SECTRIO

The Global OT and IoT Threat Landscape Assessment and Analysis Report

2023

Table of contents

Data collection and research methodology

This report has been prepared from threat intelligence gathered by our honeypot network which is today operational in over 80 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- Are targeted by APT groups or other sophisticated hackers
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT and OT
- Have the potential to host multiple IoT projects across domains in the future

Over 18 million attacks a day registered across this network of individual honeypots are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework, that we have developed within Sectrio. The network includes over 8000 physical and virtual devices covering over 4000 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.

Sectrio's threat surveillance net runs across hackers' forums, malware platforms, IM chats, the Dark Web, and other validated avenues where threat actors congregate/collaborate. Our surveillance net gives our threat intelligence more depth and relevance giving more latitude to bring out insights that are exclusive to Sectrio

This data is analyzed thread-bare by our global threat research team. The analysis focuses on these areas:

- Unearthing new threats and variants of existing threats
- Correlating the behavior of threats with threat surface areas, institutional practices, breach tactics, and security outcomes
- Understanding how the threat environment is evolving
- Preparing and sharing advisories

This report provides a context for the evolving threat landscape as well. The context is divided into three parts:

- **Triggers and actors:** what are threat actors up to: analyzed at tactical and strategic levels; how are malware evolving
- **Enablers:** what institutional gaps are aiding the growth in cyberattacks [with inputs from CISOs]
- **Impact:** how are such trends impacting cybersecurity and enterprises and governments everywhere

Key findings are published by us every year to enable businesses, decision-makers, academicians, students, CISOs, and those interested in cybersecurity to gain a comprehensive understanding of the evolving threat environment that envelops IoT deployments and OT installations and derive appropriate responses to prevent, contain and dissuade such attacks.

Additional resources

To try our IoT and OT threat intelligence feeds for free, please visit this link

For more information on the malware and attacks analyzed in this report, please visit the malware reports section of our website.

More information on the data and the cyber incidents mentioned in this report is available in the blog section of our website.

To access the CISO Peer Survey 2022, visit this link

To access our datasets, reach out to us at

An intriguing year for cyber defenders everywhere

If there was ever a year that highlighted the need for ramping up cybersecurity measures and investments, then this was it. Looking at 2022 from the vantage point of cybersecurity, it becomes difficult, if not impossible to summarize this year. With geopolitical events in diverse geographies dictating the narrative, we did see the impact of the growing footprint of Advance Persistent Threat actors across the Middle East, South Asia, North America, and Southeast Asia.

Manufacturing firms, aerospace and defense contractors, telcos, schools, oil and gas companies, and healthcare providers were among the most targeted segments in 2022. Attacks on manufacturers across segments rose significantly in 2022 indicating the continuing attention this segment is receiving from hackers. Surprisingly, data stolen from some of the victims linked to attacks in early January 2022 is still for sale on a few forums as part of the original data block it was part of.

The attacks on healthcare providers are especially worrying as security measures and security awareness in the healthcare sector are either non-existent or misaligned with the diverse threats that the sector is being increasingly exposed to.

Independent hackers are attacking healthcare providers for monetary considerations while the APT groups are playing with a different goal in mind. Chinese APT actors who breached multiple healthcare institutions in India and UK were after the healthcare records of specific persons of interest

US$ 4.3 billion

Cumulative value of published global cyber ransom payments in 2022 [Across individuals, governments and businesses]

Rising cyber insurance premiums indicate heightened cyber risks

Cyber risk insurance premiums rose for the second year in a row in 2022. Cyber risk insurance for financial firms witnessed a rise of anywhere between 10-100 percent in 2022. Increasing attacks on enterprises and the resultant scale of disruption and revenue impact have together forced insurers to limit their exposure to losses arising from cyber incidents.

The direct-written premiums for cyber insurance collected by U.S. insurance carriers in 2021 grew by 92% year over year, according to the National Association of Insurance Commissioners[1]. The rising premiums are in some instances forcing enterprises to take a pick between going for a costly insurance premium or investing in better security controls[2].

