EclecticIQ

Intelligence at the core

Intelligence
Automation
Collaboration

END OF YEAR REPORT

EclecticIQ Retrospective: A Look at the Themes & Events That Shaped the 2023 Cyber Landscape

by **EclecticIQ Intelligence and Research**

www.eclecticiq.com | research@eclecticiq.com

Executive Summary

EclecticIQ's Intelligence and Research team looked back on the 2023 cyber landscape: from the evolving tactics of Chinese state-sponsored cyber operations, the increasing integration of AI tools by threat actors, the implications of hacktivism in global conflicts, and the escalation of ransomware attacks fueled by Cybercrime as a Service.

Unraveling China's APT Tactics and Edge Device Exploits in Cybersecurity

Chinese state-sponsored cyber operations focused on stealthier tactics, utilizing zero-day exploits and "living-off-the-land" techniques. Actors target cloud environments due to organizations' rapid migration, with a notable case involving forged authentication tokens for accessing user emails. These developments mark a shift in the cybersecurity landscape for the year, with emerging threats and tactics.

The Pivotal Role of AI in Reshaping Cyber Threats and Defenses

The year 2023 witnessed substantial growth in AI, highlighted by OpenAI's ChatGPT's rapid user increase and the emergence of multiple generative AI tools. These tools have been incorporated into threat actors' toolset to generate malicious content, raising significant cybersecurity and misinformation concerns. These developments indicate an evolving landscape where AI not only facilitates content creation, but also intensifies cybersecurity threats and misinformation campaigns on social media by streamlining processes and lowering the barrier to entry. Looking ahead to 2024, the AI landscape is expected to witness an arms race in cybersecurity, driven by both defenders and offenders using AI-powered tools.

Hacktivism as a Built-in Feature of Global Conflicts Has Important Implications for Non-Military Targets

Hacktivism is becoming an important and growing risk. Global conflict stimulates cybercriminal groups to collaborate in cyberattacks that support political causes. A falling distinction between military and civilian initiated cyberattacks and disruptions to non-military targets are the primary effects. Cyberattacks and hacktivist patterns observed this year orbit the Russia-Ukraine and Hamas-Israel conflicts. The most common focus of hacktivists remains information gathering and disrupting systems and services for impact to an expanding range of users and organizations.

Cybercrime-as-a-service Fueling the Escalation of Ransomware Attacks

In 2023, ransomware attacks reached peak levels due to the proliferation of Cybercrime-as-a-service (CCaaS). CCaaS enables cybercriminals to outsource various attack elements, making more complex techniques accessible to less tech-savvy individuals. Ransomware actors now prioritize assessing costs over ransom gains, targeting small enterprises, schools, and universities. Some organizations pay ransoms due to neglecting backup strategies and turn to insurance. However, paying the ransom doesn't guarantee data retrieval, highlighting the importance of robust backup and recovery strategies.

Table of Content

A Review of Predictions From Last Year

Two of last year's predictions involved new capabilities introduced by advanced machine learning algorithms, and the last involved growing ransomware extortion techniques.

- The first included a spreading threat from fake media. In 2023, EclecticIQ analysts observed this prediction materializing. Access to new software models turned into tools have allowed an expanding user base to experiment in different ways. Convincing synthetic media, sometimes labeled "deepfakes", have spread into visual and audio formats. Deepfake services continue to expand in availability. The next pertinent threat this year is generative adversarial networks, further discussed below.

- The second prediction was about ChatGPT and its potential to fundamentally disrupt 2023's technology landscape. The opportunities we mentioned in last year's prediction did materialize and ChatGPT is now used to support a variety of use cases by companies throughout the world. Its capabilities to identify patterns and trends make it particularly suitable for multiple cybersecurity applications.

- Extortion-only groups rose to a more predominant role in the criminal ecosystem, but patterns are unlikely to rise further. It is very likely extortion-only groups fail to provide enough leverage for large ransomware settlements and are not able to compete with more traditional ransomware syndicates. Analysts now observe the popularization of malware services within the ransomware ecosystem, sometimes referred to as crimeware-as-a-service. These complex services will very likely play a key role driving more ransomware operations next year.

