EclecticIQ

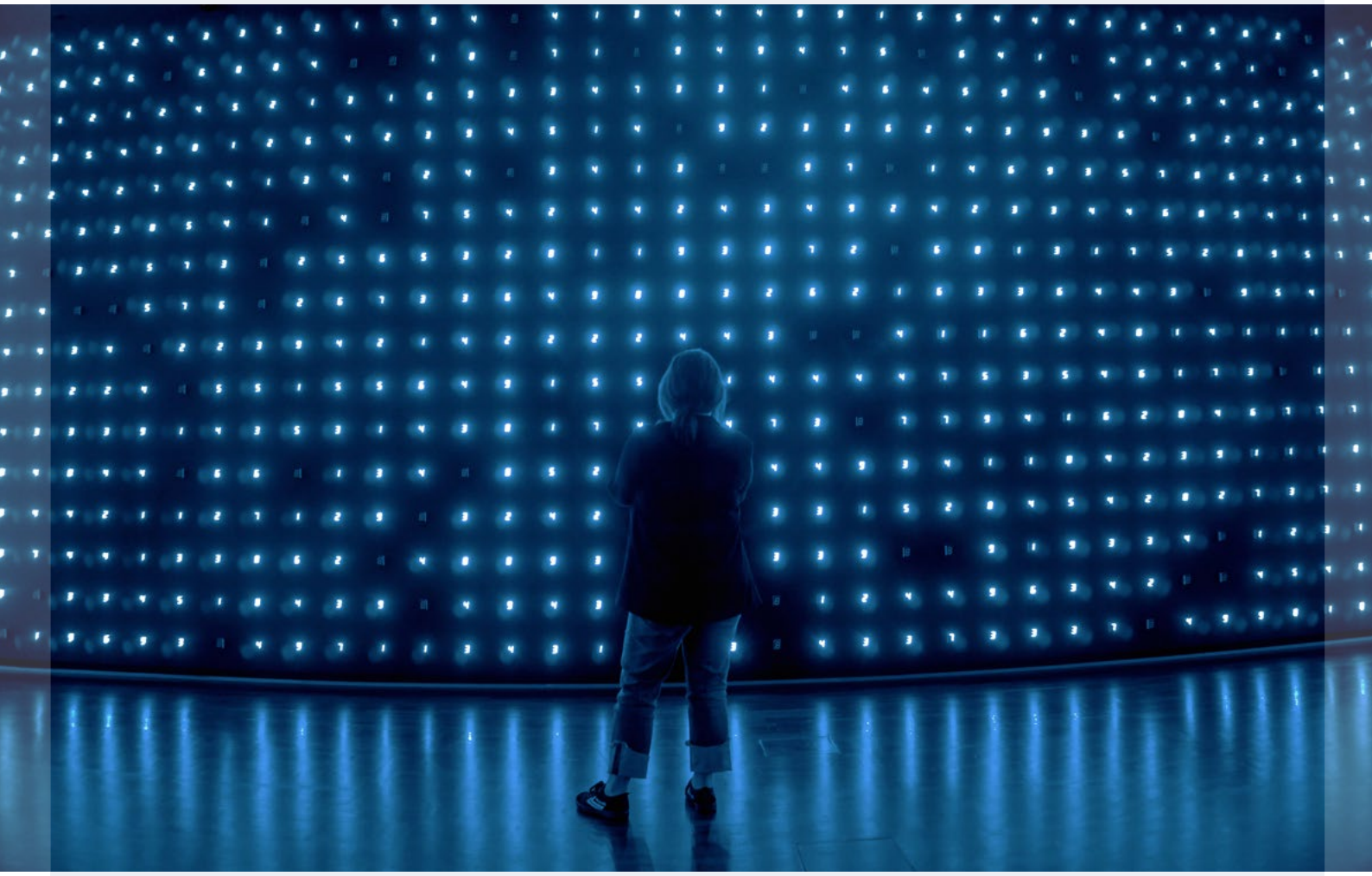
Intelligence at the core

Intelligence Hunting Response

END OF YEAR REPORT

EclecticIQ Retrospective: Themes and Events That Shaped the 2022 Cyber Landscape

by **EclecticIQ Intelligence and Research**



EclecticIQ is pleased to present our 2022 retrospective. In it, we examined malware, threat actor groups, and decentralized finance. As a European company, we also felt compelled to touch on this year's escalation of the Russo-Ukrainian War. Finally, we closed with an examination of the potential of ChatGPT, and a look at the cybersecurity industry.

www.eclecticiq.com | research@eclecticiq.com

Executive Summary

As this year draws to a close, EclecticIQ's Intelligence and Research team looked back on another year of growth and change in cybersecurity. This year brought about changes in **malware TTPs** and **threat actor groups**, which are central topics to cyber researchers around the world. The team examined **the cyber industry** itself and how it changed – albeit gradually – throughout the year. This paper also touches on the tumultuous year in **decentralized finance** (DeFi) and cyber angle of one of the year's most shocking events: **the Russian invasion of Ukraine.** Finally, EclecticIQ analysts examined the **potential of ChatGPT.**

- **Evolution of initial access tactics** and techniques used in malware drove further cyberattacks this year. Threat actors demonstrated their ability to **incorporate new technology**, including deepfake media, and resurface despite increasing pressure from coordinated infrastructure takedowns.

- **Criminal groups primarily leveraged extortion techniques.** Information stealers played a major role in criminal operations and "double/triple extortion" is becoming commonplace. EclecticIQ analysts assess **extortion will evolve during 2023 with "extortion-only" groups playing a more predominant role** in the criminal ecosystem.

- The **cybersecurity industry experienced incremental change and growth this year;** EclecticIQ analysts were most appreciative to see **governments adapt to address enduring cybersecurity challenges** and **use creative methods to disrupt cyber threat actors. In 2023,** the cyber industry should **prioritize cybersecurity education,** and companies that have not already done so should follow the lead of other companies **elevating cybersecurity to a C-suite issue.**

- **Increasing cyberattack activity coupled with decreasing market capitalization drive incentives likely to change decentralized finance over the short term.** Patterns identified in the cyberattack landscape set the stage for short-term challenges to end users and organizations alike.

- Russian **cyber operations against Ukraine did not deliver key anticipated strategic advantages.** EclecticIQ analysts assess effects of **cyber-attacks complementing military objectives did not materialize** as anticipated. Significant **support by Western partners hardened Ukraine's cyber defense capabilities.** Russian **information operations** will likely **continue** with **espionage** activities focused on **Europe's response plan to an energy crisis.**

- The introduction of **ChatGPT** presents new opportunities for CTI analysis and has the potential to **fundamentally disrupt 2023's technology landscape.**

I: Malware: Changing Malware Across 2022 Highlights Evolving Tactics for Initial Access

Awareness of important changes to malware from year to year allows information security practitioners to anticipate major threats to their environment instead of being reactive. In addition to mastering best practices, EclecticIQ analysts recommend further preparation and consideration for prominent changes highlighted using data and observations within the malware landscape from 2022 into 2023.

Government Takedowns and Industry-Led Malware Mitigation Likely to Increase with Short-Lived Impact to Malware Developers

Offensive cyber posturing efforts appear to be increasing in pace and spreading, [1],[2],[3] while long-term efficacy remains unclear. This year Microsoft affected changes to how its software handles VBA scripts (macros) by default to mitigate a common initial execution path: T1059 (Command and Scripting Interpreter) resulting from T1204 (User Execution of Malicious Link/File/Image). Prior to the changeover, data from ESET [4] found Emotet developers were already anticipating the change by modifying malware to use LNK files in malicious emails. By dropping T1059 and retooling T1204.001, threat actors quickly and successfully circumvented Microsoft's mitigation efforts. EclecticIQ analysts also observe threat actors shifting to ".iso" files in the weaponization/delivery phases to remain effective. [5],[6],[7] In another example, Dutch police attempted a takedown against Flubot infrastructure in late spring. [8] However, data from Avast in Q3 2022 showed Flubot infections increased compared to infections before takedown operations, demonstrating the takedown had limited impact at best. [9] Although official malware countermeasures may not have long lasting success, government and industry-driven changes such as these set cybersecurity examples for how technology organizations might centrally manage vulnerabilities increasingly in the future.

