ADVANTIO

2022 Threat Reports

Insights that all companies need to consider in 2023

Giorgio di Grazia

December 2022

Threat reports are important for the industry because they provide valuable information about the threat landscape as it evolves. By regularly reviewing this information, companies can gain a better understanding of the security risks they face and develop more effective security measures and strategies.

Threat reports are typically related to the collection and analysis phases of the **threat intelligence lifecycle**:

1. In the **collection** phase, threat reports are one of the sources of information that can be used to gather information about potential security threats and vulnerabilities.
2. In the **analysis** phase, threat reports are often used as a source of information that can be analyzed to identify potential threats and understand their implications.

Together, these two phases form the foundation of the threat intelligence lifecycle (which also includes dissemination and continuous improvement phases) and threat reports are an important source of information that can be used to support this work.

Types of Threat Report

There are several different types of threat intelligence, and the specific type that is most appropriate for an organization will depend on its needs. The information can be used as a source of **strategic**, **tactical** and **operational** threat intelligence.

Stakeholders can be different, from SOC analysts focused on techniques or TTPs to the CISO who need to understand security trends and develop a **threat-informed defence**.

Security teams should regularly review different kinds of threat reports to keep constantly up to date with emerging threats and provide situational awareness.

Classification of Threat reports

Some common ways to classify threat reports include:

- **By target industry**: The industry or sectors that are most likely to be targeted by the threats discussed in the report (e.g., healthcare industry, manufacturing, financial sector, etc.).
- **By attack vector**: The methods that attackers use to deliver their payloads (phishing, social engineering, ransomware, etc.).
- **By geography**: The geographic regions where the threats discussed in the report are most likely to be encountered.
- **By threat actor**: Threat reports can be classified based on the groups or individuals that are most likely to be behind the threats discussed in the report (e.g., nation-state actors, organized crime groups, hacktivists, etc.).

Gaining Value from Threat Reports

Some specific ways that organizations can use vendor threat reports include:

- **Identifying potential threats**: By reviewing threat reports, organizations can identify potential security threats that they may not have been aware of previously. This can help them to stay ahead of potential attacks and better protect their systems and data. Additionally, threat reports often provide detailed analysis of the potential impacts of specific threats. This can help organizations to develop more effective strategies for mitigating or neutralizing them.
- **Tracking the development of threats**: Threat reports can also be used to track the development of specific threats over time. This can help organizations to respond quickly and effectively to new threats as they emerge.

- **Demonstrating commitment to cybersecurity**: By using vendor threat reports as part of their security efforts, organizations can demonstrate their commitment to cybersecurity to regulators and customers. For example, **ISO 27002:2022** added a new control (**5.7**) that specifically requires the collection and analysis of information relating to security threats to produce meaningful threat intelligence.

Industry Threat Reports of Note from 2022

The following is a non-exhaustive list of the main threat reports published in 2022, listed in order of publish date. It also contains a very brief overview of key trends provided in the report.

Please note that most 2022 reports refer to events and information related to 2021.

These reports provide detailed information about the latest threats and vulnerabilities, as well as insights into trends and patterns in malicious activity. A good cyber threat report can be an invaluable resource for organizations that want to understand and protect against potential security threats.

By regularly reviewing and analyzing threat reports, organizations can gain a better understanding of the security risks they face, and can use this actionable information to inform their security strategy and decision-making. In this way, cyber threat reports can be an essential component of an organization's security efforts, and should be regularly reviewed and analyzed to ensure that the organization is adequately informed and protected.

The Global Risks Report 2022

The World Economic Forum (WEF)
January 2022

- The digitalization of physical supply chains creates new vulnerabilities because those supply chains rely on technology providers and other third parties.
- The growth of deepfakes and "disinformation-for-hire" is likely to deepen mistrust between societies, business and government. For example, deepfakes could be used to sway elections or political outcomes.
- As environmental, social and governance (ESG) concerns come increasingly into focus, businesses that fail to demonstrate strong corporate governance around cybersecurity (e.g., in the event of a breach) could suffer reputational harm in the eyes of ESG-focused investors.