Premiums per US$ million of coverage

Country	Sector	Premium cost per US$ million cover in 2022	Percentage rise range	Notes
USA	Banking	20,000	50-100	There were also instances where the premium rates had gone up by as much as 300 percent (cases where the company had reported a breach in the last 12 months). Insurance may be denied if the institution is unable to prove that it has robust controls in place.
USA	Government (County)	40,000	100	If counties do not satisfy more stringent norms and security control requirements, insurers may even reject a renewal
USA	Manufacturing	15,000	120	Earlier it was not uncommon for a midsize firm to have $10 million in coverage, that same firm is now being offered $5 million or less by most carriers. Specifically, if firms are determined to be of high risk, insurers are less likely to offer them a higher coverage limit or coverage altogether.
India	Enterprise	Approx: 5 USD per employee/ USD 2066 per million cover	Data not available	There are various coverage models deployed by insurers, the rates vary widely across the industry. For instance, an enterprise opting for multiple products from the same insurer gets nearly a 7 percent rebate over listed/quoted premiums.

Cybersecurity insurance premiums will rise significantly in 2023. With more businesses opting for cybersecurity insurance and growing threats, insurers will look at ways to reduce the risk load.

Key cyber risk trends that defined 2022

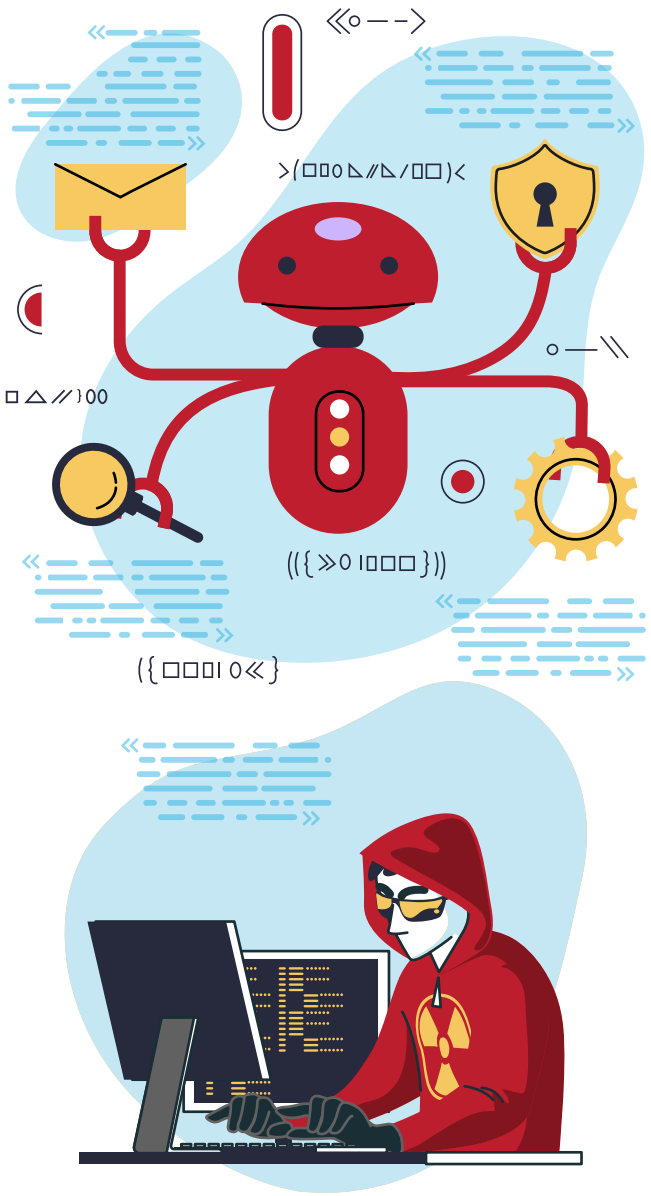
- Cyberspace became a riskier place to be in 2022: cyberattacks globally grew by a staggering 188 percent in 2022. Over 95 percent of all businesses were exposed to cyberattacks of one form or other this year ranging from Business Email Compromise all the way to data theft and loss of assets and capital investments
- The reinfection of networks belonging to enterprises that did not pay a ransom after an attack but restored their networks was done many times this year. In some instances, even victims who paid a ransom found their assets being reinfected within days of paying the ransom
- The emergence of a new hacker eco-system centered around Lockbit 3.0 variants: in addition to new hacker groups, the new variants also hastened the evolution of new tactics to target

segments such as healthcare and schools. Lockbit 3.0 has also paved the way for the emergence of new groups that are light on capabilities and tech and rely on other actors who supply the variant to these groups for targeting.