Private Vendors Elevate Threats From 'Zero-Click' Mobile Malware

Mobile must be considered under an organization's attack surface to bring mobile devices under increased security coverage, because mobile malware of high capability is almost certainly available to threat actors with the highest resources. [10] Various governments are possibly deploying mobile device malware for nefarious purposes. Mobile malware is also well established among threat actors due to the global ubiquity of mobile devices. It is possible that COVID-19 lockdowns spurred greater mobile malware interest due to ecommerce acceleration. Mobile traffic has been challenging other traffic for volume majority since approximately 2017, and now comprises a larger percentage of internet traffic than other internet connected systems. Mobile apps are a primary vector for mobile malware. [11] Measured in the beginning of 2022, one in four mobile applications contains at least one high-risk security flaw and half of apps with between five and ten million downloads include a security flaw. [12] Increased operational security for sensitive industries that rely on mobile devices is necessary to maintain an increased level of privacy and cybersecurity going forward.

New Social Engineering Cyberattacks Deploying Deepfake Media Target Cryptocurrency

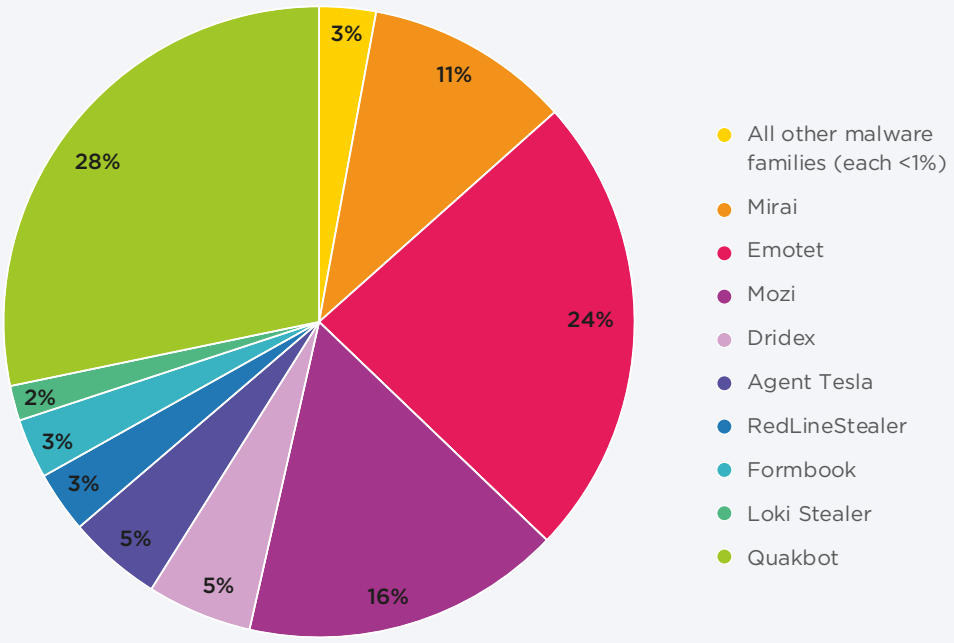
This year, deepfake media progressed in sophistication to the point it could be used by a variety of threat actors to gain targeted privileged access to organizations.

One prominent 2022 example included a reportedly convincing deepfake impersonating the CCO of Binance. [13] In another case, a likeness of Elon Musk in an interview was used to attempt to scam a broad pool of victims out of cryptocurrency via the BitVex exchange platform.[14] Almost all cyberattacks involve cryptocurrency although EclecticIQ analysts note broader experimentation with deepfakes exists on social media compared to previous years reporting. [15],[16],[17]

In 2023 The Threat of Deepfake Media Technology is Likely to Spread

The highest risk of deepfake media TTP evolution is the potential for it to be convincingly deployed in both targeted cyberattacks against privileged individuals, and in cyberattacks against broader audiences. [18] EclecticIQ analysts anticipate more convincing generative adversarial networks (GANs) – synthetic media manipulation through generating fake identities that interact in false 'networks' – will be the greatest deepfake-related threat to broader audiences. These networks are currently difficult to detect and remove. Helpful technology exists, but tools are not yet widely available to the average organization. Near-peer adversary-created deepfake cyberattacks co-opting an individual's persona will become more convincing and are most likely to be used in highly targeted attacks. The fake media earlier this year using the likeness of Ukrainian President Zelensky is an example of this type of targeted threat. [19] These attacks remain the territory of the most advanced threat actors for now. Emphasis on deploying technologies to detect deepfakes will be more important than end-user recognition training. Any such technology solution is very likely to involve content access issues involving strong privacy concerns.

According to a review of all 2022 data from EclecticIQ Intelligence Center, initial access malware and information stealers targeting account credentials were the most prevalent families, followed by remote access trojans, from data involving high-volume malware and excluding ransomware.



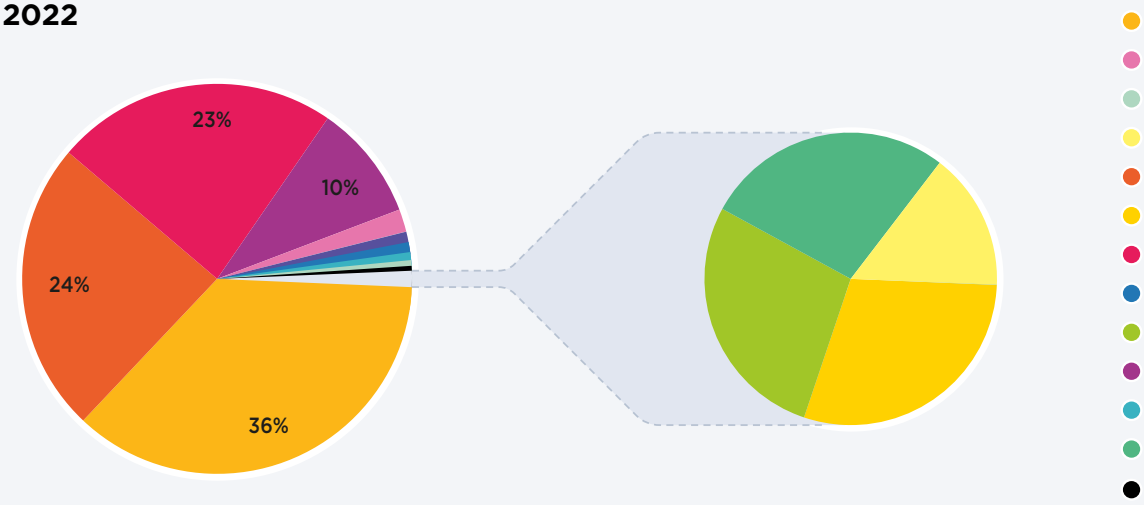
Malware families and relative percentages observed across all of 2022, based on data in the EclecticIQ Intelligence Center

Initial Access Malware Continues to Focus on Multiple Stage Infections and Increasing Versatility

Different malware families change as threat actors specialize and network with other threat actor groups. Botnets are being heavily adapted as information stealers to provide account credentials used in follow-on attacks by other threat actors. Botnets in general are also increasingly adaptable for different types of cyberattacks, driving their popularity in some of EclecticIQ's datasets.

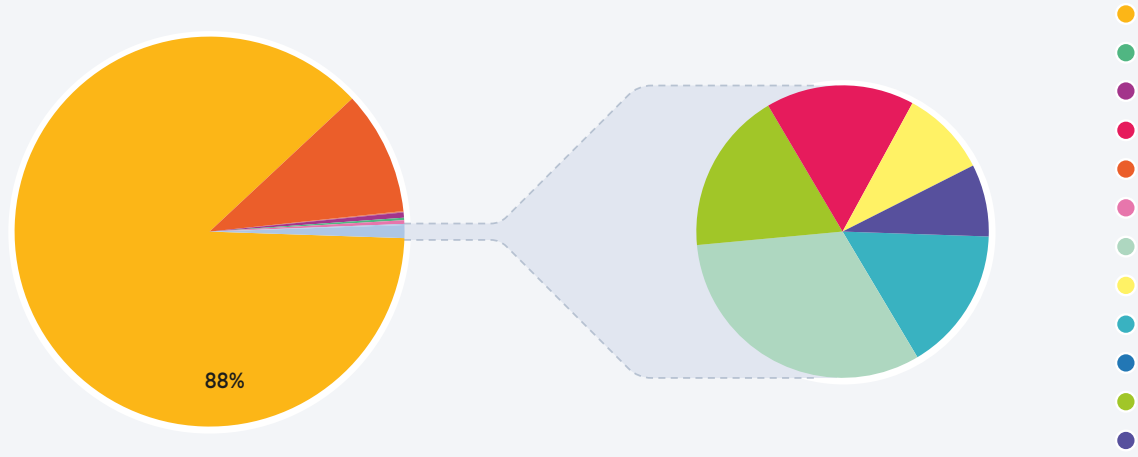
In addition to information harvesting botnets, remote access trojans and specialized dropper malware are increasing because they provide an adaptable and modular way for threat actors to effectively expand their footprint on a compromised system without detection—they are not always the final payload. XLSM malware is an example of a specialized dropper that was unable to remain successful due to Microsoft's changes to file macros earlier this year. [20] [21]

