

Global Threat Forecast: H2 2023 Predictions

Cyber security threats impacting the second half of 2023, with valuable insights to improve business cyber security posture.

securityhq.com



Table of Contents

Executive Summary	03
Vulnerabilities at Record High	03
H2 2023 Vulnerabilities Forecast	05
AI-Powered Social Engineering Attacks	05
Cloud-Based Breaches	05
Enhanced Phishing Attacks	06
Zero-Day Vulnerabilities in Supply Chain Attacks	06
H2 2023 Threat Forecast	07
LockBit – The Major Threat	07
Increase in Geo-Political Hacktivism	08
China Favourites Exposed Network Devices	09
Iran Remains Destructive	10
Recommendations To Enhance Cyber Security Posture - 6 Steps	12
About SecurityHQ	14

Executive Summary

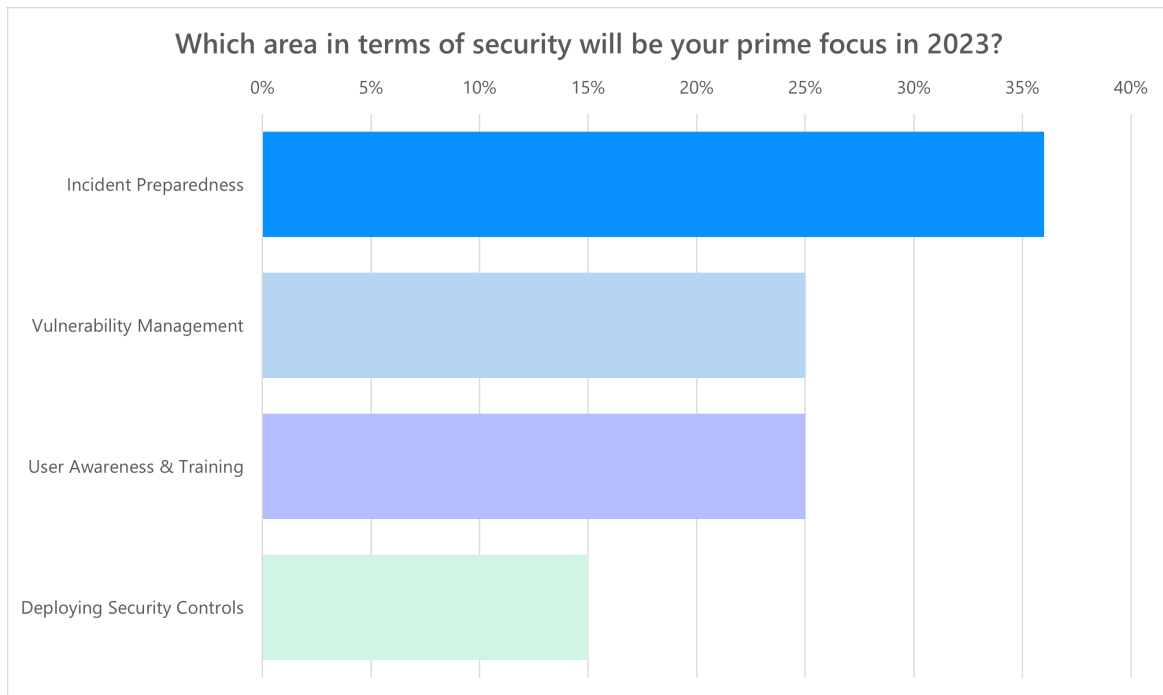
Throughout the first half of 2023 the world faced many challenges. Countless events impacted how society has functioned, how businesses developed, and how people lived. At the [beginning of 2023](#), and in [2022 SecurityHQ predicted that cybercrime would be high](#) on that list of challenges. But the scale of threats exceeded what anyone could have anticipated. Businesses have been left unable to recover from cyber-attacks. Data has been leaked on a daily basis and the processes to protect data and people are more complex than ever. According to [IBM's Cost of a Data Breach Report 2023](#), '51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.'

As a global MSSP, [SecurityHQ](#) has full visibility of threats as they evolved, and of the large campaigns and threat groups as they developed. This paper will discuss some of the vulnerabilities, evolving threats, prevalent actors, and industries targeted, and what that means with regards to the progression of threats during H2 2023. Most importantly, take a look into some of the solutions, recommendations, and actions to combat and mitigate against these threats.

Vulnerabilities at Record High

The number of disclosed vulnerabilities in 2022 was staggering, at over 26,412 vulnerabilities recorded. This statistic came directly from NIST National Vulnerability Database and is a record number that SecurityHQ expected to be topped in 2023.