Unraveling China's APT Tactics and Edge Device Exploits in Cybersecurity

From Zero-Day Exploits to Cloud Infiltration: China's APT Landscape in 2023

In 2023, nation-state threat actors aligned with the People's Republic of China (PRC) have demonstrated a stealthier and coordinated approach in their cyber operations. This development is highlighted by their increased use of zero-day exploits, indicating a notable shift to more stealthy tactics compared to previous years. [1] Chinese advanced persistent threat (APT) groups include APT27, RedHotel, UNC4841 and Mustang Panda, actively targeting Europe, the United States and East Asian countries to conduct global cyber espionage in line with economic and national security interests of PRC.[2]

CVE ID	Software
CVE-2023-22515	Atlassian Confluence
CVE-2023-20867	Vmware ESXi
CVE-2023-2868	Barracude ESG
CVE-2023-3519	Citrix Netscaler

Figure 1 - Zero-day vulnerabilities exploited by suspected Chinese state-sponsored groups in 2023

EclecticIQ researchers observed a rise in the exploitation of zero-day vulnerabilities in the wild, as well as an increased use of "living-off-the-land" techniques by Chinese APT clusters to evade detection.

Figure 1 shows a usage of zero-day vulnerabilities exploited by groups believed to be state-sponsored by China in 2023.

We assess with high confidence that Chinese state-sponsored cyber operations will very likely continue exploiting known or unknown vulnerabilities in externally facing web servers and network devices to get initial access from victim devices and try to stay undetected.

Since the organizations rapidly move their infrastructure to cloud environments, the cyber operations of APT groups aligned with the Chinese government have their focus on cloud targets. This shift is evidenced by activities like STORM-0558, which involved the use of forged authentication tokens for accessing user emails through a stolen Azure AD (now Entra ID) enterprise signing key. Such tactics are becoming the norm, with cloud environments emerging as primary targets for these groups. [3]

The Silent Threat: How Edge Devices are Exploited in Stealthy Cyber Operations

Devices located at the boundary of an enterprise network, known as edge devices, connect directly to the internet. This external exposure makes them attractive targets for a variety of threat actors. If these actors exploit a zero-day vulnerability in such devices,

they gain significant advantages in terms of ease and success of their attacks, as well as maintaining stealth during malicious operation. Executed malware on these internet-connected devices can facilitate lateral movement within the network and establish command and control channels by reverse tunneling, allowing for data exfiltration and the execution of remote commands.

Monitoring these edge devices poses substantial security challenges. Often, they are incompatible with endpoint detection and response (EDR) solutions or methods for detecting unauthorized changes and gathering forensic evidence. This gap in monitoring capabilities decreases the chances of identifying an active breach and complicates the process of attributing cyberattacks.

In 2023, Ransomware groups like Lockbit have shown a particular interest in targeting edge devices, especially those related to security, networking, and virtualization technologies. Since ransomware gangs focus on financial gain, they were using mass exploitation techniques to infect as many targets as possible across multiple sectors and using commercial remote access software like Atera to gain persistence access. [4]

Since edge device vulnerabilities help threat actors to stay undetected during their cyber operations and give

CVE	Vulnerabilty Name	Short Description
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway contain a buffer overflow vulnerability that allows for sensitive information disclosure when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server.
CVE-2023-20109	Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability	Cisco IOS and IOS XE contain an out-of-bounds write vulnerability in the Group Encrypted Transport VPN (GET VPN) feature that could allow an authenticated, remote attacker who has administrative control of either a group member or a key server to execute malicious code or cause a device to crash.
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN contain a heap-based buffer overflow vulnerability which can allow an unauthenticated, remote attacker to execute code or commands via specifically crafted requests.
CVE-2023-46748	F5 BIG-IP Configuration Utility SQL Injection Vulnerability	F5 BIG-IP Configuration utility contains an SQL injection vulnerability that may allow an authenticated attacker with network access through the BIG-IP management port and/or self IP addresses to execute system commands. This vulnerability can be used in conjunction with CVE-2023-46747.