Q1 2022



Snapshot of malware families observed during the first quarter of 2022 based on data in the EclecticIQ Intelligence Center excluding ransomware

Q4 2022



Snapshot of malware families observed during the last quarter of 2022 based on data in the EclecticIQ Intelligence Center excluding ransomware

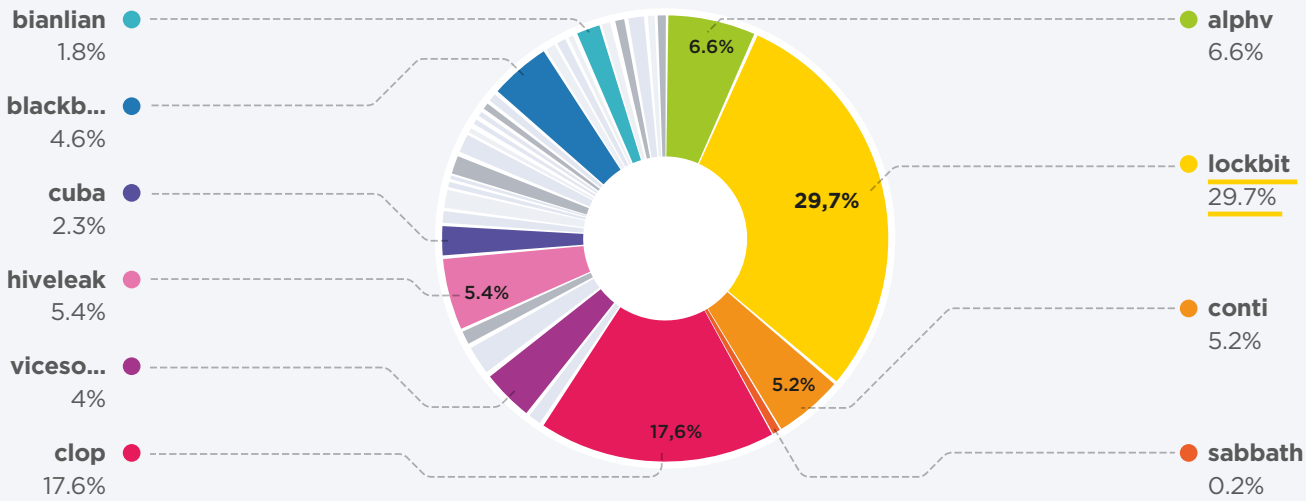
II: Threat Actor Groups: Extortion-Only Groups Played a Major Role in 2022

Criminal Groups Pushed More Extortion Techniques to Increase Payout Likelihood

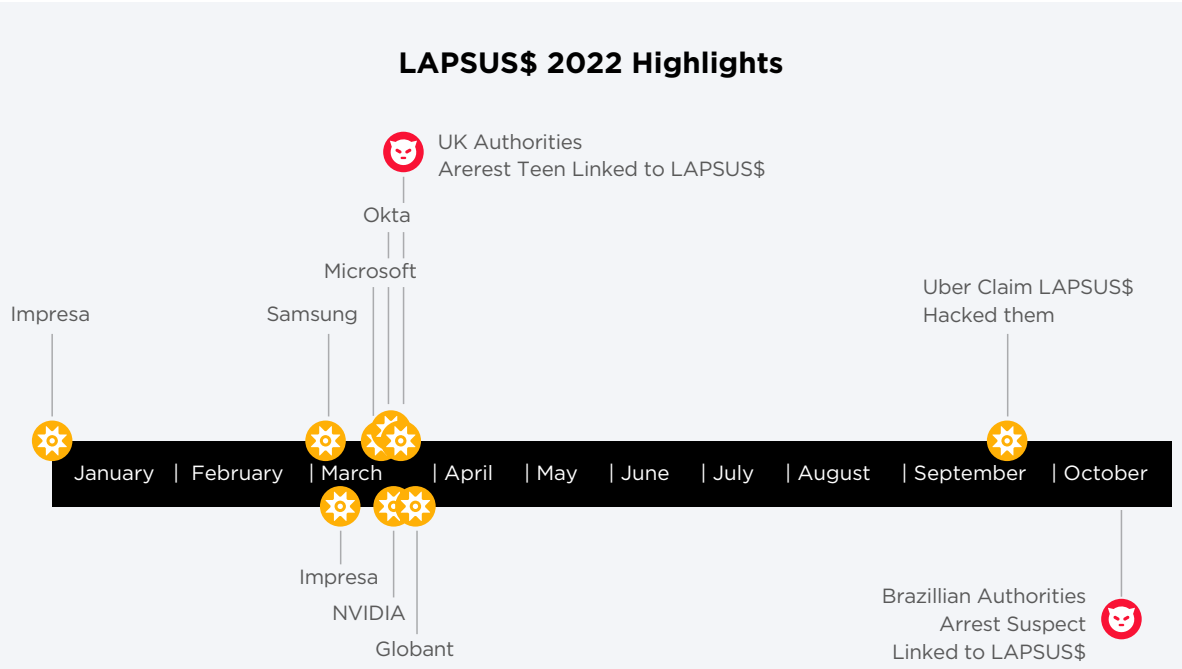
Extortion techniques dominated the cybercriminal threat landscape throughout 2022 with many ransomware groups using double extortion to maximize their odds of success. The most active group during Q1-Q3 2022, based on leak site activity, Lockbit, shifted towards a triple extortion model indicated in a criminal forum. [22] Lockbit leveraged double-extortion techniques throughout 2022, ransoming a company's internal network then exfiltrating data to blackmail the victim into payment. In Q3 2022 LockBit moved to triple-extortion by adding a targeted DDoS (distributed denial of service) capability to their toolset, further pressuring victims to pay the ransom. A new ransomware group, ALPHV, added another technique to their toolkit to put more pressure on victims to pay ransoms. The group developed and deployed a search capability for their leak site, allowing users to access leaked data more easily, with the aim of victim organizations being more inclined to pay the ransom if they knew their personal data could be easily identified and found.[23]

"Extortion-only" groups were responsible for some of 2022's most high-profile breaches [24], [25], [26], providing organizations a new threat type to prioritize. Pure extortion groups do not use a ransomware payload to encrypt victim's data. Instead, they exfiltrate data and threaten to release it publicly unless a ransom is paid. An infamous pure extortion group active in 2022 that exemplifies how these groups operate is LAPSUS$; a financially motivated group first appearing in December 2021 targeting organizations in the United Kingdom and South America. [24] During 2022, the group claimed to breach and steal data from major technology

Ransomware Group Leak Site Notifications



Percentage of Ransomware Leake Site Notifications by Group During 2022



Major Highlights of LAPSUS$ Activity During 2022

companies such as NVIDIA [27], Samsung [28], and Okta [29]. The group uses social engineering and identity-focused tactics for initial access, such as paying employees at targeted organizations for credentials, purchasing credentials and session tokens, searching open-source repositories for cleartext credentials, or deploying the Redline password stealer to obtain credentials and session tokens [30].

Conti's Political Stand Led to Dissolution of the Group

The Conti ransomware group's dissolution and reorganization shows the malleable nature of the cybercriminal ecosystem. Russia's February 2022 invasion of Ukraine led the ransomware group Conti to announce their support for the Russian government on their data leak site. The group quickly retracted their initial statement [31], but within weeks a Twitter account with the handle '@ContiLeaks' began leaking internal Conti communications publicly, citing Conti's alignment with Moscow as the motivation for the leaks. [32] The leaks caused irreparable harm to the Conti brand and ultimately led to its dissolution in its contemporary form. [33] The end of the Conti brand has not led to the end of Conti members. Smaller criminal groups like Black Basta [34] and Quantum [35] have been active since the initial leak and some of their members have been linked to Conti. On the 27th of February two more ransomware gangs, LockBit and ALPHV, took to social media to pledge their neutrality in the current war between Russia and Ukraine. [36], [37]

TrickBot Group Aligns its Targets with Russian Interests

The TrickBot Group, known for their banking trojans and data theft campaigns, was spotted deploying various ransomware families such as Conti, Ryuk and Diavol against targets in Ukraine. This is a deviation from their modus operandi as they never targeted Ukrainian organizations before the Russian invasion of February 2022. [38]

The internal Conti chats leaked by '@ContiLeaks' showed evidence of FSB cooperation with members of the TrickBot Group, which would explain the covert alignment of TrickBot targets with Russian national

interests. [39]

