Global Threat Landscape Report 2021-2022

CloudSEK TRIAD Team

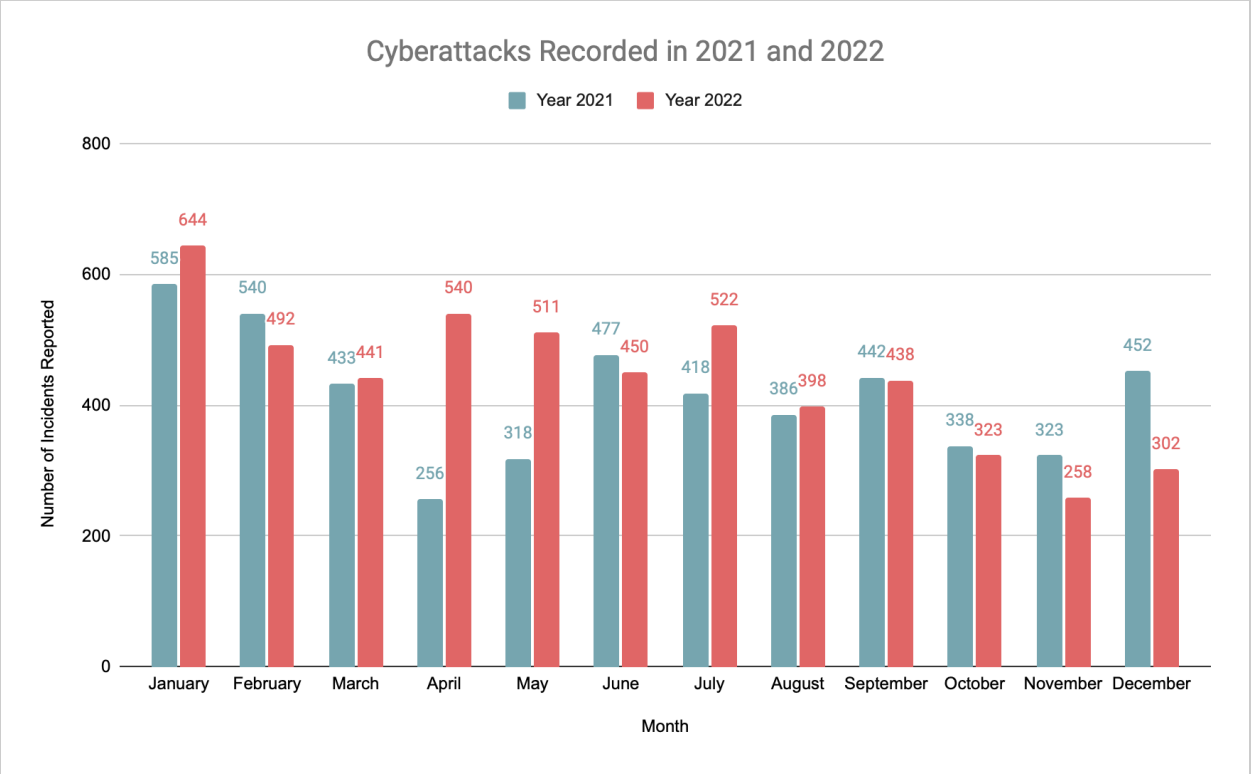
CloudSEK

Table of Contents

Overview of the Global Threat Landscape

The changing landscape of business with ubiquitous connectivity is not one devoid of threats. The heralding of the new era of hyperconnected systems carries the risk of threats looming large on the horizon. The threat landscape continues to unravel newer and more sophisticated threats to its ever-growing knowledge base. Research shows that mounting losses to cyber threats are poised to touch USD 10.5 trillion by 2025.

These overwhelming numbers tell a story of the unparalleled level of techniques, tactics, and procedures (TTPs) being employed by the new age threat actors, as well as their two primary objectives, which are to "adapt" and "persevere." The year 2021 to 2022 has seen a slew of attacks that are not only coordinated but highly sophisticated.



In this report, we have provided an overview of the major trends* observed in the global threat landscape and their correspondence with the trends in 2021. While 2021 saw a rise in initial access brokers and vulnerability exploits, 2022 witnessed a significant rise in hacktivism and cyber warfare.

***Note: The insights and distribution of threats by region are contingent on the presence of our clients in those regions.**

Latest Trends in Cyber Threats

XVigil's Underground Intelligence module records and reports the ongoing criminal activity from various underground forums. The data collected in 2021 and 2022 contained some very interesting patterns in the activity of threat actors. CloudSEK's TRIAD was able to identify the following drastic changes in the recorded patterns.

Russia Ukraine War

Russia's war on Ukraine has prompted a series of state-sponsored cyberattacks. There were instances of financially motivated attacks on Ukrainian entities and simultaneous backfires targeting the Russian government. Many threat actor groups aligned with either of the countries in the subsequent period. Russia and Ukraine's cyber rivalry eventually paved the way for a gradual increase in hacktivism activity, and numerous new hacktivist groups appeared in 2022.