Figure 2 - Exploited enterprise network security devices in 2023

higher visibility to other infected devices via lateral movement, they very likely will continue to be targeted by a wide range of threat actors from financially motivated cyber criminals like ransomware gangs to nation-state threat actors. [5]

AI Advancements and Challenges in 2023: The Surge of Generative Tools and the Rise of Malicious AI

2023 marked significant advancements in AI, with a surge in tools developed for text, audio, and image generation that allowed a wider audience to create content in ways previously unseen. OpenAI's ChatGPT 3.5 reached 100 million users in only 2 months [6] following its release in December 2022 and kept growing in popularity ever since. ChatGPT 4, a new more powerful version of the Large Language Model, was released in March 2023 as a paid service, [7] and is currently being used by individuals and organizations alike. According to a recent survey 60% of the respondents among businesses said they are currently experimenting with AI generative models or are planning to work with them in 2024, only 21% have successfully deployed these models in production so far as there are still uncertainties in the adoption of this new technology. [8]

The New Face of Cyber Threats: AI-Enabled Attack Techniques

While AI adoption is growing, 2023 has seen the release of a plethora of malicious AI generative tools as well, specifically designed to help facilitate cyberattacks. [9] Malicious AI-based generative tools streamline the process of Cyber Threat Campaigns by enabling a range of attack methods, including the creation of persuasive phishing emails and malicious payloads. Consequently, AI reduces the entry barrier, inviting new participants into the cyber threat arena. Additionally, AI serves as a catalyst for established threat actors, simplifying and accelerating every step of the campaign. Content generated through malicious AI is crafted to elude standard security protocols, posing significant challenges for both human and machine detection and prevention efforts.

Legitimate LLM tools have guardrails in place that ensure that the prompt of the user does not lead to the generation of potentially harmful content, such as malicious code or a phishing email. [10], [11] These guardrails can be bypassed via adversarial attacks [12] against these systems. These attacks, also known as jailbreaks, lead to an unwanted output that aligns with the intentions of the attacker. Therefore, in addition to using specially dedicated malicious tools, threat actors can also jailbreak legitimate AI tools such as ChatGPT to create malicious content, essentially turning the legitimate LLM into a malicious generative AI tool. As more systems get integrated into AI, we are going to see more adversarial attacks directly on these systems.

Generative AI: A New Frontier in Online Propaganda and Misinformation

AI-generated content, particularly images and videos, is becoming more widespread on social media and this has a direct impact on the misinformation and disinformation

domains. Generative AI tools are capable of rapidly producing content that can exacerbate social divisions, including generating hate speech, inciting violence, and stirring discord.[13] These tools can significantly contribute to the polarization of online communities by automating the production of fake news, fabricated images, misleading videos, and provocative social media posts. This automation manipulates public opinion and erodes trust in reliable sources, evident in instances of AI-generated false news stories and images depicting events that never occurred.[14] The role of generative AI in recent conflicts, such as those in Israel and Gaza or Russia and Ukraine, and the prevalence and impact of AI-generated content in these scenariows is still debated. Some experts suggest that the impact of generative AI might be limited due to an already saturated social media environment and limited audience attention span [15], others point out its increased prevalence compared to earlier conflicts. [16]

Cybersecurity in the Age of AI: Threats and Innovations

In 2024, AI is expected to significantly impact both the offensive and defensive aspects of cybersecurity. EclecticIQ analysts anticipate that various nations will introduce AI-specific national policies and engage in global collaborations for the safe and ethical development of AI, exemplified by the Bletchley Declaration signed at the AI Safety Summit in the UK in November 2023. [17] The landscape of AI-driven toolsets and malware is poised to evolve, with an increase in AI-driven disinformation, malicious generative AI tools, new jailbreaks, and exploitation of AI vulnerabilities, as malicious actors increasingly harness AI for nefarious purposes. Concurrently, the cybersecurity community is gearing up to counter these threats, spurred by initiatives like the DARPA AI Cyber Challenge [18], which aims to foster an AI-powered defense ecosystem. This dynamic sets the stage for an AI-centric arms race in cybersecurity, where innovation is driven by the reciprocal advancements of AI defenders and offenders.

