cybersixgill

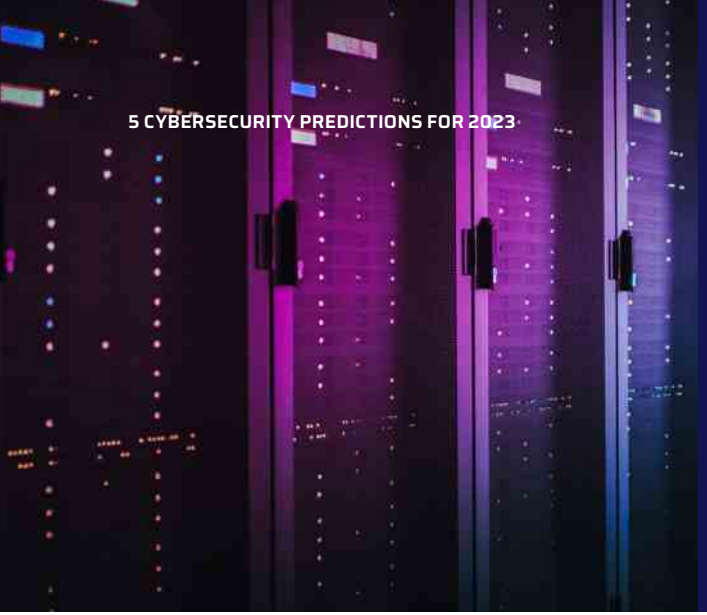
5 CYBERSECURITY PREDICTIONS FOR 2023

Introduction

What is unique about the world we are in now – is that it is not just increasingly sophisticated technology escalating cyber conflicts – but the changing vectors of motivations and new alliances among protagonists and antagonists. Cyber warfare is becoming increasingly complex as it stretches across global geographies. Attack surfaces are expanding, and we are seeing increasing threats with ideological and financial motives. Furthermore, government organizations and businesses face limited talent resources and budgets to proactively prevent attacks, forcing them to do more with less.

There's no debate that cybersecurity threats are increasing daily across almost every industry. The past 12 months have proven that adapting hasn't been easy. In fact, in 2022, 21 percent of global organizations experienced a ransomware attack. Of those, 43 percent experienced a significant impact on their business operations.

In the cyber security realm, it's impossible to predict what we will experience day after day, however, we can use threat intelligence to reveal trends likely to impact organizations in the year ahead. As 2023 gets underway, we expect a record-breaking year of cyber security breach notifications, not only because of the sophistication of threat actors but also due to considerable global flux. While the western world struggles with rising grocery bills and gas prices, the dark web economy is chugging along as usual.



TREND #1

The Rise Of New Threat Actors

The risks to global government, business organizations and individuals

The rise of the quasi-APT becomes a more entrenched cyber threat with capabilities equal to those of nation-state-sponsored threat actors.

In 2023, the quasi-APT's emergence will escalate due to the democratization of cyberweapons and the democratization of access enabled by powerful technology now accessible to the cybercriminal underground. For as little as $10 a piece, threat actors can purchase access and gain a steady foothold in their targets' systems, attaining a beachhead into highly secured organizations without having to bother with the complex, drawn-out process of gaining initial access on their own. By outsourcing access, attackers of all levels of sophistication can leapfrog several steps, getting steadily closer to the level of an APT – hence the birth of the quasi-APT.

CISOs must maintain constant vigilance, ensuring their organization can track, monitor and remediate threats from multiple focal points, adding the average Dark Web actor or the local anonymous chapter to the 'watch' list.

The cybersecurity industry will see an uptick in unexpected partnerships between nation-state actors and threat actors who are financially motivated and geographically diverse. Critical infrastructures are of crucial concern, as they will be targeted for ideological and financial reasons. These multi-geography partnerships could be harder to tackle from a law enforcement and cybersecurity perspective.

PREVENTATIVE ACTION: Automated threat intelligence and robust vulnerability management programs are now more critical than ever. Make sure your threat intelligence gives your organization visibility into the latest threat actor activity from the clear, deep and dark web.