Threat actors are known to lean heavily on these vulnerabilities. To understand how our customers are planning to counter these threats, SecurityHQ conducted some research, and asked what areas of cyber security their focus would be, in 2023. It was good to see that Incident Preparedness was at the top, with 36%, followed by [Vulnerability Management](#), User Awareness and Training, and Deploy Security Controls.



Source: SecurityHQ LinkedIn Poll, Jan 2023

© Copyright 2023 SecurityHQ

What these statistics show, is how companies security posture has matured. Incident preparedness and Vulnerability Management is at the core of security, and that will not change. But incident preparedness is not discussed enough. Often companies are not conducting tabletop exercises or lack incident response capabilities, turning to search engines for help when they don't know where to go. If teams within an organisation are turning to search engines for cyber security advice, this suggests a lack of knowledge and/or preparation which could be catastrophic.

H2 2023 Vulnerabilities Forecast

Four vulnerabilities to be aware of, going into the second half of the year.

1. AI-Powered Social Engineering Attacks

Artificial intelligence has entered almost all spheres of the business world. While AI brings numerous benefits and advancements, it also introduces new cybersecurity risks, such as social engineering attacks. These attacks entail manipulative tactics to deceive the victims into revealing sensitive information or trespassing security structures of the organizations. To execute these attacks, cybercriminals rely on AI-based natural language processing (NLP) algorithms to generate more realistic and human-like phishing emails, chatbot interactions, or voice calls. According to Forbes 'AI technology is advancing so rapidly that hackers are very possibly developing their own custom AI applications specifically designed to take social engineering to the next level.' Detecting these malicious campaigns is getting harder for the average employee, which is why significant training is required to know what to look for and how to prevent escalation.

Next Step: Learn more about [social engineering attacks](#) and steps to put in place.

2. Cloud-Based Breaches

Cloud computing has become a norm in today's digital landscape, offering scalability, flexibility, and cost-efficiency to businesses. Nevertheless, the widespread adoption of cloud services exposes organizations to new cybersecurity threats, making them a major concern in 2023. Cybercriminals target cloud environments to exploit misconfigurations, weak access controls, or insecure APIs.

A recent example of the consequences of cloud misconfigurations is the Toyota data leak, where the personal information of over two million customers was exposed after an access key was leaked on GitHub for almost five years. 'Upon discovering the GitHub repo, Toyota immediately made it private. Two days later the company changed the access key to the data server. The Japanese giant commissioned an investigation into the blunder and was unable to confirm or deny whether miscreants had spotted and used the key to pilfer data from the server.' reports The Register.

Next Step: Learn more about [Cloud Security in this infographic](#).

3. Enhanced Phishing Attacks

Phishing attacks involve cybercriminals posing as trustworthy entities with the intention of deceiving individuals into divulging sensitive information or performing malicious actions. With over 500 million phishing attacks reported in 2022 (Forbes Advisor), this number is expected to rise further this year. In fact, threat actors are continuously refining their techniques to make phishing emails and messages appear more genuine and convincing, which take a trained eye to spot.

Next Step: Read this blog on latest [HTML phishing vulnerabilities](#) to learn more.

4. Zero-Day Vulnerabilities in Supply Chain Attacks

With the increasing complexity of supply chains and the interconnectivity of various systems, zero-day vulnerabilities are anticipated to be a significant cybersecurity threat during the Summer of 2023. A zero-day attack is a strategic exploitation that involves the use of previously unknown vulnerabilities in the supply chain and has no available patches or fixes. These vulnerabilities in the supply chain can have severe consequences, allowing attackers to compromise the integrity and security of products and services. They can lead to data breaches, unauthorized access, and the potential for sabotage or manipulation of systems.

Next Step: Read an example of a [zero-day vulnerability](#).

