NETACEA

REPORT

Netacea Cybersecurity and Bot Predictions 2023

Netacea @Netacea_AI www.netacea.com hello@netacea.com

Executive Summary

Each year Netacea's Threat Research team predicts the top cyber-trends for the following 12 months. Looking towards the year ahead, we've predicted trends across cybersecurity and the bot landscape to help your business stay one step ahead of cyber-attackers in 2023.

Geopolitical and social factors continue to shape the bot landscape and attack vectors, with APIs still a rising target and state warfare influencing attack origins and motivations. Emerging and evolving technologies such as IoT devices widens attack surface area, meaning attacks grow in sophistication, volume and intensity.

As usual, the ethics and law enforcement surrounding cyber-attacks continue to change the arms race between business, state and attacker. But as governments become smarter and legislation gets tougher, bots change the game.

Cybersecurity Predictions

1 Ransomware: Less encryption, more legislation

Ransomware and cyber extortion will remain among the top cyber threats in 2023. As cybercriminals' tactics evolve, they will increasingly favor exfiltrating data over encrypting it for cyber extortion.

Double extortion ransomware (where a copy of the data is exfiltrated before it is encrypted) has surpassed traditional ransomware as cybercriminals' extortion tactic of choice. The threat of the exfiltrated data being leaked provides cybercriminals with a secondary lever with which to apply pressure on victims to pay up. However, as organizations adopt stronger backup and resilience measures, the primary impact is now being caused by the data exfiltration, rather than data encryption. This may lead to some cybercriminals forgoing encryption entirely and refocusing of exfiltration efforts. There have already been notable cases of ransomware which either skipped or **faked data encryption.**

Governments are expected to continue advising organizations against paying ransoms to prevent the financing of criminal organizations. The UK's Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) released a joint letter to lawyers in June 2022 clarifying that UK "law enforcement does not encourage, endorse nor condone the payment of ransoms" although "payments are not usually unlawful"[1]. As ransomware continues to rise, governments around the world may go a step further and introduce legislation to prohibit ransomware payments.

Sources:
1. RE: The legal profession and its role in supporting a safer UK online. (UK's Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC))

2 Phishing: Powered by AI

Machine learning and artificial intelligence have quickly become key technologies in the fight against cyber threats, for example, helping businesses to detect attacks by monitoring network patterns and analyzing anomalies or malicious behaviors. However, as AI has become more advanced and accessible, it has also been adopted by cybercriminals.

Cybercriminals will utilise AI and machine learning in 2023 to power more sophisticated phishing campaigns. With access to an ever-growing treasure trove of data, from open-source data such as job postings to personal information leaked in data breaches, criminals can craft highly targeted spear phishing lures. Researchers have already shown how next-generation language models such as OpenAI's GPT-3 can be used to generate phishing content that "outperformed those that were manually created"[2]. With GPT-4, the next evolution of the language model, rumoured for release in 2023, the threat of AI-powered phishing becomes more severe.

3 Hacktivism: From nuisance to nightmare

As the barrier to entry for cyber-attacks continues to drop, organizations will have to contend with a rising threat of hacktivism. Political, ideological and social activists will increasingly use cyber-attacks as a vehicle to promote their causes, cooperating with other threat actors to launch more damaging attacks.

Interest in hacktivism rose over 2022 due to high-profile geopolitical and social issues. A prominent example of this was the IT army of Ukraine, a hacktivist cyber warfare group created in response to Russia's invasion of Ukraine, which has launched thousands of cyber-attacks against Russian assets.[3]

Cybercrime-as-a-service offerings will help to bridge the capability gap between hacktivists and more mature threat groups. Compromised accounts, customized malware, botnets, and phishing kits easily purchasable on underground forums or private messaging channels can be used to launch sophisticated cyber-attacks. We expect hacktivists to supplement their current arsenal of primarily distributed denial of service (DDoS) and defacement attacks with large scale data exfiltration, encryption or deletion.

Sources:

2. Turing in a Box: Applying Artificial Intelligence as a Service to Targeted Phishing and Defending Against AI Generated Attacks (Black Hat USA 2021)

3. IT Army of Ukraine

4 Supply chains: Still the weak link

Supply chain attacks will continue to rise in 2023 as attackers consider all possible entry points to compromise their target organization. Enterprise organizations form a complex supply chain network with multiple dependencies operating across different geographies. Just as complex computer networks present visibility gaps for defenders, the complexity of supply chain networks makes them attractive targets for cyber-attackers.

Supply chain attacks can be extremely damaging due to the time it takes to detect, investigate and respond to them. Communication and visibility gaps between organizations can allow attackers to remain undetected for long periods of time. Response activities can also be slowed as they require coordination across multiple entities, sometimes with conflicting priorities.

The network effect of a supply chain attack also allows attackers to maximise the return for their activities, potentially compromising a wide range of organizations through a shared third party. An example of this is the supply chain attack against SolarWinds Systems in 2020, which resulted in around 18,000 organisations being possibly affected by it, including the United States government.[4]

5 Emerging technologies: Web3 and IoT

The Internet of things (IoT) is one of the bigger emergent technologies which can affect everybody, especially with digitalization of every aspect of modern life. IoT devices are being deployed everywhere, from home networks to industrial and corporate networks. The number of connected IoT devices is expected to reach over 14 billion by the end of 2022 and continue growing in 2023.[5] If secured incorrectly, these devices can offer substantial security risks and are often the target of brute force password attacks, DDoS or Person in the Middle Attacks (PitM).