Rise of Hacktivism

There have been 29 instances of hacktivist activity from 14 June to 30 September 2022. Of the total 1,731 instances from June to September, 2% have been hacktivist attacks under the following campaigns:

- **#OpIndia and #OpsPatuk**
  A pro-Palestinian Malaysian hacktivist group, DragonForce, made a global appeal to all Muslim brethren to attack Indian entities triggered by controversial comments on Prophet Mohammed by some Indian politicians. The group launched two similar campaigns named OpIndia and OpsPatuk for the same and was aided in this effort by 11 other hacktivist groups.
- **#OpIran**
  The threat actor group named 'Anonymous' launched OpIran against Iran due to the ongoing crackdown on dissent after Mahsa Amini's death. The protests began after the death of Mahsa Amini from Saqqez in Kurdistan province after her arrest by Iran's morality police for failure to follow government-mandated forms of the Hijab.
- **#OpIsrael**
  The OpIsrael is an annual campaign originally launched in 2013, by the 'Anonymous' hacker group, on the eve of Holocaust Remembrance Day. The campaign was later joined by other threat groups including GhostSec who mentions their motivation behind joining this campaign as to "condemn the merciless attacks upon Palestinian civilians".

- **#OpIndonesia**
  A campaign of web defacement targeting Indonesian entities. The motivation behind the breach is the lack of security measures enforced by the Government, thus putting the privacy of Indonesian citizens at risk. More than a dozen hacktivist groups were seen making posts on data breaches under this campaign.

Electric Vehicles Emerge as a New Target

Electric vehicles are becoming more common, but their charging stations are vulnerable to security flaws and cyberattacks. Addressing these vulnerabilities is critical to smart grid security. Energy and information technology advancements are changing the way EVs generate, manage, store, and consume energy. This also raises the stakes of prospective cyber-attacks. The recent API vulnerabilities found in various electric vehicles highlight the increasing risk of cyberattacks the industry faces.

Increased Attacks on Energy, Oil & Natural Gas

The energy sector is vital to society because it connects all important infrastructural sectors. Because energy technology was not designed with digital transformation in mind, outdated equipment used in power generation and delivery plants are frequently unable to be upgraded or patched. 2022 witnessed a surge in cyberattacks targeting this particular sector globally. A majority of these attacks were reported in USA, France, and Brazil, while Russia recorded only one such incident despite the fact that Russia is a major player in the global energy sector. A cyber attack on energy would result in the loss of electricity, gas, and oil, ultimately rendering emergency services and communication networks inoperable.

Abysmal State of Critical Infrastructure

The consequences of cyberattacks on essential infrastructure are not simply uncomfortable, but can even be fatal. Power generation and distribution, for example, are growing more complex and reliant on networks of linked devices. Power grids and other critical infrastructure were once operated in isolation. They are now much more integrated, geographically and across sectors, making critical infrastructure vulnerability to cyber-attacks and technical failures a major worry.

The energy sector is one of the most common targets of cyber-attacks on vital infrastructure, but it is far from alone. Transportation, government services, telecommunications, and essential manufacturing industries are also at risk. The latest unrelenting bombardment of cyber attacks on healthcare institutions is causing significant financial harm as healthcare systems attempt to reduce the costs of data breaches.

Increased Exploitation of Security Cameras

The ease of exploitation of vulnerable IoT infrastructure has resulted in a widespread increase in cybercriminals targeting security cameras. This increase was mainly assisted by vulnerabilities and other security weaknesses in CCTV camera designs. A few prominent incidents observed under this category include:

- A vulnerability identified as CVE-2022-30563 in the Dahua IP Camera allowed full Access to over 100 Dahua CCTV cameras worldwide.
- Access to 1.4 k Iranian Hikvision Cameras Compromised Under #OpIran Campaign
- Over 80,000 Hikvision cameras have been revealed to be vulnerable to a serious command injection bug that may be readily exploited via specially designed messages delivered to the vulnerable web server.

Vulnerabilities in the Spotlight

Exploiting vulnerabilities remain one of the favored attack vectors of cybercriminals. Two of the most discussed vulnerabilities of 2022 are:

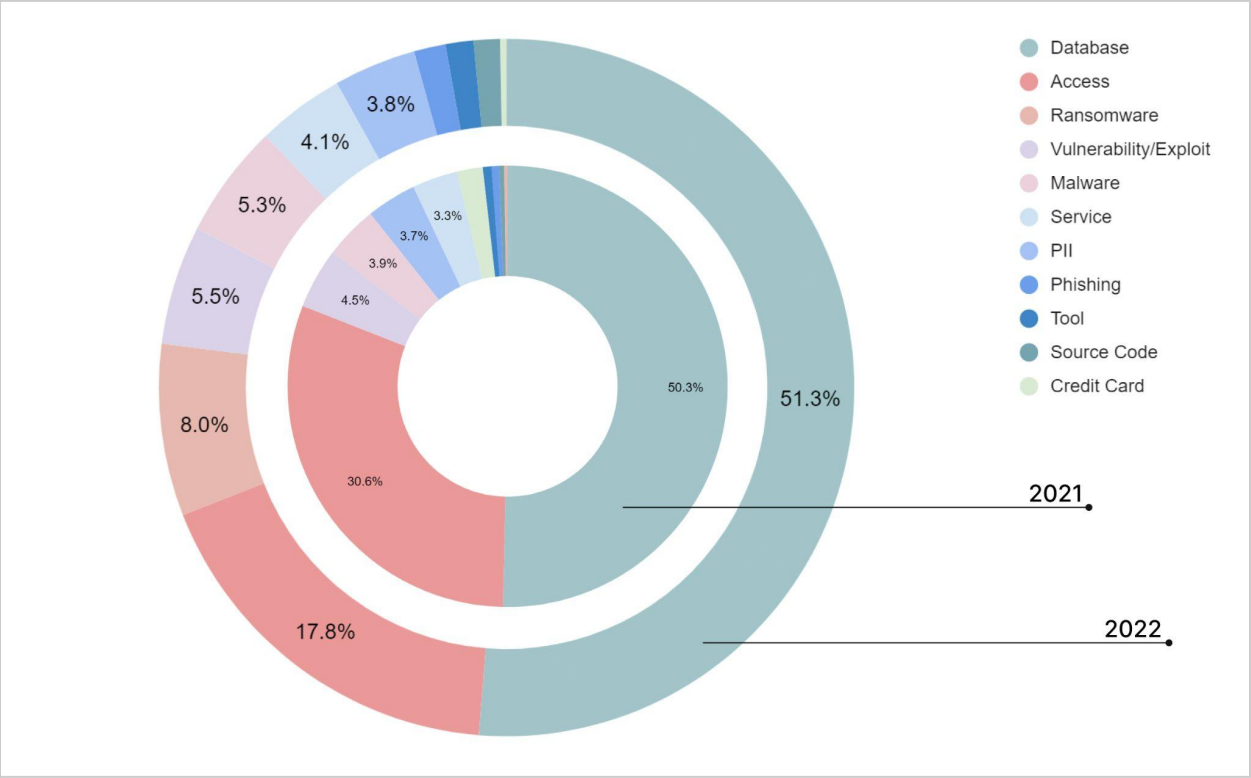
- **Log4j**
  Although the Log4j vulnerability was disclosed in December 2021, the Log4Shell (CVE-2021-44228) remote code execution vulnerability continues to be exploited in 2022 as well. Apache Log4j is a Java-based logging utility that is one of the most widely used pieces of open-source software for logging Java applications. A critical vulnerability (CVE-2021-44228) impacting multiple versions of Apache Log4j 2, was disclosed on 9th December 2021. This vulnerability affected the open-source logging framework Log4j, versions 2.0 to 2.14.1, used across the verticals.
- **ProxyLogon**
  Proxylogon is a chain of vulnerabilities (CVE-26855/26857/26858/27065) that are actively exploited in the wild by ransomware gangs and nation-state actors. They intend to compromise internet-facing Exchange instances to gain a foothold in the target network. The threat actor authenticates user access to the Exchange server by exploiting CVE-2021-26855. Followed by this, they write webshells/malware to the vulnerable server, which allows the attacker to exploit any of the listed flaws, CVE-26857/26858/27065, leading to an RCE attack.

Rise of Malware

Malware-related incidents have been reported to account for 5.28% of all instances in 2022, which is an increase from 3.9% in 2021. A wide range of malware was used, the most common of which were stealers, ransomwares, RATs, loaders, etc. Pegasus spyware, which was extensively used to target politicians and other significant figures, also gained popularity in 2021.

- **Commercial Stealers: Mars, Redline, Raccoon v2/v1, Jester, Vidar.**
  Stealers are still a major threat, with all the stolen data being sold in bulk on cybercrime markets.
- **Rats and Loaders: Smoke loader, Agent Tesla (RAT)**
  When it comes to loaders, less sophisticated adversaries (initial access brokers/APTs with lesser capabilities) use commercial loaders and RATs to carry out operations. Much more capable actors come equipped with complex malware which don't have any names, and are not publicly documented. One documented loader is the GuLoader.
- **Modified Open Source Softwares**
  Threat actors were seen using forks or modifications of decent and capable open-source malware projects to target innocent users. This technique was commonly used to target gaming apps, communication apps, browsers, crypto wallets, etc.
- **Pegasus Spyware**
  Pegasus spyware, produced by the Israeli cyber-arms firm NSO group, is a malware that can be installed discreetly on mobile phones running most versions of iOS and Android. Pegasus was developed as a program to "prevent crime and terror activities" and was meant to be sold only to the governments it had vetted and for approved purposes such as tracking down terrorists or criminals who abuse children. As of right now, Pegasus is still a very dangerous spyware.
- **Ransomware**
  Rapid increase in ransomware attacks can be attributed to the persistent activity of various ransomware groups such as LockBIT, Conti, and Hive. Almost all ransomware groups now follow the method of double extortion, wherein if the ransom is not paid, the data is leaked.