Number of Distributed Information Stealers Indicates a Thriving Market for Stolen Credentials

Stolen credentials have been a major tool for criminal groups to gain initial access, move laterally and escalate privileges within a network throughout 2022. [40] Major criminal groups like LAPSUS$ leveraged stolen credentials and credentials stealers to gain initial access into a network, leading to data exfiltration and extortion. EclecticIQ analysts observed mass distribution of information stealers in 2022. The impact of an information stealer infection can be huge compared to the cost of operating them. Modern day information stealers have the capability to steal credentials and session tokens, information easily deployed in further attacks to gain initial access into an organization's network. [30]

Criminal Groups Will Ramp up Data Exfiltration and Extortion in 2023

Extortion tactics used by cybercriminal groups will likely increase during 2023 with pure extortion playing a more predominant role in the criminal threat landscape than in 2022. Ransomware operators will continue to add non-encryption-based functionality to their toolsets to focus on data exfiltration, extortion, and leak sites to maximize potential brand damage against their victims. Large organizations are improving their ability to respond to data encryption, maintain robust backups and reduce the impact data encryption has on the organization and their willingness to pay a ransom. Ransomware groups have noticed this and shifted their focused from encryption to developing new extortion capabilities for maximum reputational damage to the victim, like adding triple-extortion capabilities [22] and search functionality to their leak site [23].

Criminal Groups will Almost Certainly Widely Distribute Information Stealers to Steal Credentials

Stolen credentials will remain a major tool for criminal groups to gain initial access, move laterally, and escalate privileges within a network throughout 2023. Information stealers are low cost, simple to use, and there are a wide range of available stealers on the criminal MaaS (Malware-as-a-Service) market. [41] The low cost of operation, and the large impact they provide makes information stealers a continued viable tool for criminal actors moving forward.

III: The Cybersecurity Industry: Gradual, Steady Progress for the Cybersecurity Industry in 2022

Instead of 2022 seeing a seminal event fundamentally altering the nature of cybersecurity, what 2022 brought was a series of incremental changes in how the cybersecurity industry operates and the way cyber issues impact daily life. In this section, the Intelligence and Research team looks at a few of these gradual but valuable changes from the past year and offers a few thoughts on how the cybersecurity industry may change even more next year.

Government Attention and Resourcing for Cybersecurity Issues Grew

Perhaps the most welcome development in 2022 was the increase in the amount and type of government attention paid to cybersecurity issues. Especially across Europe, the UK and the US, governments took

decisive action adapting bureaucracies to better deal with the challenges of digital living. Governments around the world continued to devote time and resources to making cybersecurity an enduring effort.

In September, the European Commission proposed the Cyber Resilience Act, which intends to reduce the overall likelihood of a breach and increase the ability to swiftly recover from unforeseen circumstances among critical sectors (transport, energy, health and finance). In addition to this, the European Council and Parliament in May agreed to the provisions for the new NIS2 (network and information systems) directive to replace its predecessor, the NIS. This new directive results in a new elevated baseline for cybersecurity risk management measures, and the obligations of cyber incident reporting that fall on organizations and sectors. [42]

In the US, the year began with a significant increase in cybersecurity funding earmarked in the annual budget for organizations already focused on cyber. [43] Soon thereafter, the State Department announced it would establish the Bureau of Cyberspace and Digital Policy, signaling that cyber issues are here to stay as a State Department interest area. [44] Later in the year, US authorities hosted the second International Counter Ransomware Initiative Summit, which included participation from thirty-six countries, the European Union, and several industry partners. Some of the commitments from the summit involve further international coordination and information sharing against cybercrime, and a supporting engagement with the private sector. [45]

Authorities Leveraged New Methods to Disrupt Threat Actors

A number of governments this year used creative new methods to disrupt cybercriminal threat actors. which is something EclecticIQ analysts would like to see continue. In one example, German authorities actioned a takedown against Hydra, a large darknet platform, seizing $25 million dollars' worth of Bitcoin. [46] In several other cases, national authorities leveraged new methods to retrieve cryptocurrency assets which had been used to pay cyberattack ransoms and seized domains which were used in spoofing attacks to swindle users out of money. [47], [48] EclecticIQ analysts assess governments which invest now in developing cyber and cryptocurrency related expertise will have the most success against new cyberattack techniques in 2023 and beyond.

Highlight on the Netherlands' Effort to Enhance Intra-Governmental Cooperation

As a Dutch company, EclecticIQ is particularly interested in how the Netherlands approaches cybersecurity. The Dutch have long been industry minded and innovative, and this year continued that trend. In September, the Netherlands announced an agreement to integrate the National Cybersecurity Center, Digital Trust Center, and CSIRT-DSP into a single center of information sharing. This shifts these organizations away from their previous orientation of focusing on a specific industry sector. To combat the constantly changing threat landscape and assist victims to cyber-attacks, this newly adapted integration of three organizations will now be accessible to all Dutch organizations, regardless of industry sector. By doing this, the Netherlands pivoted one step closer in elevating national cyber-resilience. For nations that have not already planned to take steps to increase their cyber resilience, following suit with the Netherlands would be beneficial as it conveys the message of a united global front against cyber adversaries. [49]

2023: Taking Action to Increase Odds of Long-Term Cyber Resilience

There is seemingly endless potential and room for growth in cybersecurity. The Intelligence and Research team identified two areas which deserve extra focus

in 2023. Rather than get too theoretical, these two suggestions are initiatives that can and should be implemented in 2023 to support long term national or organizational cyber security and resiliency.

Businesses: Elevate cybersecurity—It Needs a Seat at the C-Suite Table

While many the world's leading enterprises have adopted monumental change to integrate cybersecurity into strategic business processes over the last decade, there's work to be done in the global business community to acknowledge the reality of cyber threats and shift from reactive to proactive processes. Businesses of all sizes and across all industries—not only large organizations or tech companies—must adopt the mindset that cyber defense is a critical business need. The best positioned organizations will be those devoting time and money to establish robust cybersecurity teams before security events occur, and not after.

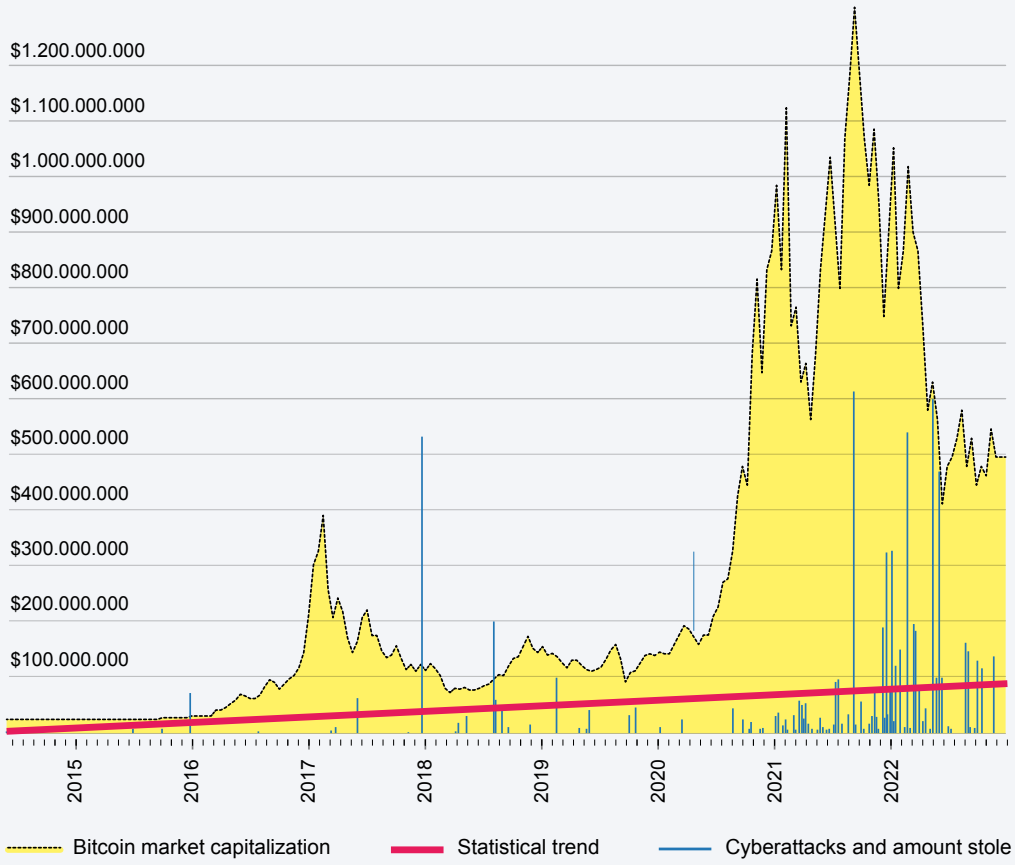
Emphasize Basic Cybersecurity Education at All Levels

Basic cybersecurity education is another area that deserves generous investment in 2023—and not just a quick anti-phishing tutorial. There is a glaring need for early and continued cyber literacy education for school-aged students, especially those who eventually choose non-cyber work. Just as financial literacy is increasingly taught in schools and drivers' education has long been a requirement for all students, so should children be taught the potential power and danger of the devices they use. Big tech companies have a role to play here by being more forthcoming about privacy considerations and potential negative effects of their products on young minds, so that cybersecurity curricula can be as relevant as possible.