In 2023, we will also see further use of Web3 technology and the deployment of centralized applications which promise increased security, reduced energy costs, increased privacy and greater control. Web3 developers will attempt to minimize the need for complex code, allowing inexperienced coders to build Web3 applications. However, as Web3 usage grows and new products and services are built on the technology, cybercriminals will look to take advantage of the hype and strike while the Web3 space is still relatively immature from a security perspective. Financial applications of Web3 technologies such as cryptocurrency will continue to be heavily targeted by cybercriminals, with more notable attacks to come against crypto exchanges.

Sources:

4. SolarWinds hack explained: Everything you need to know (TechTarget)

5. IoT 2022: Connected Devices Growing 18% to 14.4 Billion Globally (IoT For All)

Bot Predictions

1 AI-powered spam bots will be used to amplify disinformation campaigns

Spam bots are used to promote (or suppress) a viewpoint or product, or to get a user to click a malicious link. They can create and operate multiple fake accounts, which they then use to post spam content on social media platforms, forums and message boards, or via email. Geopolitical bots aim to manipulate public opinion for political purposes and operate in a similar way to spam bots. In August 2022, the SSU (Ukrainian cyber police unit) reported that it had shut down a one-million strong geopolitical bot farm.[6]

The limiting factor currently for both classes of bot is the ability to generate and post human-like text. Bot operators currently rely on a limited library of messages, resulting in repetitive and predictable output. Natural language AI models provide bot operators with a solution to this, as these can generate human-like synthetic text. Researchers have shown how OpenAI's GPT-3, a powerful natural language model, can be used to amplify disinformation narratives.[7] Bots powered by GPT-3 have also already been used to interact with users on social media platforms. With OpenAI's GPT-4 expected to be released in 2023, these bots could become even more effective and their posts almost indistinguishable from humans.

2 The ethics and legality of web scraping will continue to be unclear

Ethics and legality will continue to be a growing concern for the web scraping industry in 2023. Whilst bot activity like credential stuffing is clearly illegal, scraper bot activity occupies a greyer area. Some web scraping is clearly welcome, such as that done by search engine spiders. However, web scraping can also negatively impact online businesses.

One example of the growing focus on ethics in scraping is residential proxy networks, used heavily by web scrapers to bypass defences. Residential IP collection practices have not always been ethical or legal. Many residential IPs have historically been gathered without their owners' consent, and some still are. In a bid to promote their legitimacy and attract corporate clients, many residential proxy providers are now quick to highlight how ethical and transparent their collection of residential IP addresses is.

However, the legality of web scraping is constantly evolving, as evidenced in the six-year long LinkedIn Corporation vs. hiQ Labs court case. The argument that scraping is legal was buoyed by a perceived endorsement

Sources:

6. SSU shuts down million-strong bot farm that destabilized situation in Ukraine and worked for one of political forces (SSU)

7. Disinformation At Scale: Using GPT-3 Maliciously for Information Operations (Black Hat USA 2021)

of web scraping by the US Court of Appeals in April 2022. The Court's ruling that hiQ's scraping of public LinkedIn profiles did not violate the Computer Fraud and Abuse Act (CFAA) was taken by many to legitimise web scraping. However, seven months later, the Court ruled in favour of LinkedIn's "breach of contract" claim, on the basis that hiQ breached LinkedIn's User Agreement, which clearly prohibits scraping and creation of fake accounts. The full ramifications of this decision are yet to be determined but will certainly affect the scraper bot industry in 2023.[8]

3 Bot attacks on APIs will rise significantly

APIs have fast become the backbone of the digital economy, with API adoption on the rise across most if not all industries. However, these APIs increase the attack surface that bad bots can exploit. In Netacea's Bot Management Review 2022, a survey of more than 400 enterprise organizations, respondents reported a 70% rise in bot attacks against APIs over the previous year.[9]

We expect to see an equally significant rise in API bot attacks in 2023. Shadow APIs are at heightened risk as these effectively leave bots with an unprotected and open door to exploit. However, as bot developers eschew targeting websites in favor of going directly to the source APIs, even known and well-managed API endpoints will increasingly come under fire.

Sources:

8. LinkedIn v. HiQ and the trans-Atlantic privacy divide (IAPP)
9. The Bot Management Review 2022 (Netacea)

NETACEA

Beat bots every time with Netacea's agentless approach

Choosing the right bot management solution is a major decision for any business. Understanding the bot landscape and the threats posed to your business is the first step in staying one step ahead of malicious actors.

Blocking bots has always needed agents deployed client-side using JavaScript and mobile SDKs. Unfortunately, this approach is out of date, and agents aren't enough to fight against sophisticated bots.

Netacea's agentless technology analyzes billions of interactions for user intent to identify robotic signatures and stop threats, six times more accurately than other bot mitigation solutions.

To learn more about our 2023 cyber predictions, talk to the Netacea Threat Research team today at hello@netacea.com. Or to book a free demo of Netacea Bot Management, visit netacea.com/book-a-demo.