Commonly Employed Attack Vectors



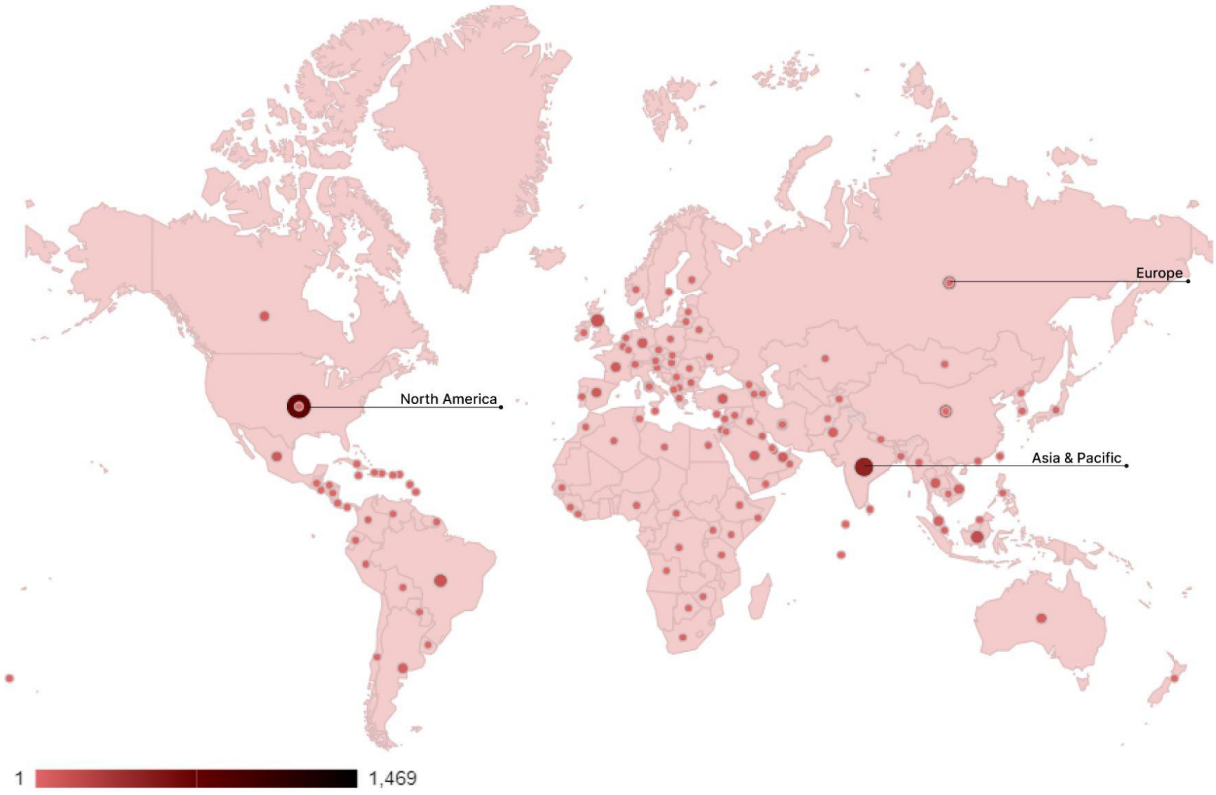
Graph depicting the major cyber threats as seen in 2021 and 2022

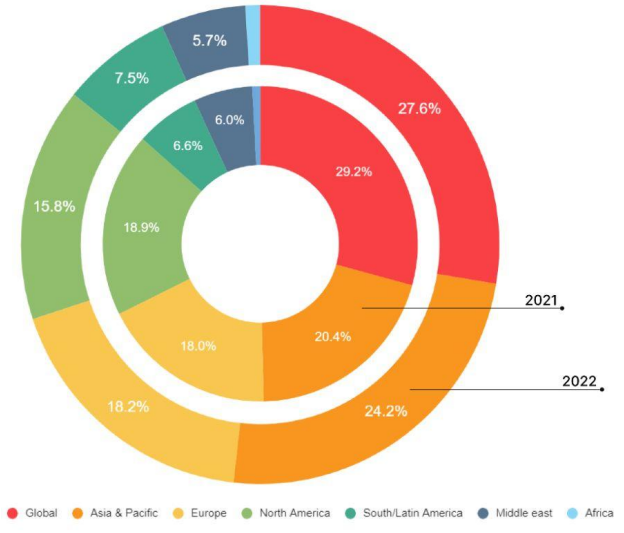
- **Database and access** were predictably the most targeted data types in both 2021 and 2022. The percentage of attacks targeting databases remained nearly the same in both years (≈50%), however, the percentage of attacks involving access dropped from 30.6% to 17.8%. Credential exposure, possibly by weak passwords and password reuse, serves as a gateway for initial attacker access and spread.
- **Ransomware** attacks increased drastically, going from the least common (0.3%) in 2021 to the third most common (8.0%) in 2022. Many new ransomware operators emerged in 2022, while some prominent ransomware groups launched their new versions (such as LockBIT 3.0). RaaS or Ransomware as a Service models also gained popularity and were used extensively in the Russia-Ukraine war.
- Attacks exploiting vulnerabilities maintained a significant presence, with 4.5% of the total attacks in 2021 and 5.5% of the total attacks in 2022.
- Attacks involving malware, PII records, phishing scams, credit card frauds, and various service models (RaaS, MaaS, etc.) were also prominent.

Favored Territories of Cybercriminals

XVigil data shows that North America, Asia & Pacific, and Europe remained the most targeted regions in both the years 2021 and 2022. However, this was not a consistent trend. North America witnessed a decline in targeted attacks but remained the third most targeted region in 2022 (down from second in 2021), while Europe rose to the second position, possibly due to the Russia-Ukraine war.