However, a significant challenge lies in the scarcity of cybersecurity professionals [19], juxtaposed with AI's role in lowering the entry barrier for cybercriminals and enhancing the capabilities of advanced persistent threats and nation states. Moreover, the pursuit of Artificial General Intelligence (AGI) by companies like OpenAI [20], which experts estimate could emerge within 5 to 10 years [21], presents a new frontier. AGI, capable of matching or surpassing human intellectual abilities, will amplify the capabilities and challenges for both cybersecurity defenders and offenders, revolutionizing the landscape with AI-powered strategies and tactics.

Cybercrime-as-a-Service Fueling the Escalation of Ransomware Attacks

In 2023, ransomware remained the biggest threat, reaching its peak levels in reported attacks. [22]–[27] Rapid diffusion of techniques and tools across the cybercriminal community contributes significantly to the persistence and evolution of ransomware threats.

The primary reason behind the escalating prominence of ransomware attacks is the proliferation of Cybercrime-as-a-Service (CCaaS). CCaaS involves the outsourcing of various elements of a cyberattack to specialized groups of attackers, akin to the outsourcing practices observed in the service sector.

This diversification and specialization of services allows attackers to hone their skills in specific areas and significantly enhance the effectiveness of their operations. Whenever a new attack method or technique emerges, cybercriminals quickly adapt to create specialized services that are made available to a wide range of attackers simultaneously. Consequently, the time lag between the development of a novel attack method and its widespread adoption has been dramatically reduced, if not eliminated.

CCaaS has lowered the barrier to entry, making it more accessible to less tech-savvy individuals. This accessibility is achieved through its ease of use, user-friendly administration consoles, and dashboards for controlling earnings. Additionally, CCaaS poses a challenge with regards to attribution to a specific group, since the means and infrastructure are shared among multiple threat actors.

Mutual Dependencies and Competitive Pressures: Understanding Cyber Threat Actor Relationships

Analysts observed threat actors collaborating or forming a cartel [28] [29], which manifests in sharing of victim

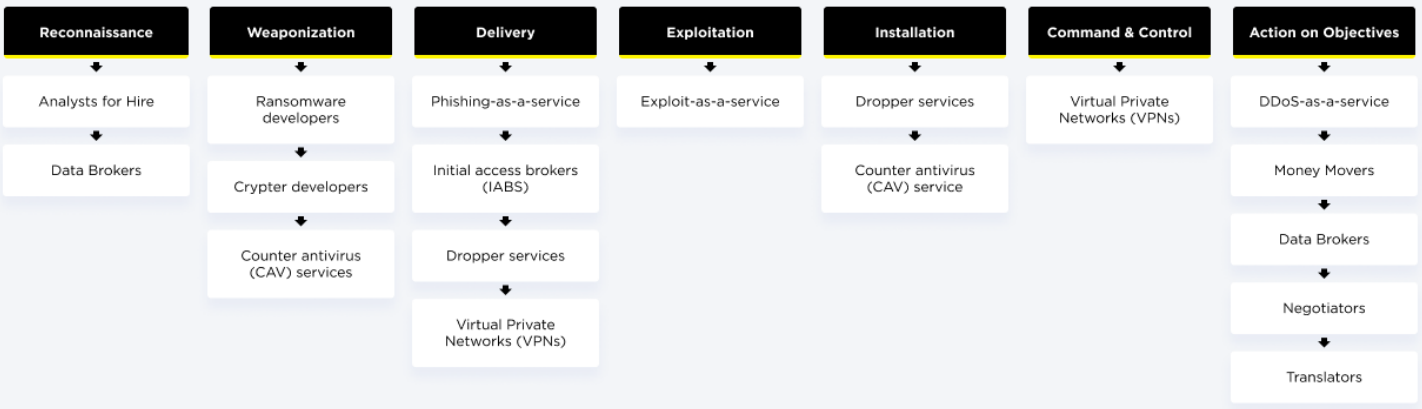

Figure 3 - CCaaS Mapped to Cyber Kill Chain

data and leak sites, infrastructure sharing, or adopting each other's tactics. The collaboration exists for a limited time, though. The more successful a ransomware gang, the more it increases its public profile, the more attention it receives from security professionals and law enforcement. As seen with REvil or Conti, the group will dissolve, rebrand, or split into new groups.

