Cyberint

Impactful Intelligence

# CYBER SECURITY TRENDS FORECAST 2023

January 2023

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

2022 brought us many different stories throughout the cybercrime industry – new ransomware groups that emerged, veteran groups that disappeared, new techniques and tools, and much more.

The cybercrime industry is very dynamic and develops and morphs daily. As a result, new trends keep on emerging that demand us to be on top of things in order to keep our organizations safe and secure.

This report will focus on all the major and relevant security trends of 2022 that we can learn from, as well as what can we conclude and predict about how these threats could reveal themselves and change in 2023.

# SUPPLY CHAIN ATTACKS

Supply chain attacks were on the rise in 2022, and according to various studies, approx. over half of the SMBs and corporate that connected to third-party vendors were affected. The companies affected came from a variety of sectors such as automotive and IT providers, which led to shifts in both customers and business operation flow. Such attacks were able to affect even small, unknown businesses by virtue of their connections to larger companies.

Several supply chain attacks took place in 2022, Toyota's major supplier, Kojima Industries Corp, forcing Toyota to halt all Japan-based manufacturing temporarily as Toyota was directly impacted, even though the attack did not deploy inside their perimeter. Additional major supply chain incidents include Okta, the IT management service business that suffered from multiple breaches that affected customers in 2022 and possibly led to sensitive unauthorized access and multiple WordPress plugin infections, which impacted thousands of hundreds of websites.

The attackers realized quite quickly how to leverage remarkable supply chain attacks into making profits, as there are cases where we witnessed a lack of transparency between the victim and its partners and/or customers due to potential revenue loss. This kind of action leaves the partner/customer impacted by potential infections.

If an attacker is accesses a valuable supply chain provider, he will consider this a golden nugget and it will try to benefit from this attack to the largest extent possible. We predict that in 2023 attackers will continue to analyze the main supply chain's center of mass that may significantly impact multiple corporations in one single hit.

# RANSOMWARE INDUSTRY'S NEW AGE

Ransomware is a well-known threat across all industries.

The disappearance of veteran ransomware groups from last year, such as Conti and PYSA, left a void in the ransomware industry and cleared the stage for LockBit3.0 to take over – which they did.

During 2022, LockBit3.0 claimed roughly 900 victims, almost equal to both Conti and LockBit combined in 2021.

The ransomware industry introduced us to dozens of new groups this year. Fortunately, not all turned out to be successful, but even two to three groups are enough to inflict significant damage. This year we encountered BlackBasta, BianLian, YanLuowang and Royal, along with many others. These groups weren't able to take Conti's place of, but they did add a significant number of nearly 300 victims to their count this year. Once established, we believe they will be a direct challenger to LockBit3.0.

The current global financial state might also affect how ransomware groups operate in 2023. Given the fact that we seem to be headed for a recession in 2023, it is likely that some sectors will have a hard time earning the same revenues and profits of recent years.

As part of their reconnaissance phase, ransomware groups tend to assess how much ransom they can demand from their victims. The change in income in specific sectors due to the recession might change the victim's profile for some ransomware groups seeking to target one sector over the other.

Overall, 2023 might be a fascinating year for the ransomware industry. We are at a stage where we have numerous new groups looking to establish themselves and become a real challenge to LockBit3.0. In addition, we finally might have an answer to Conti's rebrand.

# VULNERABILITY EXPLOITATION

In the past year, we witnessed multiple long-lasting common vulnerabilities and exposures (CVEs), which impacted multiple worldwide organizations. Some of the CVEs impacted legacy products, and others exploited new technologies and procedures implemented in the eco-system.

One new and important feature introduced in mid-2022 by Microsoft is the Mark-of-the-Web (MotW). MotW is a security feature originally provided to force saved webpages to run in the security zone of the location the page was saved from. Multiple vulnerabilities related to the mechanism were reported and patching has been released through Microsoft's Patch Tuesday and free services such as the 0patch platform to address an actively that exploits the zero-day flaw. MotW is valuable, but fragile.