Top 3 Most Targeted Regions





Top 10 Most Targeted Countries

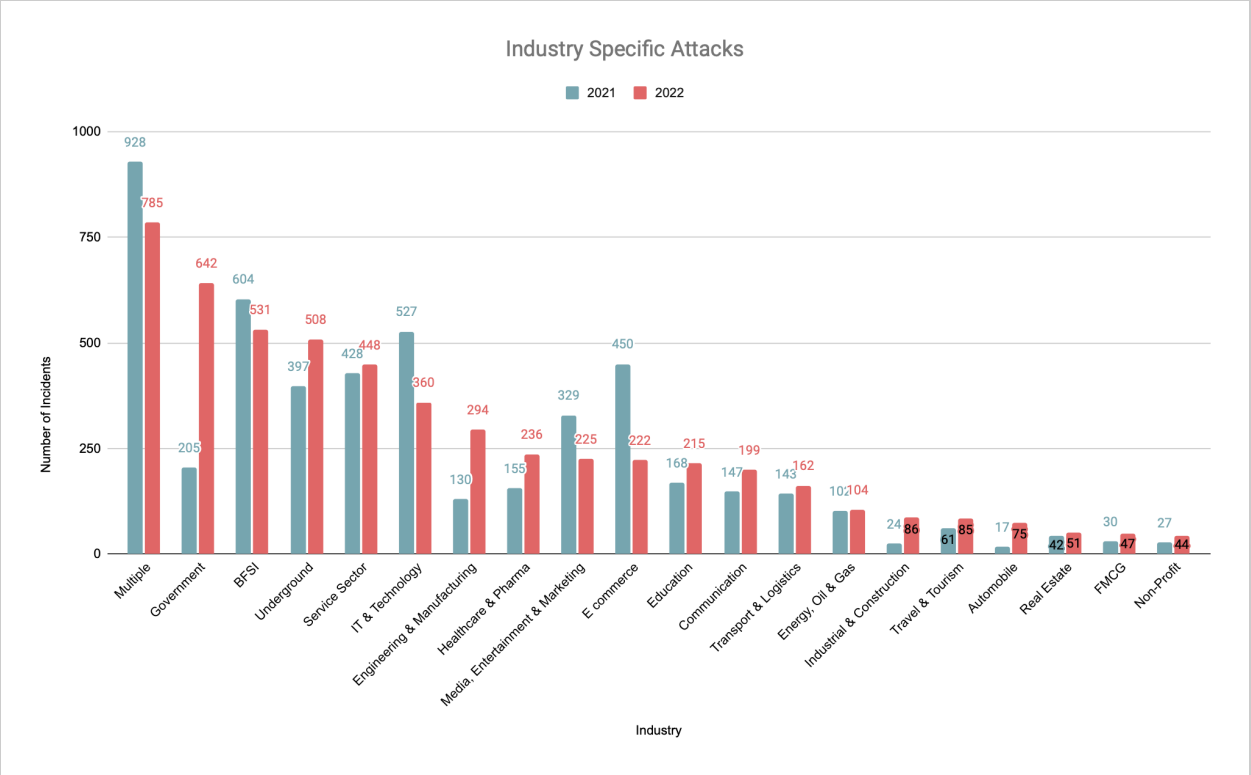
2021		2022	
Country	Count	Country	Count
USA	869	USA	779
India	395	India	491
UK	160	Indonesia	184
Brazil	119	Russia	181
China	116	China	158
France	104	Brazil	136
Indonesia	90	UK	125
Russia	87	Mexico	97
Turkey	82	Italy	87
Australia	82	France	86

Here are a few interesting region-based findings inferred from the data gathered:

- **Global** attacks remained the most significant but saw a slight decline, accounting for 29.2% of the total attacks in 2021 and 27.5% of the total attacks in 2022. This indicates that the attacks are becoming increasingly targeted and more sophisticated.
- **Asia & Pacific** remained the most targeted region, receiving 20.4% of all attacks in 2021 and 24.1% of all attacks in 2022. The number of attacks targeting Asia & Pacific increased by 26.43%. India was the second most targeted country in both 2021 and 2022. The number of attacks increased by 24.3% in 2022.
- Indonesia and Russia rose to the top 5 targeted countries in 2022 (third and fourth respectively). This can be attributed to a rise in hacktivist activities due to the #OpIndonesia campaign and the Russia-Ukraine war.
- **Europe** rose to the second most targeted region in 2022 from the third most targeted region in 2021. While it accounted for about the same percentage of all attacks in both years (≈18%), the number of attacks increased by 8.28%.
- USA remained the most targeted country, despite the decline in the number of attacks. This follows the trend of a decline in attacks in **North America** from 18.9% in 2021 to 16% in 2022. The total number of attacks observed a 9.68% decline.

Major Industries Targeted

- Attacks affecting **multiple industries** were most prominent but observed a decline from 18.7% of all attacks in 2021 to 14.8% of all attacks in 2022. The number of attacks decreased by 15.41%. This is another indication that more attacks are becoming targeted.
- Attacks on the **government sector** increased exponentially in 2022. Attacks on the government accounted for 4.1% in 2021, which increased to 12.1% in 2022 (most targeted).
- **BFSI sector** saw a 12.08% decrease in the number of attacks, but still remained the second most targeted sector. Banking and finance was the most targeted sector in 2021, responsible for 12.2% of the total attacks, and dropped to the second most targeted sector in 2022, responsible for 10% of the total attacks.
- Instances of selling/advertising various services and malwares on **underground** forums increased by 27.95% in 2022. The percentage of attacks reporting underground threats increased slightly from 8% in 2021 to 9.6% in 2022.
- Attacks on the **service sector** increased by 5.14% but their contribution to the total percentage decreased from 9.7% to 8.4%.
- **IT & technology**, **e-commerce**, and **media, entertainment & marketing** industries saw a decline in the number of attacks but remained in the top 10 industries targeted.