2022 Global Threat Report

CrowdStrike
February 2022

- In the hacktivist landscape, CrowdStrike Intelligence observed the continued development of grassroots operations and a proliferation of established hacktivist groups across the world.
- In 2021, targeted intrusion adversaries continued to adapt to the changing operational opportunities and strategic requirements of technology and world events. Russian, Chinese, Iranian and North Korean adversaries were all observed employing new tradecraft or target-scopes meant to respond to global trends.
- The analysis of the breakout time for hands-on eCrime intrusion activity in 2021 revealed an average of just 1 hour 38 minutes.
- Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Attackers have been observed using legitimate credentials and built-in tools (an approach known as "living off the land") in a deliberate effort to evade detection by legacy antivirus products.

Threat Intelligence Index 2022

IBM Security X-Force
February 2022

- Vulnerability exploitation was the top initial attack vector in manufacturing, an industry grappling with the effects of supply chain pressures and delays.
- Manufacturing replaced financial services as the top attacked industry in 2021, representing 23.2% of the attacks X-Force remediated last year. Ransomware was the top attack type, accounting for 23% of attacks on manufacturing companies.
- Phishing operations emerged as the top pathway to compromise in 2021, with 41% of incidents X-Force remediated using this technique to gain initial access.

- The click rate for the average targeted phishing campaign was 17.8%, but targeted phishing campaigns that added phone calls (vishing or voice phishing) were three times more effective, netting a click from 53.2% of victims.
- X-Force closely tracked how cybercriminals are using phishing kits throughout 2021, and their research revealed that Microsoft, Apple and Google were the top three brands criminals attempted to mimic.
- Suspected Iranian nation-state threat actor ITG17 (MuddyWater), cybercriminal group ITG23 (Trickbot), and Hive0109 (LemonDuck) were some of the most active threat groups X-Force intelligence analysts observed in 2021.
- Four out of the top five vulnerabilities exploited in 2021 were new vulnerabilities, including the Log4j vulnerability CVE-2021-44228—which was ranked number two, despite only being disclosed in December.

2022 Threat Report

BlackBerry
February 2022

- Threat actors: Many have learned to adopt and mimic private sector capabilities by using service providers such as ransomware-as-a-service (RaaS), infrastructure-as-a-service (IaaS), and malware-as-a-service (MaaS) to leverage malicious attacks. Others have created a layer of obfuscation between themselves and their targets by using IABs and impersonating other threat groups.
- Progress was made on integrating security into connected vehicles with the International Organization for Standardization (ISO), the Society of Automotive Engineers (SAE), and the United Nations (UN) providing firm guidance to automakers.
- When it comes to cyberattacks, there is zero immunity. However, there are a number of cybersecurity innovations and approaches offering stronger protection to organizations (e.g., Zero Trust framework, managed services, etc.).

2022 Ransomware Threat Report

Unit 42 (Palo Alto)
March 2022

- Ransoms (both demands and payments) continue to go up. Among the incident response cases reviewed by Unit 42 in 2021, which were predominantly in the U.S., the average ransom demanded was approximately $2.2 million.
- Multi-extortion techniques where attackers not only encrypt the files of an organization, but also name and shame their victims and/or threaten to launch additional attacks are increasingly part of ransomware tactics.
- These criminal entrepreneurs offer ransomware as a service (RaaS) to other criminals, establishing agreements that set the terms for providing actual ransomware to these affiliates, in exchange for a monthly fee or a percentage of ransoms paid.

Internet Crime Report 2021

The Federal Bureau of Investigation (FBI)
March 2022

- Business Email Compromise (BEC): The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds (with adjusted losses at nearly $2.4 billion).
- Confidence Fraud/Romance scams encompass those designed to pull on a victim’s “heartstrings.” ($956 million in losses). Romance scams occur when a criminal adopts a fake online identity to gain a victim’s affection and confidence.
- In 2021, the FBI IC3 received 34,202 complaints involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. It is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim.