- Consolidation of APT groups. A few groups turned inactive this year while a few such as Dark Pink went active out of the blue in June this year
- Ransom payments and the number of reported cyber incidents touch a record high
- Time taken for stolen data to appear on various forums fell below 7 days for the first time
- Severe degradation in the cyber offense capabilities of known Russian APT and independent groups
- Several Russian hackers formerly associated with known Russian APT groups are now offering their services to non-government customers
- With the emergence of more targets, hackers are investing more capital and time in evolving autonomous malware such as Botenago. In such cases, the first level of targeting and engagement is automated and the hacker doesn't have to be involved. The malware then targets multiple vulnerabilities to exploit and once it latches on to the right exploit, a backdoor is opened and kept open for the next wave of attacks
- The latest system to appear on the target list of hackers is a large-scale backup system. As an offshoot of distributed power supply and distribution systems, hackers could have discovered the value of these systems while they were targeting renewable energy projects in Europe.
- Attacks on non-traditional sectors such as agricultural farms and renewable energy projects are growing at unprecedented rates. Such attacks are designed to increase the rate of inflation in select countries by increasing energy and food prices.

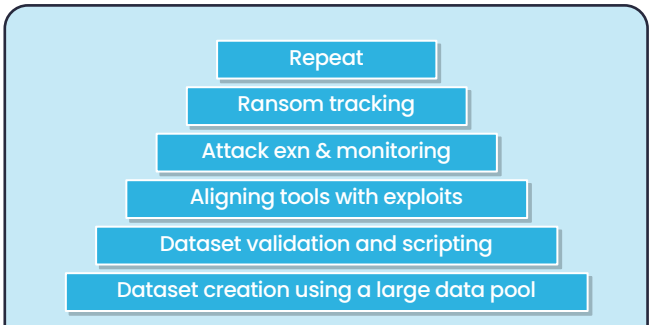
AI-powered cyberattacks are now a reality

AI-generated scripts are now being encountered in the wild. To understand the specific threats associated with the misuse of AI, we need to classify AI threats into two broad categories viz., short-term and long-term. Short-term threats are already manifesting or will manifest in 2023 while the long-term ones could take more than a year to manifest their potency.



Threat	Impact	Manifestation timeframe
AI-written scripts are added to create newer malware variants	The faster appearance of variants of potent malware and the appearance of new threat actors who are utilizing this malware	Immediate threat
AI-powered malware evolution models. AI-based no/low touch malware development	The evolution of newer malware will now be a faster affair as bad actors fine-tune malware development processes. AI will be used to probe systems and networks for vulnerabilities to exploit. New malware or modified malware could be used to weaponize these exploits. Such malware could be coded with low or negligible human intervention	Immediate threat
Large-scale bot farm control	AI will be managing bot farms across geographies turning them on and off based on the need to carry out attacks or to evade detection. This will make it tough to detect and shut down the bot farms	Long term
Reverse decoys	To lure and trap employees and privilege/credential holders to share data by using large honeypot networks that pose as extended asset ecosystems. AI will be used to create these true-to-life digital twins	Short term
AI-based supply chain attacks	Poisoned datasets could be inserted in supply chain management software during the calibration phase to generate the wrong output. This could lead to production shutdowns or aggregation of certain raw materials or production inputs at the wrong time. In the automotive and other critical sectors, AI-powered malware could keep backdoors open in critical components like semiconductor chips.	Long term
AI-based reply chain email attacks	Trained bots could intercept emails to break into mail conversations to trick employees to download malicious payload	Short term

- In September, Sectrio's researchers unearthed a Lockbit 3.0 variant which was modified using some form of AI-based scripting. While the edits were rudimentary and the malware was easily detected, the code edits presented some unique challenges:
- This could be an attempt by hackers to test the waters with AI
- Code changes included the insertion of garbage codes at various points to make the ransomware invisible to signature-based security tools
- The changes were not very significant and were probably carried out by someone who didn't want to weaponize this ransomware. The hacker/malware author could have given up early
- Either way, it does set the context for more malware authors to use AI to do basic code-level changes in the future



Hierarchy model for AI-powered cyberattacks

From an execution standpoint, by the end of 2023, we will see the entire lifecycle of an attack being managed entirely through AI-based tools. Right now AI is being used by hackers in a few areas of the overall lifecycle of an attack and this will change soon.

An Artificial Intelligence tool could identify potential targets, scan target networks and devices, locate entry exploits, leverage these exploits, deploy payloads, coordinate malware movement, harvest data and deploy or even generate erasure-proof payloads by utilizing the resources available in the target network. The footprint of these operations will be kept minuscule to evade detection systems.

We have evidence that points to multiple such use cases being tried out by hackers. The Lockbit group is trying out a new tool that automates follow-ups with the victim for ransom collection.