Government Sector

The Government Sector (including police, politicians, and military) saw a serious increase in cyber activity owing to the Russia Ukraine war. Hundreds of hacktivist groups emerged and cybercriminals around the world started voicing their protest against various governments by launching or participating in targeted campaigns such as #OpIndia, #OpIsrael, #OpIndonesia and #OpIran. The war did not only affect the two countries but resulted in worldwide disorder, disrupting global supply chains and exposing national alliances. This also resulted in an increase in state-sponsored attacks.

BFSI

The BFSI (banking, financial services and insurance) sector includes attacks faced by various financial institutions including cryptocurrency (7.72% in 2022). New and sophisticated tactics, techniques, and procedures (TTPs) targeting the industry emerged in 2022, these include phishing websites, fake APKs, reverse tunnel and URL shortening, and SMS forwarding malware. Attacks against BFSI industry not only compromises sensitive data, but can lead to financial frauds such as digital banking threats, carding, and ATM hijacking.

Underground

Activities on underground forums used to discuss, advertise and request for various cyber criminal services like ransomware, malware, malicious tools, vulnerabilities, and exploits, are continuously increasing. Threat actors form a community and find affiliates using such platforms, which helps in modeling of new attack vectors, making the threat landscape a breeding ground for new technologies.

Service Sector

Service sector comprises of various business, customer, training, and food services. The sector relies heavily on the labor being highly skilled and having an agile workforce. It is heavily dependent on upskilling and reskilling. Service sector handles sensitive client data including financial details, payment details, identification numbers, contacts information, and intellectual property.

IT & Technology

IT & Technology domain has been a pioneer in innovation and has been at the forefront of ushering in the technological paradigm. IT organizations are at the forefront of adopting and developing new technologies that are still maturing and are therefore especially vulnerable to attacks and exploits. IT industry also relies on networking and collaboration among the peers, which results in prioritizing easy access to data in lieu of security.

Engineering & Manufacturing

Engineering and manufacturing industry helps in improving the growth of the economy by improving exports and facilitating capital account surplus. Cyberattacks on the industry can result in physical infrastructure damage, halt operations, and expose intellectual property. Instances of the industry being targeted more than doubled in 2022.

Healthcare & Pharma

Attacks on healthcare industry increased by 52.2% in 2022 as compared to 2021. Compromised healthcare systems can expose sensitive PII (personally identifiable information) and PHI (protected health information), and lead to medjacking. The urgency of the medical work requires quick communication and easy access to data, which often puts cybersecurity in the backseat. Attacks on the healthcare infrastructure not only lead to financial loss, but can also be fatal to patience's lives.

Media, Entertainment & Marketing

Although this industry saw an overall decrease in reported cyber incidents, it remained in the top 10 targeted industries. Majority of incidents repoted under this industry were related to breach of entities pertaining to music, news, advertising, gaming, etc. The gaming industry in particular saw a significant number of attacks accounting for 21% of the total attacks in this sector. The FIFA phishing scams of 2022 were a part of this.

E-Commerce

Similar to the media, entertainment & marketing industry, the e-commerce industry also encountered a decrease in reported cyber incidents, however it managed to remain in the top 10. The incidents reported here were primarily related to scams/breaches in various ecommerce brands such as Amazon, Flipkart, Nykaa, etc. 2021 saw a huge number of phishing campaigns against Flipkart during the Big Billion Days Sale. Same was observed during the Christmas and New Year Sales in 2022.

Education

Education sector emerged as a valuable target for threat actors after large-scale digitization of education system, and rapid growth of online learning platforms. Attacks on the sector increased by 28% in 2022. This is especially concerning, given that a large portion of students are under the age of consent and have limited awareness about how their data can be misused.

Top 10 Threat Actor Handles Identified

The threat actor groups KelvinSecurity and AgainstTheWest were seen actively attacking entities in all the sectors throughout 2021 and 2022. Apart from these LockBIT (with all its variations), mont4na, LeakBase, bambam, Conti, and Hive were responsible for some of the prominent breaches. Even though Conti ceased its operations in the mid of 2022, it managed to make the cut of the top 3 threat actors in 2022.

2021		2022	
Country	**Count**	**Country**	**Count**
KelvinSecurity	89	LockBIT	319
barf	76	KelvinSecurity	199
Nei	46	Conti	141
mont4na	46	LeakBase	125
AgainstTheWest	42	Hive	56
kehanet00	37	AgainstTheWest	55
inthematrix1	36	mont4na	52
babam	36	BlackCat	42
Master data	35	PoCExploiterAdmin	39
pompompurin	33	Vice Society	38

KelvinSecurity

- Mostly seen operating under the handle **Kristina,** this group is in top two actors in 2021 and 2022.
- The group uses targeted fuzzing and exploits common vulnerabilities to target victims. Being highly skilled in the use of tools and having a wide knowledge of various exploits, they share their list of tools and payloads for free.
- They typically target victims with common underlying technologies or infrastructure at any given time.
- The group doesn't shy away from attention and publicly shares information such as new exploits, targets, and databases on cybercrime forums and communication channels such as Telegram.
- They also have a data leak website where other threat actors can share databases.