TREND #2

The Use of Artificial Intelligence

Serving both sides of the cyberwar battlefield

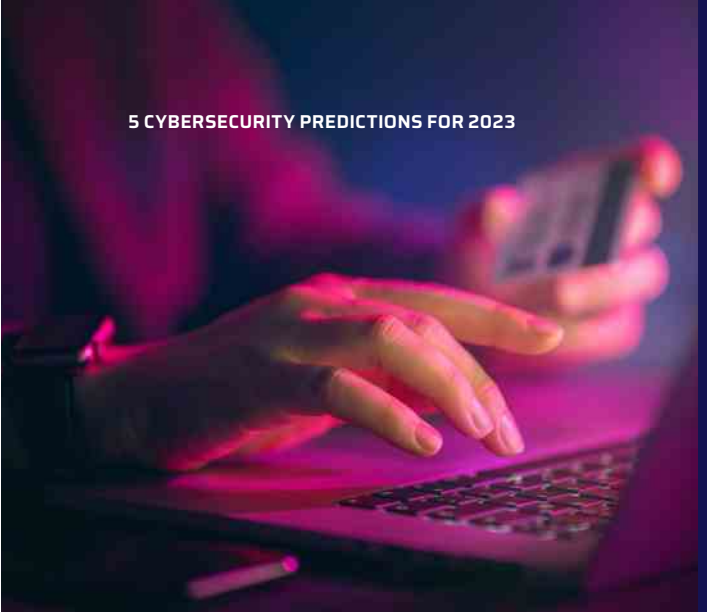
Malicious AI enables threat actors to perform nefarious activities more efficiently and overwhelm organizations being attacked. It does this by helping threat actors quickly identify password patterns, aiming to beat the targets' ability to respond.

How does artificial intelligence (AI) change the cybersecurity landscape for threat actors and organizations? According to our threat research experts, AI creates new opportunities for cyber-attacks and alliances among threat groups. As a result, organizations increasingly face more significant challenges in taking proactive cybersecurity measures.

The use of AI in cyber threat intelligence will escalate in 2023. Why now, since AI has been in play for several years? Historically, criminals have embraced technology a few years after launch when it has become easy to use. We are now at a point where teenagers can use scripts found on GitHub to do basic AI and use them for a multitude of purposes. Threat actors can use AI for an advanced 'credential stuffing' attack, helping them to recognize patterns in passwords and generate password guesses for different systems. On the other side of the battlefield, organizations use AI to respond to threat actors and criminals.

In 2023, AI automation will play an essential role in proactive cybersecurity. AI can detect real threats and build defenses, combining automation, advanced analytics, and rich vulnerability exploit intelligence to address all phases of the Common Vulnerabilities and Exposures (CVE) lifecycle.

PREVENTATIVE ACTION: Government and enterprise organizations will need to harness the power of AI for proactive cybersecurity measures that operate 24/7, moving away from a reliance on manual, reactive approaches.



TREND #3

New Attack Surfaces Arise In The ePay Space

A surge of online payments proves too tempting to resist

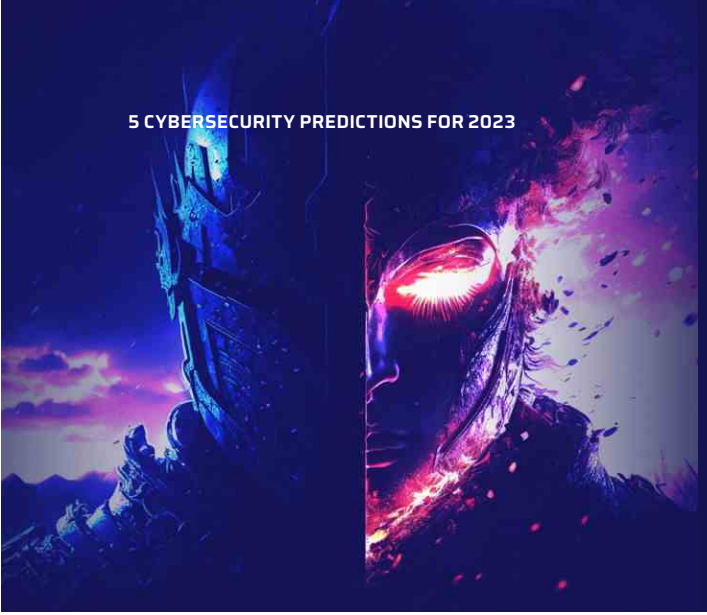
As the e-payments space grows and attack surfaces expand, we will see new opportunities for threat actors to target users and companies.

As the digital economy grows, digital crime grows with it. Soaring numbers of online and mobile interactions are creating millions of attack opportunities. Many lead to data breaches that threaten both people and businesses. At the current growth rate, damage from cyberattacks will amount to about $10.5 trillion annually by 2025.

Electronic payment methods changed significantly in 2022, and this momentum is expected to increase further in 2023. Online payments surged parallel to the growth in online shopping during the COVID-19 pandemic. According to the Electronic Payments Coalition, nearly $2 billion in mobile payments were processed daily in 2021, up 22% from the year before. At the same time, the annual survey by the Association of Financial Professionals found payment scams hit almost 75% of businesses. Thirty percent of companies in the 2021 AFP Payments Fraud and Control Survey Report said payment fraud was rising. The majority blamed adjustments brought on by the pandemic.

The COVID-19 pandemic ushered in an unprecedented era of online shopping, digital payments, and cybercrime. Biometric advances, new international standards, and cyber-security tools are all shaping the new world of fraud protection in payments. In the coming year, we will see new opportunities for cyber-attacks and alliances among threat groups targeting the ePay space, creating greater challenges for organizations.