Analysts highlight that the black-market economy is characterized by mutual dependencies but also competitive pressures. CCaaS creates ambiguity and adds complexity to understanding the dynamics of threat actors and their relationships within the cybercriminal world. Additionally, ransomware code leaks [30], [31] result in new ransomware branches that share source code. The intricate nature of the underground cyber landscape makes it difficult to definitively ascertain the extent and purpose of their cooperation.

Cybercriminals Shifting Focus: Assessing Costs over Ransom Gains

Cybercriminals follow the path of least resistance when selecting their targets, opting for victims who appear to be easier to attack. In contrast to prior years, their primary objective was not primarily centered around maximizing the potential ransom; rather, ransomware actors prioritized making a rational assessment of costs and benefits.

As a result of this strategy, we have observed a growing number of ransomware attacks targeting small and medium-sized enterprises, state and local administrations, scientific institutions, as well as schools and universities. These entities have become increasingly vulnerable due to changes in ransomware tactics and lack of financial and personnel resources.

Analysts also observed ransomware operations employed social engineering tactics, with specific focus on technical administrators, like support and help desk personnel. These individuals possess permissions that can be exploited by threat actors to obtain the initial access required to compromise accounts.

A noteworthy ransomware tactic involves the use of fearmongering strategies. [32] In this approach, criminals exploit personal information, such as home addresses and family names and specifically target individuals through phone calls and text messages. Some even go to the extreme of issuing physical violence threats to coerce victims into sharing corporate access credentials. This combination of tactics highlights the gravity of the situation and the need for vigilance in dealing with malicious actors.

Organizations Neglect Backup Strategies, Resort to Ransom Payments and Insurance

Analysts observed a trend that organizations opt to pay ransomware demands [33], [34], and assess with moderate confidence that organizations have neglected to invest in and test robust backup and recovery strategies. This oversight is particularly significant because most ransomware attacks are specifically designed to target backup data. Consequently, these organizations find themselves in situations where cyberattacks have compromised not only their primary data but also their backup repositories. As a result, they perceive themselves as having no practical means of recovery other than succumbing to the ransom demands. In response to this predicament, some organizations have turned to insurance policies to cover the costs of the ransom payments. This approach is increasingly seen as a viable option, especially when low premiums are seen as a quick fix.

Paying Ransom Does Not Guarantee Data Retrieval

Analysts highlight that paying the ransom does not guarantee the successful retrieval of data.
Data indicates that even when ransoms are paid, there is no guarantee that the attackers will provide the necessary decryption keys to recover the data. [33], [34]

In other instances, decryption has failed to successfully restore all systems. In essence, paying the ransom may not always result in the successful restoration of vital information. It is considerably cheaper for organizations to use their backup systems to recover from a ransomware attack rather than paying the ransom. Instead of spending substantial sums on ransom payments, organizations can invest in robust backup and recovery strategies. This approach reduces the financial burden, increases the likelihood of successfully restoring data in the event of a ransomware attack, and greatly improves preparedness for other incidents through disaster recovery planning.

EclecticIQ Analysts Highlight Hacktivism as an Important Growing Risk Attached to Global Conflicts

Groups of cybercriminals uniting to carry out cyber-attacks in support of political causes are shifting the cybersecurity risks faced by organizations during times of conflict. Hacktivist activity and loose cooperation between individuals and states increases nuance between military vs. civilian cyber operation and changing boundaries of conflicts. While technology and hacktivism have old-school roots, increasing hacktivism is most likely a result of increasing technology.

In 2022, overt political announcements from threat actors induced a variety of outcomes. Conti's political announcement was followed by their dissolution possibly because of increased attention, while Trickbot's announcements may have enabled them to operate with reduced fear of disruption. [35] In both cases, cyber-criminal groups announced support for Russia within the context of the war with Ukraine.

2023 involved a myriad of conflicts, but the continuing Russia-Ukraine and the Hamas-Israel violence stand out. Cyberattacks and hacktivist patterns observed in 2023 impacting organizations and users outside direct regions of conflict provide integral intelligence going forward.

Widespread Information Gathering Provides the Background for Impactful Cyberattacks

Major conflicts in 2023 have seen widespread participation in disinformation, increasing blurring of state/civilian cyberattacks, and cyberattacks disrupting systems and services. All sides engage in exhaustive information stealing campaigns that provide intelligence on further targets and points of vulnerability.