AgainstTheWest

- Having emerged in October 2021, this group identifies itself as an APT49 or BlueHornet. They have been highly focused on exfiltrating region-specific data and selling it on the dark web.
- Based on their previous activity they appear sophisticated, skilled, and organized.
- The group has been targeting various countries under campaigns including **Operation Renminbi**, **Operation Ruble, Operation EUSec, etc**.
- Time and again they collaborate with different threat actors to target various nations.
- The group has been constantly exploiting a common set of vulnerabilities and exploits to target multiple countries.
- A confidential source in contact with the group ascertained that the group was exploiting **SonarQube zero-day and Swagger UI** vulnerabilities.
- They used to have an Onion website as an alternative store to purchase data compromised by them.

Master data

- Master data is a threat actor who actively operated on a now-dead English-speaking cybercrime forum. They were actively posting data that targeted various sectors across various regions.
- Since most of their advertisements contained samples as proof to substantiate their claims, it was concluded that the actor did possess the data. However, it is not sure whether they were the original perpetrator behind the exfiltration of the data.
- On multiple occasions, the threat actor was found accessing and downloading databases from open databases, databases present in open web directories, or exploiting vulnerabilities on third-party vendors associated with an organization.
- The actor has been consistent in selling data worldwide and has been primarily dealing with data that contains PII such as phone numbers, email addresses, and passwords.

LockBIT 2.0

- LockBit 2.0 is an affiliate-based Ransomware-as-a-Service (RaaS) threat group, which employs a wide variety of tactics, techniques, and procedures (TTPs)
- The group is known for compromising victim networks by leveraging compromised access, unpatched vulnerabilities, insider access, and zero-day exploits.
- LockBit first appeared in September 2019, when it was dubbed the “.abcd virus.”
- The group is known for using double extortion to pressure victims into paying the ransom.

- The group's targets include organizations in the United States, China, India, Indonesia, Ukraine, and European countries.

mont4na

- The threat actor operating under the name of mont4na specializes in exploiting SQL injection vulnerabilities, primarily on login panels.
- The actor was inactive for nearly ten months, until late November 2021. However, there have been over 50 posts since then.
- Previously, the actor was actively selling vulnerabilities and asking buyers to fetch the databases. However, over time they have started posting login accesses and databases in some cases.
- While their targets are all over the world, mont4na has only targeted reputable companies.
- The actor is known for deleting their advertisement once the vulnerability or the access is sold.

babam

- Babam is an Initial Access Broker (IAB) on a Russian cybercrime forum, active in the auction section of the forum.
- The actor specializes in selling different types of accesses (including Citrix, RDP, RDWeb, and VPN) from across the world.
- The actor's history, and the types of accesses advertised, indicate that the actor generally extracts credentials from the logs of info stealer malware or bots.
- The actor had a high reputation on the forum, but due to payment-related issues with some buyers, they were banned from the forum on 19 October 2021.

Some Significant Global Incidents of 2022

Initial Access Compromise

- Access to the Website of King Mongkut's University of Technology, Thailand
- Compromised Service Station Controls from Russia & Kazakhstan
- Emails Exfiltrated from Colombian Military Forces
- Admin Access to Rajasthan Government's SSO Portal
- Webshell Access to a Brazilian Government's Subdomain For Sale
- Access to Barcelona Supercomputing Center, Spain
- Webshell Access to Israeli Tel Aviv Engineering College
- FTP Access to the US-Based Software Firm, IntegraSoft
- Admin Access to the Indian Cargo & Logistics Firm, Zeal Global
- Admin Access to the Main Domain of Luxury Closet, Dubai

Ransomware Incidents

- US schools are being targeted actively by Ransomware Groups
- Nvidia cloud gaming targeted by Stormous group
- South Africa state owned electricity company targeted by Everest group
- Entrust, the US based security provider targeted by Lockbit 3.0
- US universities like Whitworth Educational University & Oklahoma city university targeted by Lockbit 3.0
- Ministry of Commerce and Industry, Oman targeted by Lockbit 2.0
- Kuwait Airways targeted by Lockbit 2.0
- Indian Global Inspection Services (GIS) Targeted by Cuba Ransomware Group
- Luxury Sports Car Manufacturer, Ferrari, Allegedly Compromised by RansomEXX Ransomware Group

Data Breaches

- Confidential Documents & Logs from the Aerolineas Airlines
- Data from Naroda Nagrik Co-op Bank Limited, Ahmedabad
- 511 GB of Data from Legacy Supply Chain Services
- 2.4M User Records from E-commerce Site, Vevor
- Database Leak of Govt Azizul Haque College, Bangladesh
- Data from the Consulate General of the Republic of Indonesia in China

- Database of the Ukrainian Ministry of Social Policy Circulating on Telegram Channels
- Vehicle Loan Applications Leaked from BMW China
- Internal Documents from the Global Transport & Logistics Service Provider, Multilines International

Compromised PII & PHI

- 11M Customer PII Breached from Optus, an Australian Telecommunication Company
- 5.4M User PII Records from a Financial Diligence Offering from Refinitiv, WorldCheck
- 4.8M User PII Records from Carousell, a Singaporean Web-Based Marketplace
- 200K User Records Exposed from the Turkish E-commerce Website, DuyuMarket
- Patient Records from Instituto Marquès, Spain, Compromised
- 6M Worker & Employer PII Records from the Mexican Social Security Institute
- 21 GB Identity Cards Leaked from Indonesia's General Elections Commission, KPU
- 1M PII Records of Peruvian Citizens Exfiltrated from HRDT Teaching Hospital
- 400K PHI Records of Peruvian Citizens from the Peru Ministry of Health
- 614K Customer & Doctor PII Records from Apollo Pharmacy, India

