
135. [hXXps://www.trendmicro\[.\]com/en_us/research/22/t/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html](https://www.trendmicro[.]com/en_us/research/22/t/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html)
136. [hXXps://www.securityweek\[.\]com/conti-ransomware-operation-shut-down-after-brand-becomes-toxic](https://www.securityweek[.]com/conti-ransomware-operation-shut-down-after-brand-becomes-toxic)
137. ZeroFox Intelligence Internal Collections
138. [hXXps://www.cisa\[.\]gov/uscert/ncas/alerts/aa22-152a](https://www.cisa[.]gov/uscert/ncas/alerts/aa22-152a)
139. [hXXps://www.bleepingcomputer\[.\]com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/](https://www.bleepingcomputer[.]com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/)
140. [hXXps://www.theguardian\[.\]com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks](https://www.theguardian[.]com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks)
141. [hXXps://securityaffairs\[.\]co/wordpress/131093/cyber-crime/conti-ransomware-peru-direccion-general-de-inteligencia.html](https://securityaffairs[.]co/wordpress/131093/cyber-crime/conti-ransomware-peru-direccion-general-de-inteligencia.html)
142. [hXXps://www.bleepingcomputer\[.\]com/news/security/conti-ransomware-hacking-spree-breaches-over-40-orgs-in-a-month/](https://www.bleepingcomputer[.]com/news/security/conti-ransomware-hacking-spree-breaches-over-40-orgs-in-a-month/)
143. [hXXps://www.securityweek\[.\]com/conti-ransomware-gang-claims-cyberattack-wind-turbine-giant-nordex](https://www.securityweek[.]com/conti-ransomware-gang-claims-cyberattack-wind-turbine-giant-nordex)
144. [hXXps://www.scmagazine\[.\]com/editorial/brief/ransomware/black-basta-ransomware-impacts-american-dental-association](https://www.scmagazine[.]com/editorial/brief/ransomware/black-basta-ransomware-impacts-american-dental-association)
145. [hXXps://threatpost\[.\]com/black-basta-ransomware-qbot/179909/](https://threatpost[.]com/black-basta-ransomware-qbot/179909/)
146. [hXXps://twitter\[.\]com/BrettCallow/status/1524387838531301377](https://twitter[.]com/BrettCallow/status/1524387838531301377)
147. [hXXps://thehackernews\[.\]com/2022/06/cybersecurity-experts-warn-of-emerging.html](https://thehackernews[.]com/2022/06/cybersecurity-experts-warn-of-emerging.html)
148. [hXXps://twitter\[.\]com/bofheaded/status/1524340263657046016](https://twitter[.]com/bofheaded/status/1524340263657046016)
149. [hXXps://www.bleepingcomputer\[.\]com/news/security/new-cheers-linux-ransomware-targets-vmware-esxi-servers/](https://www.bleepingcomputer[.]com/news/security/new-cheers-linux-ransomware-targets-vmware-esxi-servers/)
150. [hXXps://blog.cyble\[.\]com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/](https://blog.cyble[.]com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/)
151. [hXXps://thehackernews\[.\]com/2022/05/new-goodwill-ransomware-forces-victims.html](https://thehackernews[.]com/2022/05/new-goodwill-ransomware-forces-victims.html)



- 152. [hXXps://thehackernews\[.\]com/2022/05/new-chaos-ransomware-builder-variant.html](https://thehackernews.com/2022/05/new-chaos-ransomware-builder-variant.html)
- 153. [hXXps://www.bleepingcomputer\[.\]com/news/security/fin7-hackers-evolve-toolset-work-with-multiple-ransomware-gangs/](https://www.bleepingcomputer.com/news/security/fin7-hackers-evolve-toolset-work-with-multiple-ransomware-gangs/)
- 154. [hXXps://www.scmagazine\[.\]com/editorial/brief/ransomware/industrial-spy-ventures-into-ransomware](https://www.scmagazine.com/editorial/brief/ransomware/industrial-spy-ventures-into-ransomware)
- 155. [hXXps://cyware\[.\]com/news/quantum-ransomware-stuns-researchers-with-blazing-fast-attack-speed-6ab9b140](https://cyware.com/news/quantum-ransomware-stuns-researchers-with-blazing-fast-attack-speed-6ab9b140)
- 156. [hXXps://thehackernews\[.\]com/2022/06/state-backed-hackers-using-ransomware.html](https://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html)
- 157. [hXXps://www.bleepingcomputer\[.\]com/news/security/ransomware-gang-now-hacks-corporate-websites-to-show-ransom-notes/](https://www.bleepingcomputer.com/news/security/ransomware-gang-now-hacks-corporate-websites-to-show-ransom-notes/)
- 158. [hXXps://www.crn\[.\]com/news/security/mandiant-no-evidence-of-lockbit-2-0-ransomware-attack-at-this-point-](https://www.crn.com/news/security/mandiant-no-evidence-of-lockbit-2-0-ransomware-attack-at-this-point-)
- 159. [hXXps://www.congress\[.\]gov/bill/117th-congress/senate-bill/3600/all-info](https://www.congress.gov/bill/117th-congress/senate-bill/3600/all-info)
- 160. ZeroFox Intelligence, Q1 Financial Sector: Financial Quarterly Threat Landscape, S-2022-05-06a
- 161. [hXXps://www.ft\[.\]com/content/d0c5815f-f0a2-49ad-8772-f4b0fbbd2c94](https://www.ft.com/content/d0c5815f-f0a2-49ad-8772-f4b0fbbd2c94)
- 162. [https://www.euronews\[.\]com/my-europe/2022/07/07/which-eu-countries-have-been-totally-or-partially-cut-off-from-russian-gas](https://www.euronews.com/my-europe/2022/07/07/which-eu-countries-have-been-totally-or-partially-cut-off-from-russian-gas)
- 163. [hXXps://www.bloomberg\[.\]com/news/articles/2022-04-08/finland-hit-by-cyber-attack-airspace-breach-as-nato-bid-weighed](https://www.bloomberg.com/news/articles/2022-04-08/finland-hit-by-cyber-attack-airspace-breach-as-nato-bid-weighed)
- 164. ZeroFox Intelligence Internal Collections