IV: Cryptocurrency: 2022 Juxtaposed Increasing Cyberattack Activity in Decentralized Finance with Decreasing Market Capitalization

Increasing Defi Market Capitalization Since 2020 Created New Opportunities for Threat Actors

Despite the recent upheaval of the decentralized finance market space, EclecticIQ analysts assess cryptocurrency is likely to continue growing its role in global finance. As observed in the graphic below, there is a significant spike in the value and frequency of attacks concerning cryptocurrency as the overall market cap exceeded $1 trillion. A major outlier is Coincheck at $532 million (January 2018). Peak cryptocurrency value coincided with the highest valued DeFi attack to date. Prior to the end of 2020 and the start of 2021, there were seldom any cyberattacks valued at over $50 million, but once cryptocurrency hit the $1 trillion mark on 7 January 2021, the frequency and worth of these attacks rose significantly, including a notable increase in large attacks over $100 million at the end of 2021. Since the total market cap of cryptocurrency fell below the $1 trillion mark on 12th June 2022, the frequency and upper bound extent of funds lost to DeFi attacks has followed suit. While DeFi attacks during the last half of 2022 incurred a higher average loss than ever before at $79 million, the frequency of attacks valued at over $1 million for a 5-month period during cryptocurrency's peak has decreased 30% until now.



The graphic left shows large (over $1 million) DeFi cyberattacks are producing increasingly erratic losses and becoming more frequent. The increasingly erratic cyberattacks cluster occurred during the same 2021-2022 period as cryptocurrency peak market value. The non-normal distribution is indicative of growing instability of the system, suggesting that cyberattack risk is creating pressure on DeFi systems. $2 billion was lost due to large cyberattacks on decentralized finance platforms during peak market capitalization. Between the months of September 2021 and September 2022, cryptocurrency reached its highest market capitalization at just under $3 trillion.

Many cryptocurrency reports during the first half of the year centered around high-value thefts. The primary TTPs successfully leveraged by threat actors in major DeFi cyberattacks [50]–[52] include smart contract exploitation, flash loans, and compromise of critical systems. Large scale fraud like rug-pulls are giving way to increased social engineering targeting individuals. A comparison of cryptocurrency cyberattack data from April 2022 with current data shows cyberattack risk is not improving and previously forecasted trends continue to afflict this newer vertical. [53], [54]

More frequent and increasing average losses from large cyberattacks:

- 2014 - 2020: 30 attacks valued at over $1 million.
- 2020 - 2023: 114 attacks valued at over $1 million (an increase of 380%).
- 2014 - 2021: $40 million average cost of large cyberattacks. (Without the Coincheck outlier the average falls to $26 million.)
- 2021 - 2022: $59 million average cost of large cyberattacks.
- Mid-June 2022 – Late 2022: $80 million average cost of large cyberattacks.

Governments Are Introducing Regulation and Oversight to Cryptocurrencies at the National Level

Regulators will almost certainly seek to normalize or create designated cryptocurrencies alongside traditional fiat currencies with an eye to reduce risk to users, disrupt illicit funding streams, and benefit from taxation [55]. EclecticIQ analysts expect further government regulation push in the wake of FTX's collapse and the secondary market aftershocks resulting indirectly from improperly exposed cryptocurrency assets.

El Salvador Adopted Bitcoin into its National Financial Network in 2021. [56]–[58] Other governments also show interest and will take different paths toward normalizing decentralized finance. [59], [60] Regulation is very likely to center around identity validation and will come at the cost of reduced privacy. Oversight will spark increasing law enforcement cyber operations to protect new cryptocurrency assets.

Coordinated Law Enforcement Operations Increased in The Last Two Years Against Defi Cyberattacks

Major DeFi fraud has been the initial area of focus for coordinated law enforcement efforts. Government regulation will almost certainly support further guidance for law enforcement operations against more types of cyberattacks. EclecticIQ analysts expect continued organized law enforcement operations in DeFi will expand to include cross-border support and target larger threat actor groups and crime rings. Expanding focus is likely to have a top-down deterrent effect, reaching the individual level.

Recent examples of law enforcement efforts to counter large-scale fraud:

- The 2016 Bitfinex cyberattack. [61]
- DeFi organizations are accused of catering to laundering operations that include Tornado Cash. [62]
- Individual threat actors are accused of laundering tens to hundreds of millions of dollars. [63],[64],[65]

The Unregulated, Non-Standardized Nature of the Current DeFi Ecosystem is an Advantage for Malicious Actors

Increased government oversight will likely increase security standardization, such as more stringent checks on code practices and requirements of DeFi systems which have previously proven exploits for threat actors. Regulation aimed at smart contract code will have the largest impact to reduce cyberattacks. [54] Legitimizing

national forms of cryptocurrency will attract additional cyberattack activity, as threat actors seek to maximize profit across multiple target types and cryptocurrencies become more widely available and interoperable. For example, innovative malware has been observed organizing command and control connections inside of blockchains. [66] Further novel efforts mixing malware and cryptocurrency are inevitable.

Critical System Compromise Exposing Keys and Targeted Attacks Against High-Value Individuals Will Remain the Most Challenging Attacks to Mitigate

Smart contract and flash loan vulnerabilities still featuring prominently in major cyberattacks can each be mitigated through more rigorous and accountable code review. Current tooling provides the means to do this. A large portion of the remaining attacks are caused by access to cryptographic keys in validation systems. Cyberattacks exposing private keys in critical systems will remain very high risk; both because skilled threat actors are very likely to continue to deploy resources for the high reward provided, and because the growth of individual and critical systems will provide a growing target.

Asymmetric Cryptocurrency Adoption and Risk Will Likely Lead to Uneven Global Infrastructure Consolidation

EclecticIQ analysts assess end-users in less stable economies will be more vulnerable to losses from cyberattacks compared to end-users in wealthier countries who are relatively more financially insulated. Countries with higher relative wealth, like the US, are financially better insulated to cyberattacks and high rate of DeFi project adoption allows DeFi institutions there to mature faster, which should make them less risky for users. [67] As more countries host official or unofficial cryptocurrency, the risk to end-users and DeFi organizations in economically vulnerable countries and countries with high corruption rates will be highest. Together, the likely impact is asymmetric global cryptocurrency growth. Wealthier countries adopting DeFi sooner will more likely attract talent to advance and grow their organizations faster and sooner than others, if they can maintain financial stability. Infrastructure will change unevenly leading to uneven leverage for related cyber policy. It is unclear what, if any, effect this will have on end-user adoption globally.

V: The Russia-Ukraine War: Cyber Operations had Limited Effects

Pre-War Russian Cyber Operations Did Not Deliver Key Anticipated Strategic Advantages to Russia

The escalation of the Russia-Ukraine conflict into a war demonstrates that Russia's cyber warfare efforts against Ukraine failed to deliver upon strategic objectives - to undermine confidence in Ukraine leaders, and to make Ukraine abandon its rapprochement with the West - with the anticipated result of making the Ukrainian population more malleable and prone to capitulation to Russian threats.

Since at least 2014, Russia conducted cyber operations against Ukrainian entities for the purposes of disruption, intimidation and distribution of Russian narratives. [68]–[70] Weeks before the invasion, on the day of invasion and in the months after, Moscow executed seemingly

standalone cyber operations to disrupt public life, trigger economic disturbance, and undermine confidence in Ukrainian leadership. [71] Cyber operations involved Denial of Service attacks on Ukrainian government and civilian websites [72],[73] deployment of disruptive malware [74], and espionage campaigns. [75], [76] Other tactics include information campaigns on social media and messaging services to distribute narratives and false information to demoralize Ukrainians, sow division between Ukraine and its allies, and strengthen support for Russia among Ukrainians, European political parties, and Russian minorities in former Soviet Union states. These cyber operations did not deliver the primary anticipated strategic value: Ukraine did not stop its rapprochement to the West, so Russia invaded Ukraine on February 24th, escalating to military force attempting to prevent the country from joining a Western alliance.