**The most exploited vulnerabilities in 2022 include:**

- Follina (CVE-2022-30190)
- ProxyLogon (CVE-2021-26855)
- Log4Shell (CVE-2021-44228)
- Spring4Shell (CVE-2022-22965)
- F5 BIG-IP (CVE-2022-1388)
- Google Chrome zero-day (CVE-2022-0609)
- Mark-of-the-Web Bypass Vulnerability (CVE-2022-41091)

As mentioned above, two of the most impactful CVEs in 2022 were reported in 2021. In general, sometimes it takes time for CVEs to accelerate: In some cases it depends on the exploit availability and in others, it derives from the maturity of the exploitation. This fact demonstrates how valuable and critical it is to keep track of CVE evolution over time, in particular the CVE that impacts organizational assets.

As reporting and disclosure of CVE numbers steadily increase each year, it seems that the process is becoming mainstream, and companies are adapting to utilize this data for the benefit of their environments. Cyberint predicts that in 2023 the trend will continue growing and more CVEs will be reported, and supply chain vulnerabilities will continue to have the most severe and long-range impacts on cross-sector companies worldwide.

# CLOUD SERVICES

In the last few years, cloud services have become mainstream. As more organizations migrate their operations to the cloud, and more companies are "born in the cloud", it has become increasingly important to ensure that cloud environments are secure and compliant with industry standards and regulations. This involves implementing a variety of measures such as access controls, network security, and vulnerability management. It also requires staying up to date with the latest threats and adopting best practices for cloud security.

Companies migrating to the cloud should consider the "Shared responsibility model". The fact that cloud vendors claim they offer secure architectures might not be enough, and securing every system is the responsibility of both the customer and the cloud vendor.

Looking back at 2022, several high-profile cloud-related security incidents made headlines, highlighting the risks organizations face when adopting cloud technologies. For example, BlueBleed, which went public last October, holds sensitive data of more than 65,000 entities in over 110 countries, cause a huge industry hype, and was due to a misconfigured Azure Blob Storage buckets. Another incident involving Microsoft was the extortion group Lapsus$'s hacking of Microsoft's Azure DevOps server and theft 37 GB of data. The data was mainly related to source code for the various internal Microsoft projects, including Bing, Bing Maps, and Cortana. Another example is Pegasus Airlines, a low-cost Turkish airline, which suffered a data breach that exposed 6.5TB of sensitive data, due to misconfigured AWS S3 bucket.

As the industry keeps on adjusting itself to the cloud reality, so do the threats and opportunities. Most of the cloud breaches we have already seen usually come down to misconfigurations, overly permissive permissions, or unprotected public-facing servers or storage services.

Looking at 2023, it's very plausible that more such threats will arise, as both the industry shifts to the cloud and the threat actors' understanding of "where" to look for the more critical and exciting finds increases, as threat actors become more sophisticated.

# THREAT ACTORS ARE THINKING OUTSIDE OF THE BOX

## CYBERCRIMINALS TAKING POLITICAL SIDES

We are mainly used to seeing hacktivists taking sides and committing malicious acts in areas of the world with political conflicts. During 2022, and especially after the Russia-Ukraine conflict began, we started seeing more threat groups of different types, such as DDoS actors, ransomware groups and data leakage groups, taking sides.

As more and more groups are moving on from the "it's all about the business" position and taking action against what they believe to be wrong, we can only assume that more groups will take matters into their own hands as they target entities of different countries worldwide. We already saw this in 2022 when almost every threat group took sides in the Russia-Ukraine conflict and when the riots in Iran began.

The trend of different threat groups standing up for "what's right" is on the rise, although the reason is not necessarily their goodwill. These groups try to justify their actions and draw a different picture in which the victim is the real enemy, possibly to just gain good PR.

While we hope that the war in Ukraine will come to a resolution as soon as possible, these events might compel more and more underground and criminal threat groups of all kinds to act.

## OT ATTACKS

The operational technology attacks, which previously were the purview of big threat actors/APTs due to the possible complexity and harsh impact they might have, spread into hacktivist operations in 2022, which significant raised the hacktivist bar.

Operational Technology (OT) systems are found in critical infrastructure environments and prioritize product or service availability and human safety. Cyberattacks on OTs have been on the rise, with almost all kinds of OT organizations experiencing a side-effect of breaches in the past year. Gartner predicts that by 2025, cyber attackers will weaponize OT environments to harm or kill humans.