Growing Hacktivism Will Increase Uncertainty and Impact on Non-Military Entities

Disinformation seeded online is of huge growing concern and perhaps easiest to participate in. The risk affects the greatest number of users. Cyberattacks that focus on disinformation may include "deepfakes". Disinformation and misinformation will increasingly impact non-military organizations inside conflict zones. Information security is lacking tools and intelligence required to effectively tackle the rising risk curated

particularly by new AI-type software and generative adversarial network content. These new capabilities will be deployed against unprepared civilian organizations.

The Russia-Ukraine war has already seen deepfake attempts on both Zelensky and Putin. [36] The Hamas-Israel conflict is demonstrating how multifaceted the risk to information can be, from false accusations to false missile threats. [37], [38] Disinformation via social media has the potential to exacerbate tensions and stimulate additional hacktivism.

State Agencies Supporting Hacker-Proxies Create Larger Impact and Risk Conflict Escalation

Cyberattacks on an interconnected entity, such as a bank, risks spreading further conflict outside the immediate conflict zone. Conflict may spread to more populations online and outside of the original conflict zones, if more groups codependently initiate better resourced cyberattacks. Even if isolated to online communities, spreading hacktivism rooted in physical conflicts potentially increases the difficulty for resolution.

In the Russia-Ukraine war, NPR reports a possible situation where entities connected to an official Ukraine government organization may have helped a hacker-proxy group infiltrate a large bank based in Russia, Alfa-Bank, exposing personal public records. [39] Resources from government entities enable greater impact in such situations. Such an event demonstrates how spillover from a regional conflict might affect growing populations of users.

System and Services Disruption Remain the Most Common Focal Point for Hacktivists

Disruptive cyberattacks take the form of wipers, denial of service, ransomware, and common hacking. These cyberattacks impact more users than other tactics.

Service disruption cyberattack risk is very likely to peak immediately following conflict outbreak. Data from Cloudflare demonstrates this trend well in the Israel-Hamas conflict. [37] DDoS cyberattack volume was highest immediately after the Hamas offensive and then tapers off but remains above zero. Organizations across many verticals are impacted to a measurable degree.

Wipers have been directed by unidentified hacktivists at many different targets during both conflicts. An Iran APT group is reported to be supporting pro-Palestine groups with wiper capabilities. [40] ESET documented indicators of compromise showing unidentified threat actors deploying wipers that were prepared well in advance. [41]

A pro-Palestine group of loose affiliates claimed (via Telegram) to have hacked a flour production company in Israel, causing damage and preventing normal operation to sections of operations. [42] Self-proclaimed hacktivists' cyberattacks potentially span diverse targets during times of conflict.

Broader and Bigger Regional Conflicts Will Catalyze Increased Hacktivism

EclecticIQ analysts observed a strong continuation of trends previously observed with further threat actors overtly claiming sides during major conflict and likely spurred to participate in cyberattacks that might not otherwise occur. The trend is very likely to expand along with the impacts, as more powerful technologies such as AI-type software spread and as historical conflicts provide a growing library of examples to future would-be hacktivists.

References:

[1] "Charting China's Climb as a Leading | Recorded Future Global Cyber Power." Accessed: Nov. 28, 2023. [Online]. Available: https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power

[2] "Stealth Mode: Chinese Cyber Espionage Actors Continue to Evolve Tactics to Avoid Detection," Mandiant. Accessed: Nov. 28, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/chinese-espionage-tactics

[3] M. T. Intelligence, "Analysis of Storm-0558 techniques for unauthorized email access," Microsoft Security Blog. Accessed: Nov. 28, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

[4] "Remote Monitoring & Management Abuse - Red Canary Report," Red Canary. Accessed: Nov. 29, 2023. [Online]. Available: https://redcanary.com/threat-detection-report/trends/rmm-abuse/

[5] "Attackers Are Probing for Zero-Day Vulns in Edge Infrastructure Products." Accessed: Nov. 29, 2023. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/attackers-probing-zero-day-vulns-edge-infrastructure