Anticipated Effects of Cyber Operations Complementing Military Objectives Did Not Materialize...

EclecticIQ analysts assess the effects of cyber operations during the war provided few, if any, tactical advantages for Russian military forces. While Russian forces attacked Ukraine by land, air, and sea, Russian cyber actors conducted operations to:

1. damage systems and services of institutions in Ukraine [77]
2. hinder civilians' ability to access information and critical life services
3. undermine confidence in the country's leadership [78]

OSINT reporting shows a correlation between kinetic and cyber actions – both in geography of targets and timing of attack. [75] Analysts cannot determine if this correlation was due to coordinated efforts between Russian military and cyber units, or due to a set of shared goals. Even if coordinated, analysts determine that few, if any, operations provided significant tactical advantage in support of military objectives. If there were successful cyber-attacks intended to support of Russian military action, they failed to produce measurable effects. Despite the advancement of Russian forces and continued cyber-attacks reported, Ukraine government bodies, public and private services continued to function.

...Except for the Attack Targeting ViaSat Satellite Internet

The exception is the cyberattack against satellite internet provider ViaSat that disabled 10.000 modems across Europe between 5 a.m. and 9 a.m. Kyiv time - the same time as Russian forces started in offense on Ukrainian territory. [79] Victor Zhora, a high-ranking Ukrainian cybersecurity official later called the attack "a really huge loss in communications in the very beginning of war." [80]

Analysts note the lack of verifiable information about successful cyberattacks during the war complicates the picture. It is likely Ukraine would not publicly release the full extent of the impacts of Russian cyber operations or sophisticated correlation with Russian kinetic strikes. A disclosure would give Russia insight into the efficacy of their cyber operations and in turn may alter its war planning. It is also likely Moscow seeks to obscure the true number and purpose of its cyberattack plans, keeping hidden reports which either failed or which had more surreptitious missions such as espionage or sabotage.

Kinetic Over Cyber Attacks - Strengthened Western Support Has Hardened Ukraine Cyber Defenses

EclecticIQ analysts assess Russia will almost certainly continue using kinetic actions as primary means to achieve its objectives as the war drags into 2023. Considering that Russian cyber operations do not seem to be systematically integrated into its military campaigns and did not provide substantial strategic or tactical value, they will likely play a secondary role in

the war. The intensified kinetic strikes against critical infrastructure targets in Ukraine since October signal Russia rather relies on its kinetic capability rather than on cyber capability.

EclecticIQ analysts assess increased cyber support by Western governments [81] [82] and private organizations [83] [84] [85] significantly improved Ukraine's network defenses and its detection and response capabilities. It is plausible Russia currently lacks capabilities to execute cyber operations in Ukraine, as it may have "burned" sensitive access to Ukrainian critical infrastructure in previous attacks. Analysts cannot rule out Russian cyber actors working on new capabilities, but considering Russia's cyber operations did not provide substantial advantages in Ukraine to date, analysts have little reason to expect a sudden change in 2023.

EclecticIQ analysts assess Russia will likely continue executing information campaigns influencing Ukrainian and international audiences and will pursue network exploitation of Ukrainian and allied entities for espionage. Russia is likely trying to obtain information about planned sanctions, military and civil support by Western governments, and any other information that can be used as leverage in future negotiations. Russian espionage activities will likely target Europe´s response plan [86] to the energy crisis that, among other goals, seeks diversification by accessing new energy markets, accelerated expansion of renewable energies, and investments in energy infrastructure.

VI. Emerging Technologies: ChatGPT

ChatGPT: A Powerful but Limited Model for CTI Analysis

San Francisco-based OpenAI released ChatGPT, a prototype chatbot based on version 3.5 of the company's Generative Pre-trained Transformer (GPT-3.5) large language model, just as the year neared its close. [87] Designed to produce human-like answers to prompts, ChatGPT took technologist and security communities by storm for its enhanced accessibility and ease of use compared to previous GPT iterations. [88] EclecticIQ analysts experimented with ChatGPT and see potential – albeit currently limited – with applications in the cyber realm ranging from exploit development, malware analysis, signature development to content generation for information operations.

ChatGPT for malware analysis

ChatGPT has the potential to empower human analysts to scale their workload by speeding up simple static code and file analysis. ChatGPT is likely to help decrease the time needed to statically analyze malware samples. Early testing shows it to be effective at reading and telling a user what a piece of code or disassembly is doing, even

reproducing C code from the assembly fed into it, showing early potential in assisting reverse engineering workflows. [89]

ChatGPT for CTI analysis

GPT modeling in its current iteration will almost certainly not replace a CTI analyst or traditional tooling in most workflows. GPT is not trained on recent data or specifically trained on sufficient information security data sets to address core CTI use cases; i.e., it's unable to provide recent context or perform basic CTI workflows such as a hash lookup. The model is also unable to accurately model unstructured intelligence reporting in to structured intelligence standards such as STIX2.1 or into frameworks like MITRE ATT&CK. EclecticIQ analysts also observed ChatGPT produce factually incorrect attribution on a well-known threat actor, potentially creating a scenario were less knowledgeable analysts or people outside the industry are actioning inaccurate information.

ChatGPT for information operations campaigns

EclecticIQ analysts assess this technology may lower the barrier to entry for propaganda campaigns or information operations, particularly through enabling users to quickly scale generated content. EclecticIQ's Intelligence and Research team experimented with running hypothetical propaganda prompts through ChatGPT to understand the model's full potential. The propaganda content examples generated faced several limitations.

First, they are generated from trained data derived from Western, English-speaking sources, which limit ingenuity in the model's capabilities. Second, they depend on directives providing specific strategic or operational objectives derived from the threat actor's strategy. This means the content must already be largely devised by the human originator and the model's contribution is primarily generating the "fat" around a propaganda message rather than devising doctrinally cogent information operations lines of effort. Finally, while the model can produce content in multiple languages, it is not yet developed enough to produce non-English language content sophisticated enough to compete with nuanced target audience analysis conducted by nation-state professional information operations personnel.

Despite limitations, ChatGPT and other GPT-derived applications present significant disruptive potential in 2023 and served as an exciting technological close to 2022. EclecticIQ analysts expect further development and training of GPT and similar applications to present enormous creative challenges in 2023, not only for cybersecurity defenders and analysts but for the global professional workforce. For example, did you notice the title for this subheading was generated with ChatGPT?

References:

[1] "Microsoft and others orchestrate takedown of TrickBot botnet," ZDNET. https://www.zdnet.com/article/microsoft-and-other-tech-companies-orchestrate-takedown-of-trickbot-botnet/ (accessed Dec. 01, 2022).

[2] "Joint standing operation against cyber criminal syndicates," Our ministers – Attorney-General's portfolio. https://ministers.ag.gov.au/media-centre/joint-standing-operation-against-cyber-criminal-syndicates-12-11-2022 (accessed Dec. 01, 2022).

[3] "Researchers Quietly Cracked Zeppelin Ransomware Keys – Krebs on Security." https://krebsonsecurity.com/2022/11/researchers-quietly-cracked-zeppelin-ransomware-keys/ (accessed Dec. 01, 2022).

[4] ESET Threat Report T 1 2022," WeLiveSecurity, Jun. 02, 2022. https://www.welivesecurity.com/2022/06/02/eset-threat-report-t12022/ (accessed Dec. 01, 2022).

[5] J. V. C. Writer, D. R. July 28, and 2022, "In a Post-Macro World, Container Files Emerge as Malware-Delivery Replacement," Dark Reading, Jul. 28, 2022. https://www.darkreading.com/endpoint/post-macro-world-container-files-distribute-malware-replacement (accessed Dec. 01, 2022).

[6] "Suspected AsyncRAT Delivered via ISO Files Using HTML Smuggling...," eSentire. https://www.esentire.com/blog/suspected-asyncrat-delivered-via-iso-files-using-html-smuggling-technique (accessed Dec. 01, 2022).

[7] N. E. C. Writer, D. R. May 27, and 2022, "ChromeLoader Malware Hijacks Browsers With ISO Files," Dark Reading, May 27, 2022. https://www.darkreading.com/application-security/chromeloader-malware-hijacks-browsers-iso-files (accessed Dec. 01, 2022).

[8] "Politie stopt internationaal verspreiding FluBot malware." https://www.politie.nl/nieuws/2022/juni/1/02-politie-stopt-internationaal-verspreiding-flubot-malware.html (accessed Dec. 01, 2022).

[9] "Avast Threat Labs releases Q3 2022 Threat Report." https://blog.avast.com/q3-2022-threat-report (accessed Dec. 07, 2022).