Throughout 2022, over half of global cybersecurity incidents affecting organizations with operational technology (OT) systems resulted in outages that put physical safety at risk. The IT network attack remains the main infection vector for incidents against OT-related industries.

The two main sectors targeted are transportation and discrete manufacturing. Once again, this year ransomware was used in almost all attacks. There were two notable hacktivist attacks: In Belarus, they stopped trains in three cities, and in Iran, they set a steel mill on fire.

Following the abovementioned 2022 OT review alongside the recent "mainstreaming" of OT attacks in the attack landscape, we expect to see an increase in this attack vector as a part in both attacking IT to access OT and solely OT endpoint attacks in 2023.

## HEALTHCARE IS A LEGIT VICTIM

Ever since 2020, when the ransomware industry really took off, there was consensus that the healthcare sector will never be targeted. At first, we could see many threat groups and ransomware groups maintaining their moral standards. However, in 2022 we witnessed a shift as more and more threat groups launched campaigns against healthcare organizations.

Last year we witnessed 239 data breach cases targeting the healthcare sector, while in 2022 we saw the victim count grow to 482, a massive increase of 202%.

When it comes to the ransomware industry in particular, we might see more groups targeting this sector in 2023, given the fact that this sector was already "normalized" and now acts as a "legitimate" sector to target. In addition, a successful campaign in the health sector might be rewarded with a huge ransom given the fact that the leverage on the victim is huge due to the lives at stake.

# INFO STEALERS

Info Stealers are malware that gathers data from an infected computer and sends it to the attacker. They became more common in early 2021, with a substantial increase in 2022. As new info stealers occasionally emerge, a handful such as Redline, RaccoonV2, Vidar, BlackGuard and Mars, top the charts.

A few of the active stealers were updated with a new capability - fetching data from Telegram and Fileless data exfiltration. Before exfiltration, the first version saved stolen data on disk. After stealing the data, the new version sent it directly. Alongside the improvements of capabilities we can see also some improvements in the encoding and encrypting methods.

The best-selling stealer is Redline. RedLine Stealer is malware available on underground forums for sale. Its delivery methods are maintained and it exploits new vulnerabilities such as the Chrome V8 JavaScript and WebAssembly engine vulnerability (CVE-2022-1096, CVSS 9.1). It helps operators **breach organizations and individuals**. The stealer spreads through malicious spam emails, third-party loaders, and fake Windows updates.

Another info stealer, BlackGuard, first appeared in March 2021 and several versions have been released since then. It was offered for rent for $200 a month, but the operators announced they were suspending the project due to the loss of their developer during Russia's invasion of Ukraine.

Although we did not witness any outstanding new development in 2022, info stealers have maintained their agility in terms of delivery and exfiltration data and are highly profitable to the attacker. We assume that the infection volume will keep steadily increasing until a new player appears and puts a spoke in the stealer wheel. Cyberint recommends enabling MFA in all accounts related to prevent account takeovers.

# AI CYBERCRIME


As AI became an integral part of our lives in many ways, so did the relationship between AI and cybercrime.

Towards the end of 2022, we witnessed a truly remarkable tool named ChatGPT by OpenAI. This service provided enhanced AI capabilities in the form of a chat where users can ask certain questions or make certain requests, and the ChatGPT will reply with an AI-based answer.

While most users asked ChatGPT to write rap songs or recommend great movies, some threat actors looked to utilize this tool for creating exploit kits, backdoors, reverse engineering pieces of software and much more.

Although the AI technology that wrote these tools cannot replace the work of a skilled developer or researcher, it might herald the start of a new era in two main ways: The first is that the entry-level required for threat actors to get into the cybercrime industry might be lower now that there is a tool that can write basic hacking tools. The second is that giving this technology to skilled threat actors might significantly shorten their developing time, searching for bugs and vulnerabilities and improving their current tools and products.

It was only a matter of time before artificial technology entered the cybercrime industry and today we are witnessing one of the first implementations and uses of AI by threat actors. It is highly likely that during 2023 we might see several innovations and shortened times between new malware variants given this technology.

Cyberint

# CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

## ISRAEL
Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

## UNITED KINGDOM
Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

## USA – TX
Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

## SINGAPORE
Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

## USA - MA
Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

## JAPAN
Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

## ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.