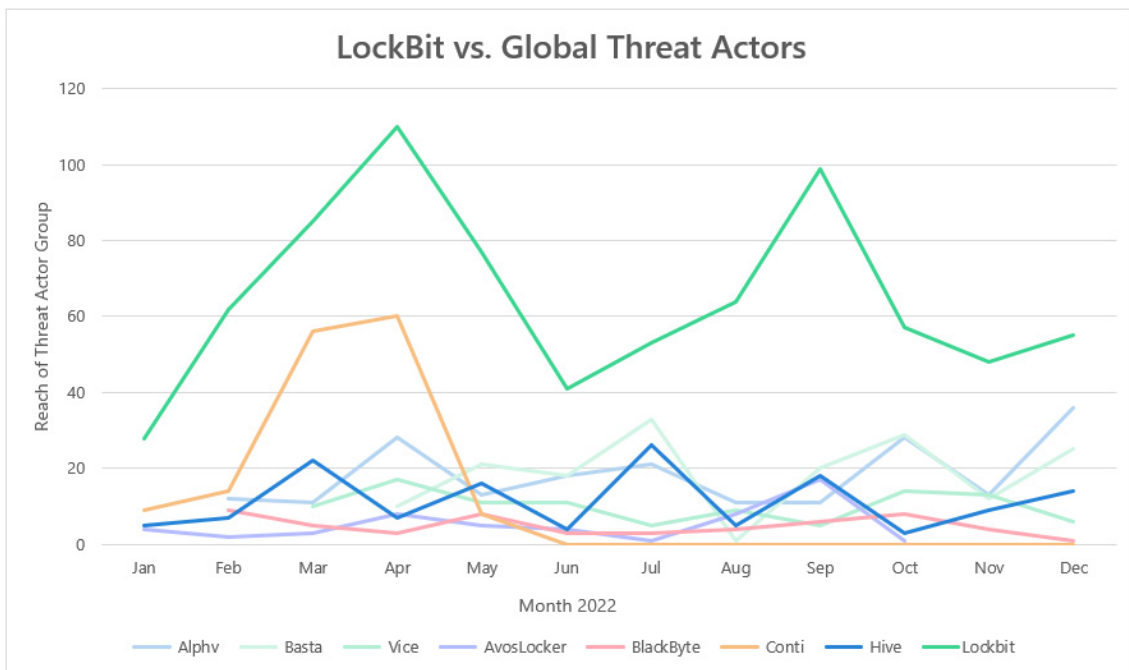
H2 2023 Threat Forecast

1. LockBit – The Major Threat

Based on SecurityHQ intelligence alone, in 2022 there was a 33% increase in active ransomware groups. This number will increase in 2023, which is why organisations need to focus on [LockBit](#) right now, as they will likely be the major threat actor in 2023.

- Active since September 2019
- The LockBit ransomware gang is one of the most notorious organized cybercrime syndicates that exists today.
- Most prolific RaaS operator in 2022. Not always in control of LockBit attacks.
- SecurityHQ highlighted LockBit as an adversary to be watch out for during the 2022 Global Threat Forecast Webinar.

LockBit have gained a lot of popularity throughout 2022, which is highlighted by the red line in the diagram below. Showing a month-by-month snapshot, LockBit are a ransomware as a service group, stand head and shoulders above other top players, including Alphv, Basta, Vice, Conti, and Hive.



Source: Leak site of each mentioned ransomware group, Jan 2023

© Copyright 2023 SecurityHQ

And the gang is very confident in its capabilities. LockBit have a well publicised bug bounty programme, where they encourage the user to find vulnerabilities in the encryptor, even in their web platform, and offer a million dollars to anyone who can DOX the owner or operator of LockBit. That's how confident they are that their anonymity is impermeable.

'The issue with LockBit is that the media are very quick to jump on a story. In a recent attack against the RoyalMail, the news was plastered with 'Russian ransomware hits RoyalMail', but, following the attack, operators of LockBit came out and said it was one of their affiliates who conducted the attack. The affiliate could have been based anywhere, so it is not always the operator themselves, it can be the affiliate that makes the attack.' - **Aaron Hambleton, Director of Middle East & Africa, SecurityHQ.**

Because of this, LockBit is self-designed to avoid encryption in any devices that are in Russia, or other Commonwealth of Independent States. That itself speaks volumes and is most likely because they don't want to have any reactive responses from Russian government. Imagine if an affiliate targeted Russian organisations, LockBit would find themselves in hot water very quickly. Their design ensures that this does not happen.

'LockBit are a fascinating group to follow, and the more we understand how they work, the better chance we have to remediate threats, and push intelligence into what we provide globally.' - **Aaron Hambleton, Director of Middle East & Africa, SecurityHQ.**

Next Step: Read more about LockBit in this blog '[The Prolificacy of LockBit Ransomware](#)'.

2. Increase in Geo-Political Hacktivism

Since the start of the Invasion from Russia into the Ukraine, this being the largest attack in Europe since World War Two, there have been significant cyber-attacks both coming from, and aimed at, Russia.

In response to the physical attack from Russia, the Ukraine have made a series of cyber-attacks. Known as the 'IT Army', a volunteer-based site has been formed. On this site lies a hitlist of Russian targets, as well as information including IP addresses of said targets and businesses. According to the Council on Foreign Relations, 'The Ukrainian IT Army is a threat actor comprised of international and Ukrainian volunteer hackers working in collaboration with officials from Ukraine's Defence Ministry to target Russian infrastructure and websites. The IT Army is organized through a Telegram channel where new Russian targets are listed for volunteers to attack'.