[10] "Russian zero-day firm offers $1,5m for a Signal RCE exploit," Cybernews, Nov. 22, 2022. https://cybernews.com/news/russian-zero-day-firm-offers-15m-for-a-signal-rce-exploit/ (accessed Dec. 01, 2022).

[11] N. NAME, "Mobile app statistics to keep an eye on in 2022," Cybersecurity ASEE, May 05, 2022. https://cybersecurity.asee.co/blog/mobile-app-statistics-to-keep-an-eye-on/ (accessed Dec. 02, 2022).

[12] "Global mobile traffic 2022," Statista. https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/ (accessed Dec. 01, 2022).

[13] "Scammers Created an AI Hologram of Me to Scam Unsuspecting Projects," Binance Blog. https://www.binance.com/en/blog/community/scammers-created-an-ai-hologram-of-me-to-scam-unsuspecting-projects-6406050849026267209 (accessed Dec. 01, 2022).

[14] "Elon Musk deep fakes promote new BitVex cryptocurrency scam," BleepingComputer. https://www.bleepingcomputer.com/news/security/elon-musk-deep-fakes-promote-new-bitvex-cryptocurrency-scam/ (accessed Dec. 07, 2022).

[15] R. DePompa and D. Molina, "Swapped Out: Hackers target social media users with high-tech fake videos," https://www.wsaz.com. https://www.wsaz.com/2022/05/16/swapped-out-hackers-target-social-media-users-with-high-tech-fake-videos/ (accessed Dec. 01, 2022).

[16] "Norton finds deepfakes and crypto scams rising in Australia," SecurityBrief Australia. https://securitybrief.com.au/story/norton-finds-deepfakes-and-crypto-scams-rising-in-australia (accessed Dec. 01, 2022).

[17] "Instagram account taken over by imposter who posted deepfake video of Tampa man," NewsBreak. https://www.wfla.com/8-on-your-side/better-call-behnken/instagram-account-taken-over-by-imposter-who-posted-deepfake-video-of-tampa-man/ (accessed Dec. 02, 2022).

[18] "Increasing Threat of Deepfake Identities." https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf (accessed Dec. 01, 2022).

[19] J. Pearson and N. Zinets, "Deepfake footage purports to show Ukrainian president capitulating," Reuters, Mar. 17, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/

[20] "XLSM Malware with MacroSheets | McAfee Blog XLSM Malware with MacroSheets," McAfee Blog, Aug. 06, 2021. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/xlsm-malware-with-macrosheets/ (accessed Dec. 01, 2022).

[21] DHB-MSFT, "Macros from the internet are blocked by default in Office - Deploy Office." https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (accessed Dec. 01, 2022).

[22] "LockBit ransomware gang gets aggressive with triple-extortion tactic," BleepingComputer. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/ (accessed Dec. 01, 2022).

[23] "ALPHV's ransomware makes it easy to search data from targets who do not pay," TechRepublic, Jul. 07, 2022. https://www.techrepublic.com/article/alphv-ransomware-search-data/ (accessed Dec. 01, 2022).

[24] V. Navali, "LAPSUS$ Data Breach Against Several High-Profile Victims," SentinelOne, Mar. 28, 2022. https://www.sentinelone.com/blog/lapsus-data-breach/ (accessed Dec. 01, 2022).

[25] E. Naone, "Threat Assessment: Luna Moth Callback Phishing Campaign," Unit 42, Nov. 21, 2022. https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/ (accessed Dec. 01, 2022).

[26] "Karakurt Data Extortion Group | CISA." https://www.cisa.gov/uscert/ncas/alerts/aa22-152a (accessed Dec. 01, 2022).

[27] "Hackers to NVIDIA: Remove mining cap or we leak hardware data," BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-to-nvidia-remove-mining-cap-or-we-leak-hardware-data/ (accessed Dec. 01, 2022).

[28] "Hackers leak 190GB of alleged Samsung data, source code," BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/ (accessed Dec. 01, 2022).

[29] "Okta Says Security Breach by Lapsus$ Hackers Impacted Only Two of Its Customers," The Hacker News. https://thehackernews.com/2022/04/okta-says-security-breach-by-lapsus.html (accessed Dec. 01, 2022).

[30] K. McCafferty, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction," Microsoft Security Blog, Mar. 22, 2022. https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/ (accessed Dec. 01, 2022).

[31] "Conti ransomware gang backs Russia, threatens US," SearchSecurity. https://www.techtarget.com/searchsecurity/news/252513982/Conti-ransomware-gang-backs-Russia-threatens-US (accessed Dec. 01, 2022).

[32] "(2) conti leaks (@ContiLeaks) / Twitter," Twitter. https://twitter.com/ContiLeaks (accessed Dec. 01, 2022).

[33] AdvIntel, "DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape," AdvIntel, May 20, 2022. https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape (accessed Dec. 01, 2022).

[34] J. Miller-Osborn, "Threat Assessment: Black Basta Ransomware," Unit 42, Aug. 25, 2022. https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/ (accessed Dec. 01, 2022).

[35] Vitali Kremez [@VK_Intel], "Gift for the community: Post-#Conti #ransomware operation mindmap world. Enjoy! https://t.co/yw3CU4Qikc," Twitter, Aug. 09, 2022. https://twitter.com/VK_Intel/status/1557003350541242369 (accessed Dec. 01, 2022).

[36] Dmitry Smilyanets [@ddd1ms], "#ALPHV #ransomware: 'We are extremely saddened by what is happening. In our business, there are no nationalities, fictional borders, or any other reason why people can kill people…' https://t.co/bRDetLLKbx," Twitter, Feb. 28, 2022. https://twitter.com/ddd1ms/status/1498374586509180928 (accessed Dec. 07, 2022).

[37] Lawrence Abrams [@LawrenceAbrams], "LockBit ransomware gang releases statement that they will not take sides in Russia's invasion of Ukraine. 'For us it is just business and we are all apolitical. We are only interested in money for our harmless and useful work.' https://t.co/WAOqVTC8Zw," Twitter, Feb. 27, 2022. https://twitter.com/LawrenceAbrams/status/1498015863370358791 (accessed Dec. 07, 2022).

[38] "Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine," Security Intelligence, Jul. 07, 2022. https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/ (accessed Dec. 07, 2022).

[39] "Conti Group - Tooling, Leaks and Russian FSB Ties - Cyber Security Consultants - Alchemy." https://www.alchemysec.com.au/conti-group-tooling-leaks-and-russian-fsb-ties/ (accessed Dec. 07, 2022).

[40] Recorded Future, "Initial Access Brokers Are Key to Rise in Ransomware Attacks." Aug. 02, 2022. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

[41] M. Labs, "Infostealer Comparison: Top Stealers in 2022." https://blog.morphisec.com/infostealer-comparison (accessed Dec. 01, 2022).

[42] Cybersecurity: how the EU tackles cyber threats." https://www.consilium.europa.eu/en/policies/cybersecurity/ (accessed Dec. 01, 2022).

[43] T. Starks, "Biden budget requests big increase for cybersecurity," CyberScoop, Mar. 28, 2022. https://www.cyberscoop.com/biden-fiscal-2023-budget-request-civilian-agencies-cybersecurity/ (accessed Dec. 01, 2022).

[44] J. Warminsky, "State Department's cyber bureau begins operations," CyberScoop, Apr. 04, 2022. https://www.cyberscoop.com/state-departments-cyber-bureau-begins-operations/ (accessed Dec. 01, 2022).

[45] T. W. House, "FACT SHEET: The Second International Counter Ransomware Initiative Summit," The White House, Nov. 01, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/ (accessed Dec. 01, 2022).

[46] "Germany takes down Hydra, world's largest darknet market," BleepingComputer. https://www.bleepingcomputer.com/news/legal/germany-takes-down-hydra-worlds-largest-darknet-market/ (accessed Dec. 01, 2022).

[47] "Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency 'Pig Butchering' Scheme," Nov. 21, 2022. https://www.justice.gov/usao-edva/pr/court-authorizes-seizure-domains-used-furtherance-cryptocurrency-pig-butchering-scheme (accessed Dec. 01, 2022).

[48] "Nederlandse gedupeerden geholpen in unieke ransomware-actie." https://www.politie.nl/nieuws/2022/oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html (accessed Dec. 01, 2022).

[49] N. C. S. Centrum, "Nationale cybersecurity organisaties gaan krachten bundelen - Nieuwsbericht - Nationaal Cyber Security Centrum," Sep. 07, 2022. https://www.ncsc.nl/actueel/nieuws/2022/september/7/nationale-cybersecurity-organisaties-gaan-krachten-bundelen (accessed Dec. 01, 2022).