Cyberattacks driven by geo-political and geo-economic considerations

- Cyberattacks motivated by geo-political considerations (including those traced back to known hacktivist groups) rose by a staggering 288 percent in 2022. Sectrio's threat researchers used various means to ensure the correct attribution. The process (influenced by Carnegie Endowment for Peace)[3] followed included these steps:
- Investigation and event characterization: this step covers an analysis of the event, context, TTPs, actors involved, evasive and obfuscation maneuvers, timing, tactic signatures, potential motivations, and reasons for choosing a particular target
- Clustering the attack: based on previously observed patterns the attack is categorized
- Post-event claims: verifiable claims including ransom demand, mode of payment, and other claims made by the hacker group
- Data released: the forums in which data dumps appear often indicate a known pattern that can be mapped back to a known threat actor
- Verifiable chatter in known hacker forums

A revision of playbooks?

While in the past many attacks emerged in the immediate aftermath of a geopolitical event, from the year 2021, we are seeing deferred attacks or attacks that emerge without being anchored to a geopolitical tremor in the real world. This could be because the countries that are hosting APT groups or state-backed hacker agencies have revised their playbooks. The number one priority agenda item for APT groups is to create a nuisance value for the victim through cyberattacks and all groups are aware of the fact that any attack could invite a swift reprisal from the target country's APT groups or actors backed by them. Such attacks could also escalate into an all-out armed conflict between the countries involved.

Conti signs off with a large attack on Costa Rican government

Russian ransomware group Conti group carried out a brazen attack on the Costa Rican government in April 2022. Over 5 days, the hacker group using various forms of privilege escalation and manipulation, managed to exfiltrate data and encrypt data.

Whle the exact ransom asked for remains unknown, we do know that the hackers managed to deploy remote access tools to ensure continued access to key systems in case the initial access is lost. This added another tactic to the already expanding playbook that hackers are using to create and exploit breaches.

10 days later Conti group started winding up

Geoeconomics is another factor driving cyberattacks. The motives behind such attacks could include:

- Disruption of supply chains supporting the economy of a country considered an adversary
- IP theft for deriving gain at a macroeconomic level
- To create a regional resource imbalance
- Deprive an adversary country of resources critical to its economy
- Disrupt the economic potential of an adversarial country
- Impose a critical infrastructure restoration cost on another country
- Lower the investment potential

State-backed cyberattacks have become an option of choice for many countries to extract an economic cost for actual or perceived grievances. The targets for such attacks are carefully chosen to ensure maximum impact in terms of costs. In 2022, we saw attacks on critical infrastructure across various countries including attacks on the financial backbones such as stock exchanges and banking infrastructure, social security systems, mass transit services, and ports. Such cyberattacks are designed to create long-term financial disruption either in terms of the costs of reconstruction or the costs incurred due to the infrastructure being rendered unusable.

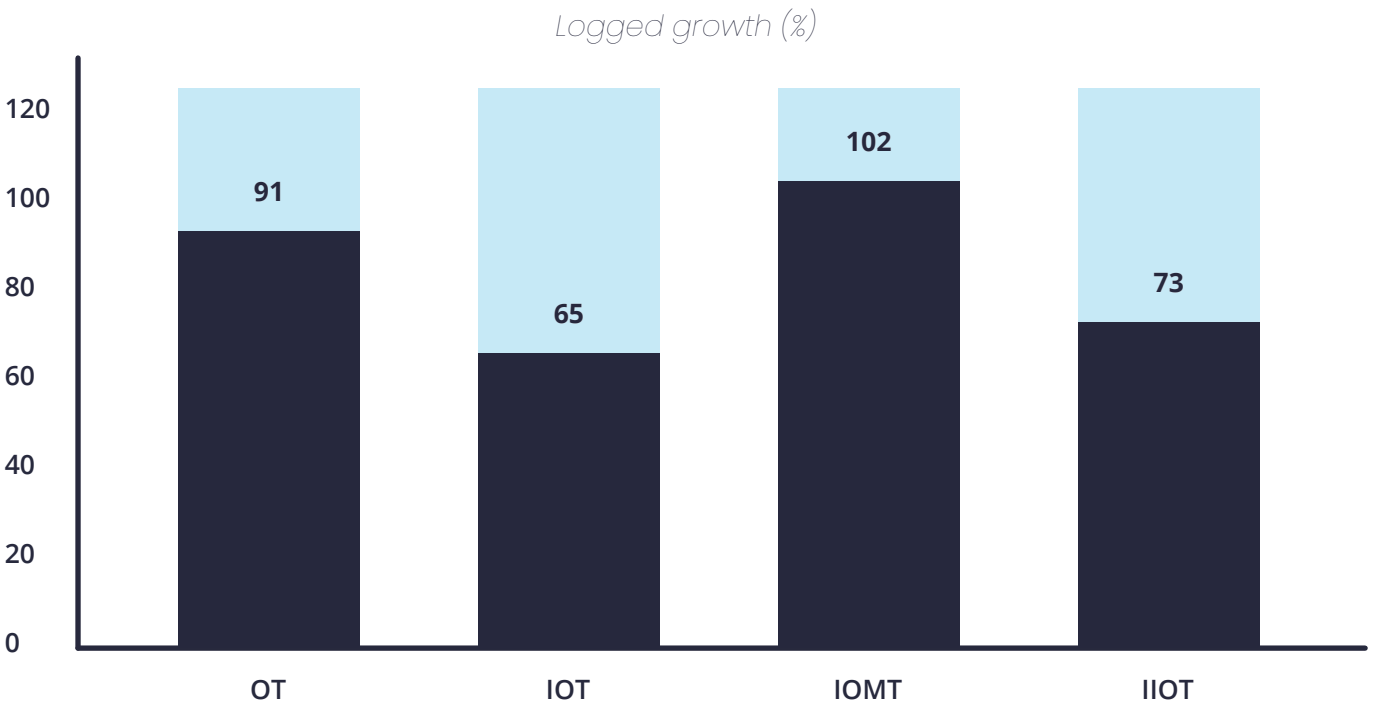
Why are cyberattacks rising?