Credential Combinations List Shared

- 13K Records of Email Addresses, Passwords & Password Salt from Pokemasters.net Forum
- Email & Hashed Passwords from the Spanish Social News Website, Meneame
- Patients' Login Credentials Leaked from Shaffi International Hospital
- 3K Customer Login Credentials from a Ukrainian Internet Shop, 3G-Mag
- Credentials from Flowroute, a Communication Service Provider for Cloud Based Platforms
- Email Address and Hashed Passwords from the Marketing Automation Platform, Aritic
- Email & Password Combos from the National Research and Innovation Agency, Indonesia
- Email-Password Combolist from US Real Estate Company, Billingsareahomes.com
- 15K Records of Email & Password Combos from the German Software Developer, SAP
- 567K PII Records & Access to the Judiciary Systems of the Supreme Court of Argentina
- Email & Password Combinations from Nailsworth Town Council, UK

Major Vulnerabilities & CVEs Reported

- Microsoft Office vulnerability
- Zimbra Vulnerability CVE-2022-37042, CVE-2022-30333
- DogWalk, an Actively Exploited RCE Vulnerability in Windows MSDT

- Critical Authentication Bypass Vulnerability in Fortinet Products
- Multiple RCE Vulnerabilities Affecting Veeam Backup & Replication
- Exploit for CVE-2022-26809, an RCE Vulnerability in Windows RPC
- Two New Post-Auth 0-Day Vulnerabilities Affecting Microsoft Exchange Servers
- Appsmith Patches Full-Read SSRF Vulnerabilities
- Multiple Websites Using VMware Vulnerable to Remote Code Execution Via Spring4Shell
- 5.4M User Records Leaked Via Previously Patched Twitter Vulnerability
- CVE-2022-26138: Atlassian's Questions for Confluence Actively Exploited in the Wild
- Misconfigured Third Party CDN Exposes IT Service Provider's Sensitive PII Documents
- Overlooked Webhooks Exploit Endpoint Vulnerability in Slack Channels
- Internal Documents Exfiltrated by Exploiting a Local File Disclosure Vulnerability on Vodafone Italy's Subdomain
- Unauthenticated Confluence RCE Vulnerability (CVE-2022-26134) Actively Exploited in the Wild

Conclusion

The past two years witnessed evolving attack surfaces and continuous increase in sophistication of tools and tactics employed by threat actors. Data from XVigil shows a significant decrease in attacks falling under multiple industry categories and global regions, which is suggestive of the fact that the attacks have become more focused. However, the favored targets (both region and industry-wise) essentially remained the same consisting of BFSI, healthcare, education, and government sectors from North America, Asia & Pacific, and Europe. This consistency in pattern could imply one of the following:

- Threat actors make maximum monetary or political (in case of cyber warfare) profits by attacking these industries/regions.
- These industries/regions have the weakest security measures, thereby making them the obvious targets.

In either case, the resultant outcome is dangerous for users around the world as it puts the security of their data at risk. Hence, it is important for individuals as well as organizations to monitor the latest developments in adversary tactics, tools, and procedures, so that we can protect ourselves from becoming a victim of such incidents.

References

- Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 - CloudSEK
- Wr0ng P@$$w0rd! : Hackers Continue to Thrive on Weak Passwords - CloudSEK
- Increased Cyber Attacks on the Government Sector in Indonesia - CloudSEK
- FIFA World Cup Qatar 2022 Cyber Threat Landscape - CloudSEK
- Cyber Threats Targeting Global Banking & Finance Customers - Download Report - CloudSEK
- Increased Cyber Attacks on the Global Healthcare Sector - CloudSEK
- Cybercriminals Exploit Reverse Tunnel Services and URL Shorteners to Launch Large-Scale Phishing Campaigns - CloudSEK
- Cyber Threats Targeting the Global Education Sector on the Rise - CloudSEK
- Unearthing the Million Dollar Scams Targeting the Indian Electric Vehicle Industry - CloudSEK
- Abysmal State of Global Critical Infrastructure Security - CloudSEK
- The Darkweb Crypto Lifecycle: How Cyber Criminals Misuse and Cash Out Crypto Funds - CloudSEK
- Cryptocurrency Racket: The Growing Perils of Investing in Mysterious Cryptocurrencies - CloudSEK
- Blog and Research - Cyber Attacks and Digital Risk - CloudSEK
- Threat Intelligence - CloudSEK
- Five active ransomware gangs and their tactics (part one)
- Infostealer Comparison: Top Stealers in 2022
- Log4Shell Multiple Critical Vulnerabilities: Updated Advisory
- Government icons created by Freepik - Flaticon
- Bank icons created by Freepik - Flaticon
- Hacker icons created by Freepik - Flaticon
- Service icons created by Freepik - Flaticon
- Data icons created by Darius Dan - Flaticon
- Automation icons created by Becris - Flaticon
- Health icons created by Freepik - Flaticon
- Marketing icons created by Freepik - Flaticon
- Ecommerce icons created by Freepik - Flaticon
- Education icons created by Freepik - Flaticon

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats. Our Cloud SaaS platform constantly seeks security solutions for our customers' digital risks.

To learn more about how CloudSEK can strengthen your external security posture and deliver value from Day One, visit https://cloudsek.com/ or drop a note to info@cloudsek.com.