[50] R. R. October 12 and 2022, "Everything We Know About the Mango Markets Hack." https://www.bankinfosecurity.com/everything-we-know-about-mango-markets-hack-a-20250 (accessed Dec. 01, 2022).

[51] R. Behnke, "Explained: The Wintermute Hack (September 2022)," halborn, Sep. 26, 2022. https://halborn.com/explained-the-wintermute-hack-september-2022/ (accessed Dec. 01, 2022).

[52] "Bad Code Update Lets Hackers Steal $190M From Cryptocurrency Bridge Nomad |." https://www.spiceworks.com/it-security/security-general/news/nomad-bridge-crypto-heist/ (accessed Dec. 01, 2022).

[53] "Attack Patterns Produce Growing Losses Targeting Mutual Vulnerabilities Endemic to Decentralized Finance." https://blog.eclecticiq.com/attack-patterns-produce-growing-losses-targeting-mutual-vulnerabilities-endemic-to-decentralized-finance (accessed Dec. 01, 2022).

[54] T. Tsihitas, "The Biggest Cryptocurrency Heists of All Time," Comparitech, Jun. 28, 2019. https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/ (accessed Dec. 01, 2022).

[55] [55] T. W. House, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets," The White House, Sep. 16, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ (accessed Dec. 01, 2022).

[56] J. Hernandez, "El Salvador Just Became The First Country To Accept Bitcoin As Legal Tender," NPR, Sep. 07, 2021. Accessed: Dec. 01, 2022. [Online]. Available: https://www.npr.org/2021/09/07/1034838909/bitcoin-el-salvador-legal-tender-official-currency-cryptocurrency

[57] N. Renteria and A. Esposito, "El Salvador's world-first adoption of bitcoin endures bumpy first day," Reuters, Sep. 08, 2021. Accessed: Dec. 01, 2022. [Online]. Available: https://www.reuters.com/business/finance/el-salvador-leads-world-into-cryptocurrency-bitcoin-legal-tender-2021-09-07/

[58] "IMF urges El Salvador to remove Bitcoin as legal tender," BBC News, Jan. 26, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.bbc.com/news/world-latin-america-60135552

[59] "White House Is Set to Put Itself at Center of U.S. Crypto Policy," Bloomberg.com, Jan. 21, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.bloomberg.com/news/articles/2022-01-21/white-house-is-set-to-put-itself-at-center-of-u-s-crypto-policy

[60] Reuters, "South Africa moves to regulate crypto assets," Reuters, Oct. 20, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.reuters.com/technology/south-africa-moves-regulate-crypto-assets-2022-10-19/

[61] "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," Feb. 08, 2022. https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (accessed Dec. 01, 2022).

[62] "Tornado Cash Token Tumbles After Developer Arrest," Bloomberg.com, Aug. 12, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.bloomberg.com/news/articles/2022-08-12/tornado-cash-cryptocurrency-torn-tumbles-after-developer-arrest

[63] "Man verdacht witwassen tientallen miljoenen euro's aan cryptovaluta [English below]." https://www.politie.nl/nieuws/2022/september/13/03-man-opgepakt-witwassen-cryptovaluta.html (accessed Dec. 01, 2022).

[64] "Arrest Made in $46 Million Dollar Cryptocurrency Theft." https://webcache.googleusercontent.com/search?q=cache:K15Q_kNh0UAJ:https://hamiltonpolice.on.ca/news/arrest-made-in-46-million-dollar-cryptocurrency--theft/&cd=4&hl=en&ct=clnk&gl=de (accessed Dec. 02, 2022).

[65] "Estonian duo accused of $575m cryptocurrency scam," BBC News, Nov. 22, 2022. Accessed: Dec. 01, 2022. [Online]. Available: https://www.bbc.com/news/world-europe-63711843

[66] "Disrupting the Glupteba operation," Google, Dec. 07, 2021. https://blog.google/threat-analysis-group/disrupting-glupteba-operation/ (accessed Dec. 01, 2022).

[67] G. M. Caporale, W.-Y. Kang, F. Spagnolo, and N. Spagnolo, "Cyber-Attacks and Cryptocurrencies," CESifo Working Paper, Working Paper 8124, 2020. Accessed: Dec. 01, 2022. [Online]. Available: https://www.econstor.eu/handle/10419/216520

[68] "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," WeLiveSecurity, Jan. 02, 2016. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/ (accessed Nov. 29, 2022).

[69] E. Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," Washington Post, Jan. 13, 2018. Accessed: Nov. 28, 2022. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

[70] "Industroyer echoes Stuxnet in its threat to critical infrastructure," Industroyer echoes Stuxnet in its threat to critical infrastructure. https://www.eset.com/int/industroyer/ (accessed Nov. 29, 2022).

[71] "The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine," Mandiant. https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine (accessed Nov. 17, 2022).

[72] "UK assesses Russian involvement in cyber attacks on Ukraine," GOV.UK. https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine (accessed Nov. 08, 2022).

[73] "Ukraine: DDoS attacks on govt sites originated from Russia," BleepingComputer. https://www.bleepingcomputer.com/news/security/ukraine-ddos-attacks-on-govt-sites-originated-from-russia/ (accessed Dec. 01, 2022).

[74] "Technical Analysis of the WhisperGate Malicious Bootloader | CrowdStrike," crowdstrike.com, Jan. 19, 2022. https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/ (accessed Nov. 22, 2022).

[75] Microsoft, "Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine," Apr. 2022, [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[76] "IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine," WeLiveSecurity, Mar. 01, 2022. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/ (accessed Mar. 15, 2022).

[77] "An update on the threat landscape," Google, Mar. 07, 2022. https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ (accessed Nov. 08, 2022).

[78] "The deepfakes in the disinformation war – DW – 03/18/2022," dw.com. https://www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433 (accessed Nov. 23, 2022).

[79] L. Mathews, "Viasat Reveals How Russian Hackers Knocked Thousands Of Ukrainians Offline," Forbes. https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/ (accessed Nov. 23, 2022).

[80] R. Satter, "Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official," Reuters, Mar. 15, 2022. Accessed: Nov. 08, 2022. [Online]. Available: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

[81] "U.S. Support for Connectivity and Cybersecurity in Ukraine," United States Department of State. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/ (accessed Nov. 29, 2022).

[82] "UK boosts Ukraine's cyber defences with £6 million support package," GOV.UK. https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package (accessed Nov. 29, 2022).

[83] "Defending Ukraine: Early Lessons from the Cyber War," Microsoft On the Issues, Jun. 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (accessed Nov. 29, 2022).

[84] "Helping Ukraine," Google, Mar. 04, 2022. https://blog.google/inside-google/company-announcements/helping-ukraine/ (accessed Nov. 29, 2022).

[85] "Cisco joins long list of security companies supporting Ukraine," BleepingComputer. https://www.bleepingcomputer.com/news/security/cisco-joins-long-list-of-security-companies-supporting-ukraine/ (accessed Nov. 29, 2022).

[86] "EU action to address the energy crisis," European Commission - European Commission. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/eu-action-address-energy-crisis_en (accessed Nov. 29, 2022).

[87] "Artificial intelligence is permeating business at last | The Economist." https://www.economist.com/business/2022/12/06/artificial-intelligence-is-permeating-business-at-last (accessed Dec. 08, 2022).

[88] A. Johnson, "Here's What To Know About OpenAI's ChatGPT—What It's Disrupting And How To Use It," Forbes. https://www.forbes.com/sites/ariannajohnson/2022/12/07/heres-what-to-know-about-openais-chatgpt-what-its-disrupting-and-how-to-use-it/ (accessed Dec. 08, 2022).

[89] I. Kwiatkowski, "Gepetto." Dec. 08, 2022. Accessed: Dec. 08, 2022. [Online]. Available: https://github.com/JusticeRage/Gepetto

EclecticIQ

Intelligence at the core

Intelligence Hunting Response

About the EclecticIQ

EclecticIQ is a global provider of threat intelligence, hunting and response technology and services.

Stay ahead of rapidly evolving threats and outmaneuver your adversaries by embedding Intelligence at the core™ of your cyberdefenses with our open and extensible cybersecurity platform and ecosystem.

The most targeted organizations in the world – including governments and large enterprises – use our platform to operationalize threat intelligence, enable threat hunting, detection and response, and accelerate collaboration.

Founded in 2014, EclecticIQ is a leading European cybersecurity vendor operating worldwide with offices and teams across Europe and UK, North America, India and via value-add partners.

Contact us at:
info@eclecticiq.com
www.eclecticiq.com