Here are some of the unique reasons:

- The number of phishing emails intercepted by Sectrio's threat research team has gone up by 779 percent in 2022. Over 112,00,000 phishing emails were intercepted by Sectrio's threat researchers across domains. According to US CISA[4] "More than 90% of successful cyber-attacks start with a phishing email."
- The sale of compromise-prone IoT devices (or even pre-compromised devices) has continued unabated in 2022. Many of these devices including smart cameras, vehicle tracking devices, and personal gadgets lack any form of security other than a password. These devices also have chips and firmware with stealthy backdoors (with regular C&C communication) and often send data to servers located in countries without adequate data security laws. Such devices could be hijacked to serve as conduits to enable DDoS attacks or to pass on infected traffic
- Expansion of threat surface area: with the unchecked addition of untested devices with questionable supply chain origins and lack of security audits and testing, it was only a matter of time before these devices and networks turned into an opening for malware and hackers to exploit.
- In sectors like oil and gas, earlier, many traditional activities such as site exploration and geo-probing were all conducted in complete isolation. Today, however, such activities are being conducted with the involvement of connected systems with basic levels of security. With more activities being digitized without adequate attention to security new risks have emerged.
- Malware development and release cycles have shrunk: in October 2022 alone, we saw the emergence of 7 new variants of Lockbit 3.0 emerge in the wild in quick succession. With the emergence of new players, the demand for new and unique malware has risen significantly. Currently, this demand is being met through variants of existing malware. In 2023, however, we expect more potent malware to emerge than ever before. This trend is also being aided by the emergence of Zero days and the development of malware in unknown labs and research centers belonging to private hacker groups.
- Sectors such as space tech are being targeted through firmware trojans
- Expanding data dumps on the Dark Web

- Rise of APT-trained actors and threat actors who are carrying out cyberattacks in the guise of hacktivism
- Sophisticated actors are now acting with more knowledge of the processes and systems to be targeted. In the cement manufacturing sector, we saw attacks on heat recovery systems and health instrumentation systems. Easy availability of components from the pre-owned market and elsewhere is enabling hackers to build digital twins on sandbox environments to play out security responses from enterprises and to figure out workarounds. Such devices and their digital counterparts are also helping hackers uncover Zero days which are then sold on the Dark Web and other places through a sale or via an online auction.
- Unsecured OT networks are accessible through the internet. This provides an opening for hackers to access other parts of the enterprise network including WiFi networks that connect with non-corporate devices and equipment. In one instance Sectrio's researchers uncovered a convergence of a corporate network with the WiFi network of a facility used by the senior management of an enterprise. This means that all corporate communications and mail and other communication can potentially be sniffed by hackers or embedded malware.