As well as holding specific individuals and organisations to ransom, industries including electricity, water, oil, medicine, and transport have been heavily targeted via supply chain attacks, in a bid to fully disrupt operations. With each party, and supporting delegations from both sides, attempting to ensure complete carnage, the impact on people, processes, and infrastructure has been severe.

'Cyber-attacks orchestrated by the GRU have attempted to undermine international sporting institution WADA, disrupt transport systems in Ukraine, destabilise democracies and target businesses.' – GCHQ

These geopolitical issues have completely changed the game because the affiliation between government and Quasi Government have now merged. Russia have given the go-ahead to target anyone who is an enemy of the state. GCHQ, NSA, CIA, are all targeted, but are equally well protected. Which means now attacks are filtering down to the smaller chains, the ones with less security in place, and it is open season. These attacks are not necessarily sophisticated, they are just well-resourced.

'It is believed that Russia will continue its aggression throughout 2023 and it is expected to target Eastern European companies, especially NATO countries. Supply chain attacks will be a continued avenue for Russian backed adversaries.' - **Aaron Hambleton, Director of Middle East & Africa, SecurityHQ.**

- Killnet is a pro-Russia threat group that has been active since at least January 2022. Killnet is known to target the websites of organisations in critical sectors with DDoS attacks, aiming to cause disruptions.
- NoName057(16) is one of the most active hacktivist groups targeting the Ukraine, observed to date. One of their translated posts, reads 'Today is a new day of regular victories on the cyber front! Victory is ours!'. This group are actively going after anything related to countries that fall into the grey zone between Russia and the rest of the world, and this information is publicly available. It's important to recognise that this is one of many extremely active hacktivist groups, and this is how they publish and take pride in their work.

3. China Favourites Exposed Network Devices

China's APT10 were very successful back in 2016, specifically when they targeted MSPs through operation Cloud Hopper. SecurityHQ predict that in 2023 these state sponsored groups will continue to go after exposed network devices because they are already public and exposed to the internet. Why would an APT go for endpoint when they know security controls, like [EDR](#), is deployed, when they can go for an exposed network device?

APT40 are known to adapt their approach based on their target. They don't apply 'one size fits all', which shows their capability and flexibility. APT40 are linked to the Peoples Republic of China, with espionage believed to be their prime motive.

Any industries of interest to the state, such as engineering or transport, that will further the development of the Chinese state, are targeted. In general, these groups are not formed to destroy or manipulate, but to collect and harvest information. China is seeing what is happening in Russia and are adapting their playbooks accordingly.

- Chinese Threat Actors continue to focus their efforts on exploiting Zero-Day vulnerabilities on internet facing devices.
- Chinese TA's prefer managed network devices.
- APT40 observed exploiting FortiOS Zero-Days early in 2023.
- [Storm-0558 attack Microsoft](#) using forged encryption keys to target Outlook.

Prevalent Chinese Threat Actors



Espionage Specialists



ChinaChopper



Data Exfiltration



Highly Targeted Operations



State Sponsored



Target Network Devices



Zero-Day Exploits



Keylogging Malware



LOL Techniques



Customised Backdoors



Adaptive Attacks

*Icons from flaticon.com

4. Iran Remains Destructive

Iranian threat actors are very well known for being destructive and disruptive.















Take APT35 as an example, they are attributed to the Islamic Revolutionary Guard (IRG), which is the political motivation to gather intelligence with a highly targeted approach. This group custom-make their malware. They are not reusing, they are not rebuying, they make each malware specific to their target. Which also means that it does not have a signature.

‘These are clever and time intensive campaigns. They are known for their destructive techniques, where they wipe systems using the Master Boot Record (MBR) wiper, and there is no coming back from that. Money is not the financial gain; they just want to cause damage.’ - **Aaron Hambleton, Director of Middle East & Africa, SecurityHQ.**

SecurityHQ predict that:

- Destructive and disruptive attacks will keep Iranian Threat Actors an elevated threat. They are trying desperately to increase their knowledge and their capability.
- Iranian Threat Actors will continue intelligence gathering activities to increase their presence, to be shown for having their capabilities, and to enforce the message that they are not to be messed with. They are not maybe as sophisticated as other geographies, but sophistication is not their goal. Their goal is to destroy if they must.
- Focus will likely remain on the Middle East for geo-political reasons. Recently this has put them back into the spotlight, but they work within the grey zone extensively, forming a narrative particularly against Israel. SecurityHQ have seen attacks targeting the Middle East, particular towards Jordan, Lebanon, and the UAE specifically.
- Government & telecommunication sectors remain prime targets.