[6] R. Shewale, "ChatGPT Statistics: Detailed Insights On Users (2023)." Accessed: Dec. 01, 2023. [Online]. Available: https://www.demandsage.com/chatgpt-statistics/

[7] T. Weitzman, "Council Post: GPT-4 Released: What It Means For The Future Of Your Business," Forbes. Accessed: Dec. 01, 2023. [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2023/03/28/gpt-4-released-what-it-means-for-the-future-of-your-business/

[8] M. Bilan, "Statistics of ChatGPT & Generative AI in business: 2023 Report," Master of Code Global. Accessed: Dec. 01, 2023. [Online]. Available: https://masterofcode.com/blog/statistics-of-chatgpt-generative-ai-in-business-2023-report

[9] Livia Gyongyoși, "Malicious Generative AI Tools. Buzz, Threat, and Solution," Heimdal Security Blog. Accessed: Dec. 01, 2023. [Online]. Available: https://heimdalsecurity.com/blog/malicious-generative-ai-tools-solution/

[10] C. Anderson, "Guardrails on Large Language Models, Part 1: Dataset Preparation." Accessed: Nov. 03, 2023. [Online]. Available: https://avidml.org/blog/llm-guardrails-1/

[11] C. Anderson, "Guardrails on Large Language Models, Part 2: Model Fine Tuning." Accessed: Nov. 03, 2023. [Online]. Available: https://avidml.org/blog/llm-guardrails-2/

[12] A. Zou, Z. Wang, J. Z. Kolter, and M. Fredrikson, "Universal and Transferable Adversarial Attacks on Aligned Language Models." arXiv, Jul. 27, 2023. doi: 10.48550/arXiv.2307.15043.

[13] D. O. Gordon Curt Devine,Allison, "How antisemitic hate groups are using artificial intelligence in the wake of Hamas attacks," CNN. Accessed: Nov. 23, 2023. [Online]. Available: https://www.cnn.com/2023/11/14/us/hamas-israel-artificial-intelligence-hate-groups-invs/index.html

[14] "How generative AI is boosting the spread of disinformation and propaganda," MIT Technology Review. Accessed: Nov. 03, 2023. [Online]. Available: https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/

[15] F. M. Simon, S. Altay, and H. Mercier, "Misinformation reloaded? Fears about the impact of generative AI on misinformation are overblown," Harvard Kennedy School Misinformation Review, Oct. 2023, doi: 10.37016/mr-2020-127.

[16] W. Bedingfield, "Generative AI Is Playing a Surprising Role in Israel-Hamas Disinformation," Wired. Accessed: Nov. 03, 2023. [Online]. Available: https://www.wired.com/story/israel-hamas-war-generative-artificial-intelligence-disinformation/

[17] "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," GOV.UK. Accessed: Nov. 03, 2023. [Online]. Available: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

[18] "DARPA AI Cyber Challenge Aims to Secure Nation's Most Critical Software." Accessed: Nov. 03, 2023. [Online]. Available: https://www.darpa.mil/news-events/2023-08-09

[19] C. Combs, "Cyber security talent gap amid AI boom could be perfect storm, expert warns," The National. Accessed: Nov. 03, 2023. [Online]. Available: https://www.thenationalnews.com/business/technology/2023/11/03/cyber-security-talent-gap-amid-ai-boom-could-be-perfect-storm-expert-warns/

[20] "About." Accessed: Nov. 24, 2023. [Online]. Available: https://openai.com/about

[21] P. McGuinness, "When AGI?," AI Changes Everything. Accessed: Nov. 24, 2023. [Online]. Available: https://patmcguinness.substack.com/p/when-agi

[22] Fortinet, "The 2023 Global Ransomware Report." Accessed: Nov. 24, 2023. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

[23] Federal Office for Information Security, "The State of IT Security in Germany in 2023", [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=8

[24] Verizon, "2023 Data Breach Investigations Report," Verizon Business. Accessed: Nov. 23, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[25] T. I. Team, "Global ransomware attacks at an all-time high, shows latest 2023 State of Ransomware report," Malwarebytes. Accessed: Nov. 24, 2023. [Online]. Available: https://www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report/

[26] "Internet Organised Crime Assessment (IOCTA) 2023," Europol. Accessed: Nov. 26, 2023. [Online]. Available: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

[27] Trellix, "The CyberThreat Report – November 2023," 2023.