Growth in cyberattacks across OT, IoT, IIoT and IoMT



- Quantitatively, IoMT devices registered the maximum growth in attacks (starting from a low base)
- OT registered the 4th consecutive year of rising attacks
- IIoT and OT attracted the highest number of sophisticated attacks
- APT actors accounted for about 39 percent of all attacks on OT
- IIoT and IoMT devices were mostly attacked by independent hackers

ICS vulnerabilities continue to haunt enterprises

Vulnerabilities associated with industrial control systems (ICS) continue to pose a significant threat to businesses everywhere. From health and safety instrumentation to control systems linked to specific functions, hackers are going after everything. In addition to APT groups and private hackers, several groups are targeting ICS systems by exploiting vulnerabilities. They have developed tools that can target ICS devices and networks. Some of these tools can operate to conduct multi-day scans, detect vulnerable devices and networks and either access or control them after compromising them. IT and OT environments that are hosting workstations that can be exploited by either breaching the operating system or by exploiting vulnerabilities in the motherboard. Once the devices are compromised, the hackers target other connected devices and systems by moving laterally and gaining access to other networks as well. It is up to the actor to decide when they want to create a disruption, stop the attack, ask for ransom, or use the compromised network to carry out more attacks.

Human Machine Interfaces or HMIs could also be compromised by hackers.

In the case of power plants and large manufacturers, we have seen hackers staying dormant for extended periods. In laboratories such as those connected to sensitive research, hackers keep exfiltrating data till they are detected or may even alter the calibration of key devices to alter test results. Both of which are detrimental to the research output of these labs.

As the lines between IT and operational technology (OT) network continue to blur, new vulnerabilities and threats imperil conventional OT security measures. Dangers to physical operations are growing from connected devices, third-party access, cloud-based applications and nested networks including programmable logic controllers (PLCs).

The safety and functional guardrails in an OT network can be compromised across multiple levels. For instance, OT threats can move laterally across network segments residing at the controller level also called the Purdue level 1.This is where PLCs operate the physical functions. Remote code execution and vulnerabilities associated with authentication bypass can be used to breach the PLC and take the attack to the next level. This moves the attack from the PLC to the connected devices.

Soft targets

In 2022, hackers stepped up attacks on academic institutions and healthcare facilities across the globe. Here are a few reasons why these two sectors are being attacked more frequently.

- Cybersecurity awareness levels: healthcare and educational staff are often not sensitized on cybersecurity issues. They are also often not aware of the threat environment that surrounds their institutions.
- Healthcare facilities often employ a wide range of devices with a varying range of security requirements. In some cases, devices are deployed with little or no security leaving them open to attacks from outside the network.
- Teaching aids including projectors and cameras are often hacked into or appended to bot farms to facilitate DDoS attacks

- Lack of patching: since most of these devices(and workstations) continue to work without patching and updates, they are used as such leaving them vulnerable
- Considering the value of patient data and the facilities, healthcare providers are often under pressure to pay off ransoms faster
- In the case of K-12 institutions, when systems are rendered inaccessible, schools are forced to pay the ransom to prevent disruption of learning and the leak of confidential student data on the Dark Web
- Healthcare data is often permanent. Once this data is leaked, the victim cannot modify it in any way. State-backed hackers are also tracking the healthcare data of politically and strategically important persons belonging to countries of interest.
- Schools are often used by rookie hackers as training grounds as well to hone their skills

Expanding threat surface

In May 2022 as part of a research effort, Sectrio's threat research team conducted scans online to study how accessible OT networks were. We were able to identify 7,31, 860 network ports connected with OT services globally that were digitally accessible through a routine scan across 23 facilities around the globe. These ports were connected with over 1,80,000 devices that were easily accessible from the internet.

One of the objectives of this research was to show how OT ports were connected to the Internet and the active exchange of data could potentially take place between these ports and anyone on the internet

OT-connected ports that are accessible from outside

Rank	OT network port	Possible OT Service targeted	The approximate number of devices accessible	Primary use
1	2222	Rockwell-csp2	65,000	General industrial automation
2	20000	DNP	31,435	Utilities
3	9600	Micromuse-ncpw	25,070	Manufacturing
4	5007	Linuxcnc	28,000	Manufacturing
5	4000	Custom Discovery Port	21,000	Oil and Gas
6	1883	MQTT	4,000	IIoT, Manufacturing
7	1911	Custom Discovery Port	900	Building automation and control
8	47808	Bacnet	1,490	Building automation and control
9	44818	Ethernetip	2,200	General industrial automation
10	18245	OPC Client	3,700	General industrial automation

Source: Sectrio Threat Research Team survey conducted between 1st May 2022 and 23rd May 2022.
Over 1,50,000 network ports located across the globe responded to an attempt to scan. Of these, over 75,000 had unique IP addresses belonging to countries that have a significant density of projects that house OT.