2022 Threat Detection Report

Red Canary
March 2022

- Ransomware continued to dominate the 2021 threat landscape, and Red Canary observed operators taking new approaches.
- Supply chain compromises were a major theme, starting with SolarWinds, Kaseya and Node Package Manager (NPM) package compromises mid-year, and ending with Log4j.
- Adversaries exploited vulnerabilities affecting popular enterprise platforms to drop web

shells, spread ransomware, and more (e.g., ProxyLogon, ProxyShell, PrintNightmare, Kaseya VSA)

- The threat landscape continued its trend toward a software- as-a-service (SaaS) economy, muddying the already murky waters of attribution.
- Malicious installers led to rotten Apples and adware, as macOS systems continued to be targeted.
- Adversaries continued to use and abuse legitimate remote monitoring and management (RMM) software to move data and control infected hosts.

M-Trends 2022

Mandiant
April 2022

- Mandiant observed a high volume of compromises attributed to vulnerabilities and misconfigurations in on-premises Active Directory and cloud-based infrastructures, resulting in an expanded attack surface for successful privilege escalation and both lateral and vertical movement by attackers.
- Exploits remained the most frequently identified initial infection vector. In 37% of intrusions, attackers leveraged exploits to gain access. Supply chain compromise was the second most prevalent initial infection vector, accounting for 17% of intrusions with an identified vector.
- Financial gain: three out of ten intrusions stemmed from attackers seeking monetary gain through methods such as extortion, ransom, payment card theft and illicit transfers.

Data Breach Investigations Report

Verizon
May 2022

- Most breaches (82%) involved a human Element. Social engineering was implicated in 20% of breaches. About two-thirds of breaches involved phishing, stolen credentials and/or ransomware.
- Over half of breaches involved the use of either remote access or web applications. The vast majority of breaches (95%) had five or fewer steps. The four key paths to data breaches are: credentials, phishing, exploiting vulnerabilities and botnets.
- Almost four out of five breaches were attributable to organized crime. The number-one motive was financial gain. The number-two motive was espionage.
- Ransomware has continued its upward trend with an almost 13% increase (for a total of 25% of breaches).
- Supply chain was involved in 61% of incidents this year. Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, nation-state threat actors may skip the breach altogether and opt to simply leverage the access.
- Error continues to be a dominant trend and is responsible for 14% of breaches.

Cost of a Data Breach Report 2022

IBM Security (with Ponemon Institute)
July 2022

- Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report.
- 83% of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach.
- 60% of organizations studied stated that they increased the price of their services or products because of the data breach.
- The average cost of a data breach for critical infrastructure organizations studied was USD 4.82 million — USD 1 million more than the average cost for organizations in other industries. 28% experienced a destructive or ransomware attack, while 17% experienced a breach because of a business partner being compromised.
- 11% of breaches in the study were ransomware attacks.
- Use of stolen or compromised credentials remains the most common cause of a data breach (19%).
- 45% of breaches in the study occurred in the cloud.
- The top five countries and regions for the highest average cost of a data breach were the United States at USD 9.44 million, the Middle East at USD 7.46 million, Canada at

USD 5.64 million, the United Kingdom at USD 5.05 million and Germany at USD 4.85 million.

- 304 days was the average time to identify and contain a data breach.