[28] Jon DiMaggio, "Ransom Mafia - Analysis of the World's First Ransomware Cartel," Analyst1. Accessed: Nov. 28, 2023. [Online]. Available: https://analyst1.com/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel/

[29] Lucian Constantin, "What is Ransom Cartel? A ransomware gang focused on reputational damage," CSO Online. Accessed: Nov. 28, 2023. [Online]. Available: https://www.csoonline.com/article/574109/what-is-ransom-cartel-a-ransomware-gang-focused-on-reputational-damage.html

[30] A. Delamotte, "Hypervisor Ransomware | Multiple Threat Actor Groups Hop on Leaked Babuk Code to Build ESXi Lockers," SentinelOne. Accessed: Nov. 28, 2023. [Online]. Available: https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/

[31] 3xp0rt [@3xp0rtblog], "The source code of the HelloKitty ransomware has been leaked on the XSS forum by kapuchin0 (Gookee). https://t.co/rjGnD87NRL," Twitter. Accessed: Nov. 28, 2023. [Online]. Available: https://twitter.com/3xp0rtblog/status/1710387356979560800

[32] M. I. R. Intelligence Microsoft Threat, "Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction," Microsoft Security Blog. Accessed: Nov. 03, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

[33] J. Buffington, Dave Russell, and Julie Webb, "Ransomware Trends 2023 Report," 2023, [Online]. Available: https://www.veeam.com/wp-ransomware-trends-report.html

[34] Sophos, "State of Ransomware 2023." Accessed: Nov. 26, 2023. [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[35] "EclecticIQ Retrospective: A Look at the Themes & Events that Shaped the 2022 Cyber Landscape." Accessed: Nov. 29, 2023. [Online]. Available: https://blog.eclecticiq.com/eclecticiq-retrospect-a-look-at-the-themes-events-that-shaped-the-2022-cyber-landscape

[36] G. B. Mueller, B. Jensen, B. Valeriano, R. C. Maness, and J. M. Macias, "Cyber Operations during the Russo-Ukrainian War".

[37] Omer Yoachimik and Jorge Pacheco, "Cyber attacks in the Israel-Hamas war," The Cloudflare Blog. Accessed: Nov. 08, 2023. [Online]. Available: http://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

[38] Tommaso Canetta, "EDMO - Preliminary analysis of the Israel/Hamas conflict-related disinformation," EDMO. Accessed: Nov. 06, 2023. [Online]. Available: https://edmo.eu/2023/10/17/edmo-preliminary-analysis-of-the-israel-hamas-conflict-related-disinformation/

[39] J. McLaughlin, "Ukrainian hackers and intel officers partner up in apparent hack of a top Russian bank," NPR, Oct. 25, 2023. Accessed: Nov. 29, 2023. [Online]. Available: https://www.npr.org/2023/10/25/1208352887/ukraine-russia-bank-hack

[40] P. Paganini, "Iranian Agonizing Serpens APT is targeting Israeli entities with destructive cyber attacks," Security Affairs. Accessed: Nov. 08, 2023. [Online]. Available: https://securityaffairs.com/153703/apt/iranian-agonizing-serpens-apt-wipers.html

[41] ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper," ESET. Accessed: Nov. 08, 2023. [Online]. Available: https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/

[42] P. Paganini, "Pro-Palestinian hackers group 'Soldiers of Solomon' disrupted the production cycle of the biggest flour production plant in Israel," Security Affairs. Accessed: Nov. 08, 2023. [Online]. Available: https://securityaffairs.com/153778/security/soldiers-of-solomon-hacked-israel-flour-plant.html

EclecticIQ

Intelligence at the core

Intelligence
Automation
Collaboration

About EclecticIQ

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

The most targeted organizations in the world – including governments and large enterprises – use our platform to automate intelligence management at scale and accelerate collaboration across security teams.

With our open and extensible cybersecurity platform and ecosystem, they are able to stay ahead of rapidly evolving threats and outmaneuver adversaries by embedding Intelligence at the core™ of their cyberdefenses.

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

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