PREVENTATIVE ACTION: Our experts have identified significant economic motivation on the dark web to go after ePay. Ensuring your organization has access to conversations between criminals on the dark web will give you the earliest indication of an impending targeted attack before it escalates into a breach such as ransomware.



TREND #4

Same Fight, New Regulations

Federal regulatory requirements may bring about increased attacks for businesses

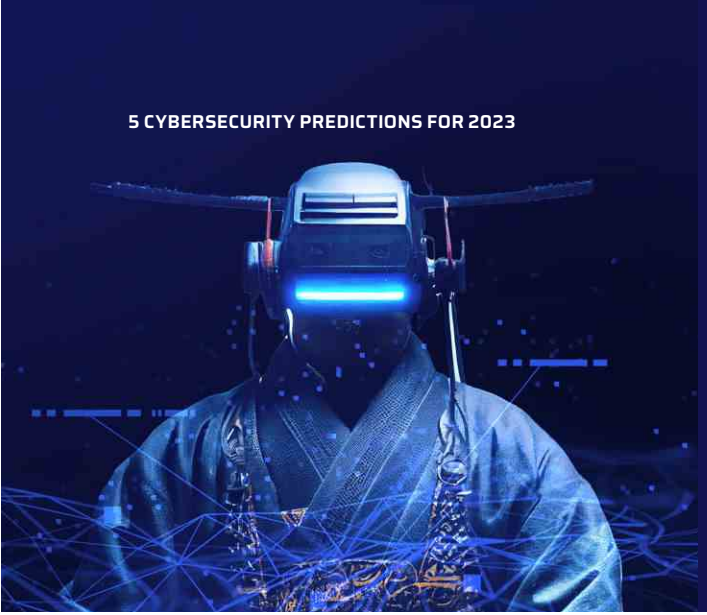
As the year progresses, noticeable disparities will arise in addressing cybersecurity in both the private and public sectors. New government regulations and reduced budgets will force security teams to do more with less.

Come 2023, in the United States – there will be different experiences for the government versus companies, with the private sector on its own regarding the increasing number and ferocity of attacks.

Businesses will need to respond to new federal regulatory requirements. In doing so, they may experience increased attacks, given their predisposition to take visible political stances and engage in boycotts against other countries.

The Federal Government will focus on using resources to protect its organizations as politically motivated attacks increase from state-sponsored organizations and individuals and organizations politically motivated and incited by current actions - but are not state-backed. They are motivated by finances and the strong desire to take a stance (through technology), as their form of protest.

PREVENTATIVE ACTION: Keep your regulatory database up to date and ensure your organization has adequate notice of changes. Make senior leadership aware of the repercussions of any public political statements from the government or key stakeholders so that the business can agree upon the level of acceptable risk exposure. Check to see if your threat intelligence vendor gives you early warning access to conversations amongst threat actors planning to target your organization or make a political protest.



TREND #5

A Change Of Approach

CISOs seek new cyber strategies to cope with budget cuts and maintain c-suite confidence

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern environments and enable digital transformation by using robust authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention.

Over the coming months we anticipate CISOs will continue to consolidate technologies and tools in a bid to manage budget cuts. As budgets continue to be squeezed throughout the year, cutting security awareness and staff training may be tempting. Organizations may start to abandon compliance-based awareness campaigns of the past in favor of extensive behavior and culture change programs that promote safer workplace practices.

We will also see the prioritization of security controls and solutions that protect customer-facing and revenue-generating workloads. Investments in Zero Trust models are therefore set to continue to rise, supporting cloud migration and remote access without compromising security.

PREVENTATIVE ACTION: It is crucial to remember that most data breaches still result from human error, so staff training is essential. Before consolidating your security stack, undertake a thorough validation assessment to identify duplication or underutilized tools. If investing in zero trust, look for vendors capable of servicing a 99.999% uptime, covered by a strong service level agreement to support remote workers.

Summary

Nothing is stagnant in cybersecurity. Cybercrime is increasingly lucrative, even more so than drug trafficking. We expect a record-breaking year of cybersecurity breach notifications, not only because of the sophistication of threat actors - but also due to more significant changes in the world.

To protect your organization, re-think your threat intelligence and gain access to the earliest indications of risk, moments after they surface on the clear, deep and dark web.

About Cybersixgill

Cybersixgill brings agility to cyber defense, with fully autonomous threat intelligence solutions to help organizations proactively detect and protect against phishing, data leaks, fraud, malware, and vulnerability exploitation - enhancing cyber resilience and minimizing risk exposure in real-time. Cybersixgill's proprietary algorithms extract data from a wide range of sources, including content from limited-access deep and dark web forums, underground markets, invite-only messaging groups, code repositories, paste sites and clear web platforms, as well as an unparalleled archive of indexed, searchable historical data from as early as the 1990s. This data is processed, correlated and enriched with machine learning techniques to create profiles and patterns of malicious threat actors and their peer networks delivering critical insight into the nature, source and context of each threat.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases.

Learn more at www.cybersixgill.com

Follow us

cybersixgill