Prevalent Iranian Threat Actors

	 Surveillance Operations	 Harvesting Tools
	 Screenshots	 Keystrokes / Clipboard
	 Attributed to IRGC	 Political Motivation
	 Custom Malware	 Time Intensive Campaigns
	 State Associated	 Time Intensive Campaigns
	 Destructive Attacks	

*Icons from flaticon.com

Recommendations To Enhance Cyber Security Posture – 6 Steps

1 Account Reconciliation

SecurityHQ typically see many highly privileged accounts in Active Directory, often used during attacks. Are accounts being reconciled? And when was the last time these were checked?

2 Asset Visibility

It needs to be clear what assets are, in order to protect them. Find those assets, run discovery scans, and put them into the vulnerability management cycle.

3 Vulnerability Detection

Initial access brokers are out there who specialise in weaponizing CVE's and using that to sell access to organised and much more sophisticated groups. Ask these questions...

- How quickly are vulnerabilities being detected?
 - Quicker detection time will make a major difference to your defence posture.
- How often are scans taking place? Every year, 6 months, 3 months, weekly?
 - How often scans are made, will impact visibility and, therefore, vulnerability.
- Can vulnerabilities be listed, to stay ahead of the curve?
 - Tweak vulnerability scanning cycle to help with that detection.

4 Threat Hunting

It is important to be proactive when it comes to detecting Indicators of Compromise (IOC's) and Indicators of Attack (IOA's). SecurityHQ know that adversaries are evolving their tactics, which means businesses need to be looking for things that they can assume have happened, even if they have not. Shift away from IOC's and look more towards Indicators of Attack or TTP's. Provide the hypothesis, and believe that a compromise has happened, even though it might not have been alerted.

Next Step: Read our white paper '[A Checklist for Effective Threat Hunting](#)' for more on this.

5 Threat Intelligence & Real-Time Detection & Response

With the increase of zero-day vulnerability exploitation, having threat intelligence and detection and response is no longer a strategy, it is a necessity. Businesses should have controls in place. Humans are a point of failure, no matter what tooling is used. If one member of the team falls for a crafty phishing scam, that is all it takes. The outcome of real-time detection and improved speed of response means responding to and blocking attacks before they have the chance to develop further. Response to a threat in rapid time, before it has the time to implement further actions, can mean the difference between a breach or securing assets in time. Reduce the time it takes to respond to threats, the greater chance at responding to the threat correctly, meaning a reduction in the chance of further escalations.

6 Preparedness

In a worst-case scenario, is it clear what steps to take? Have tabletop exercises been completed? Is it clear who needs to be in the room at the right time? Are incident response playbooks up to date with the right contacts and who should be called in? Businesses need to know this to be ready to respond to these inevitable threats. Education plays a large part in being prepared and educated.

Next Step: Download our webinar '[Tips to Educate and Protect Your Staff from Security Threats](#)'.

To learn more on this topic, download the SecurityHQ webinar recording of '[Global Threat Landscape 2023 Forecast](#)'.

About SecurityHQ

SecurityHQ's Threat Intelligence team is a cohesive global unit dedicated to Cyber Threat Intelligence. Our team is focused on researching emerging threats, tracking activities of threat actors, ransomware groups, and campaigns, to ensure that they stay ahead of potential risks.

Beyond their investigative work, the Intelligence team provides actionable threat intelligence and research, enriching the understanding of SecurityHQ's customers worldwide. United by a common commitment, the SecurityHQ Threat Intelligence team delivers the insights needed to confidently navigate the intricacies of the cyber security threat landscape.

To speak with an expert, get in contact.

How Does SecurityHQ Differ?

SecurityHQ is a Global MSSP, that detects, and responds to threats, instantly. As your security partner, we alert and act on threats for you. Gain access to an army of analysts that work with you, as an extension of your team, 24/7, 365 days a year. Receive tailored advice and full visibility to ensure peace of mind, with our Global Security Operation Centres, and utilize our award-winning security solutions, knowledge, people, and process capabilities, to accelerate business and reduce risk and overall security costs.

**Have a question?
We would love to
hear from you.**

Safeguard your business, people
and processes with SecurityHQ

Reach us

sales@securityhq.com | +44 20 332 70699



Americas	+1 312 544 0538
Asia	+91 72760 90836
Australia	+61 42026 7281
Europe	+44 20 332 70699
Middle East	+971 4354 9535
Africa / SADC	+27 10 157 0654