NFTs and Financial Crime

Elliptic
August 2022

- Over $8 million of illicit funds has been laundered through non-fungible token (NFT) based platforms since 2017 – representing 0.02% of trading activity originating from known sources.
- Over $100 million worth of NFTs were publicly reported as stolen through scams between July 2021 and July 2022, netting perpetrators $300,000 per scam on average. July 2022 saw over 4,600 NFTs stolen – the highest month on record – indicating that scams have not abated despite the crypto bear market.
- Tornado Cash, a US-sanctioned mixer, was the source of $137.6 million of cryptoassets processed by NFT marketplaces and the laundering tool of choice for 52% of NFT scam proceeds before being sanctioned by OFAC in August 2022. Its prolific use by threat actors engaging with NFTs further emphasizes the need for effective sanctions screening by NFT platforms.
- Social media compromises – particularly of NFT project Discord servers – have surged in 2022, accounting for 23% of all NFTs (close to 5,000, worth around $20 million) stolen this year. The growing availability of tailored malware that can bypass multi-factor authentication is likely to be partially responsible.

Digital Defense Report 2022

Microsoft
November 2022

- Cybercrime continues to rise as the industrialization of the cybercrime economy lowers the skill barrier to entry by providing greater access to tools and infrastructure.
- The threat of ransomware and extortion is becoming more audacious with attacks targeting governments, businesses, and critical infrastructure.
- Attackers increasingly threaten to disclose sensitive data to encourage ransom payments.
- Human operated ransomware is most prevalent, as one-third of targets are successfully compromised by criminals using these attacks and 5% of those are ransomed.
- The most effective defense against ransomware includes multifactor authentication, frequent security patches, and Zero Trust principles across network architecture.
- Credential phishing schemes which indiscriminately target all inboxes are on the rise and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises.
- Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities. The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict. IT supply chain being used as a gateway to access targets. Identification and rapid exploitation of unpatched vulnerabilities has become a key tactic. Rapid deployment of security updates is key to defense.
- Attackers are increasingly leveraging vulnerabilities in IoT device firmware to infiltrate corporate networks and launch devastating attacks. 32% of firmware images analyzed contained at least 10 known critical vulnerabilities.
- Cyber influence operations are becoming increasingly sophisticated as more governments and nation states are using these operations to shape opinion, discredit adversaries, and promote discord.

ENISA Threat Landscape (ETL) 2022

ENISA
November 2022

- 60% of affected organizations may have paid ransom demands.
- Phishing remains a popular technique but we see new forms of phishing arising such as spear-phishing, whaling, smishing and vishing.
- Significant rise on attacks against availability, particularly DDoS, with the ongoing war being the main reason behind such attacks. Largest Denial of Service (DDoS) attack ever was launched in Europe in July 2022 (Prolexic platform; the victim is an Akamai customer in Eastern Europe); Internet: destruction of

infrastructure, outages and rerouting of internet traffic.

- Escalating AI-enabled disinformation, deepfakes and disinformation-as-a-service.
- Cybercriminals exhibit increasing capability and interest in supply chain attack: Third-party incidents account for 17% of the intrusions in 2021 compared to less than 1% in 2020.
- Managed Service Providers (MSPs) have also been increasingly targeted by ransomware threat groups (as well as state-sponsored groups) due to their trusted network connectivity and privileged access to their customers. In May 2022, the cybersecurity authorities of the United Kingdom, Australia, Canada, New Zealand and the United States released an alert informing organizations about the cyber threats to MSPs and their customers.
- In 2021, there were 66 disclosures of zero-day vulnerabilities observed. Moreover, the number of disclosed vulnerabilities is growing yearly, together with the growing number of proof-of-concept exploits. Cybercriminals jump on the disclosure of vulnerabilities to find additional weaknesses, weaponize them, and exploit them in the wild.
- Widespread cloud adoption provides attack opportunities for cybercriminals.
- Cybercriminals continue to disrupt the industrial sector.
- Data exfiltration and extortion without the use of ransomware. Ransomware gangs cited victims' cyber insurance policies during the negotiation phase. Prominent groups that conduct such activities are LAPSUS$ (also known as DEV-0537) and Karakurt.
- Nearly 50% of threats target the following categories; public administration and governments (24%), digital service providers (13%) and the general public (12%) while the other half is shared by all other sectors of the economy.