Country-wise availability of ports that responded to scan attempts

Countries	Number of ports that responded to scan attempts
United States	153,000
United Kingdom	99000
Germany	67765
Singapore	54030
Japan	38977
India	16543
South Korea	16001
France	15987
Italy	5980
Indonesia	5600
Others/unknown	258,977

This indicates that OT communications ports have not been closed either voluntarily or accidentally by the teams that manage these networks.

Threat actor focus: APT41's expanding capabilities pose a significant economic threat

- Chinese hacker group APT 41 has been in the news for multiple instances of cyberattacks, espionage, cyber piracy, and cybercrimes for at least a decade now. In 2022, however, APT 41's activities have expanded significantly to net more data and geo-political leverage for its backers. This trend does have implications for governments and institutions of economic significance in various countries as they will now be targeted with multi-tactic and multi-platform tactics that will not just be hard to detect but hard to counter as well.
- While APT 27 the other Chinese APT group is now more or less focused on Taiwan and quite open (and vocal) with its threats, APT 41 has adopted an entirely different doctrine towards cyber espionage. APT 41's information gathering approach rests on:
- Gathering critical information on a target through sporadic yet persistent episodes of breach
- Deploying malware that remains unannounced on networks, conduct reconnaissance lasting over 200 days at a stretch
- Leverage Zero Days to hijack assets while keeping the hack a secret to be leveraged during a crisis or geopolitical confrontation
- Modifying TTPs constantly to evade detection
- Sharing harvested data with other groups including APT27 for further mining and exploitation
- Rapid targeting of entities using primary breach and using data mopped up from the Dark Web and dead drops. APT 41 is among the fastest APTs. It can roll out an attack on a new target in less than 24 hours after being instructed to do so.
- Focused and adaptive strategy to create breaches in networks of interest. It doesn't shy away from tapping telecom networks for obtaining confidential data for targeting specific entities
- There is a large repository of data collected by this group that is repurposed for launching attacks. This includes databases with login and access credentials
- Remote malware assembly and dissemination is another capability that APT 41 uses to deploy malware. SQL injection in websites with weak security is a common tactic this group uses.
- Targeting governments and industry associations to collect data for subsequent cyberattacks.

APT 41 has been focusing a lot of intercepting government conversations, high-tech research, and select targets using spear phishing, listening, water holes, RATs and backdoors, and communication chain attacks. The group specializes in attacks on large and tough-to-breach targets including telcos and defense projects. Its training regimen includes making trainees start their stint with APT 41 with first-level attacks on select Taiwanese targets. They are then deployed on select projects across South and South-East Asia.

APT 41 is also known to pursue subtle monetization options and has been known to sell stolen IP in closed forums through intermediaries. What APT 41 does with the money it earns is not fully known. While North Korean Lazarus is known to hand over its earnings to the government, some part of APT 41's revenues may be shared with their handling agency within the Chinese government.

The economic threat from APT 41

The rising activity levels of APT 41 will eventually lead to an economic impact on various countries where its targets reside. APT 41 can theoretically connect attacks across critical infrastructures to create a single attack wave that causes business shutdowns, and exfiltration of confidential economic information including impending regulations or data that could lead to lowering of sentiment in the stock markets and pressures on the currency of countries.

This wave could also degrade the ability of a nation to respond to an economic or military threat or an internal disturbance. Overall, such a destabilization could impact not just the target country but the region and many multilateral institutions as well. If the past attacks of APT 41 are anything to go by this group is being prepared for attaining much larger objectives of the government agencies that they report to. The long-term stealthy intervention-driven network, communications, and asset reconnaissance point to a larger game plan.

Major APT actors and their activities in 2022

Chinese APTs dominated the cyber threat landscape in 2022. Not only did they expand their footprint but they also got away with large-scale data theft and cyber aggression of magnitudes never seen before.

Among the sectors, defense and aerospace continue to be among the most sought-after sectors for targeting by APT actors. As per our research of over 170 complex attacks with clear attribution and from data gathered from public sources, chatter among validated sources, and information leaked from within the groups, we were able to paint a picture of the sectoral targets sought by APT groups across the globe.

A word of caution here. This data is influenced heavily by APT groups such as Lazarus from North Korea that are more active than say Polonium from Iran which is a seasonal and event-driven APT actor. The former is almost perennially active thereby accounting for a bigger percentage of attacks as compared to the latter which by virtue of its relative inertia accounts for a much lesser chunk of the overall attack pie so to speak.

Some APT actors focus almost exclusively on enterprises, supply chains, and manufacturing. Chinese APT Bronze AKA SLIME34, DEV-0401 for instance ran a campaign in mid-2022 targeting a range of industry verticals for conducting industrial espionage. Its targets included pharmaceutical companies in India and Brazil, two major defense vendors in Europe, media companies, and even a US start-up. Among APT groups in China, North Korea, Russia and Iran, affiliated actors often switch APT groups for projects. For instance, Russian APT group Cozy Bear AKA The Dukes/YTTRIUM and another Russian APT group Fancy Bear AKA Group 74, PawnStorm, Sednit, Snakemackerel often exchange affiliated actors on a need basis. This is why we sometimes see a similar hacker profile and behavior turning up across different hacking episodes.

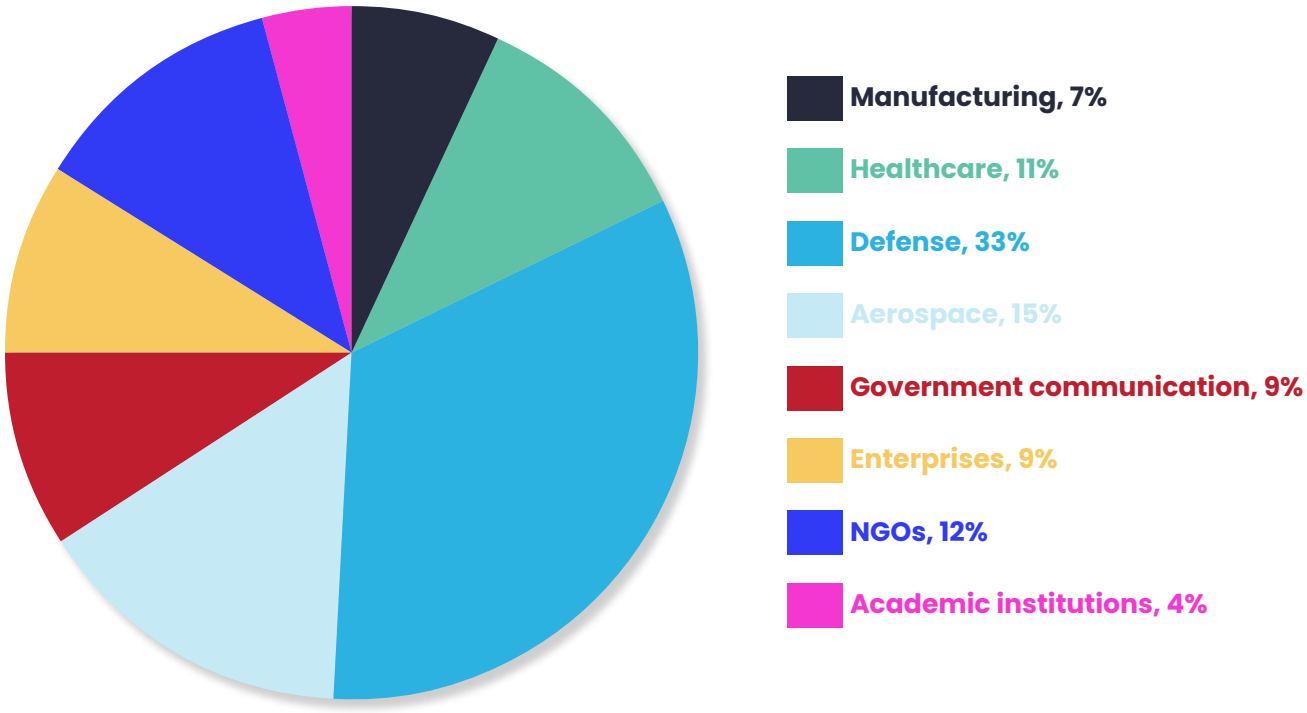
Beating sandbox environments

Most of the malware and multi-loaders used by APTgroups are now designed to evade sandbox environments to delay detection and to avoid engaging the wrong targets. Common methods to evade detection include studying registry keys, execution delays, hardware environment analysis, activity analysis, validating credentials and data and checking the version of the operation system and running prcesses.

Major APT groups, footprint, their targets and period of operation

Group	Origin	Campaign	Targets	Time frame
Dark Pink/Cicada	South-East Asia	Falcon – Data theft and snooping	Armed forces, hacktivist groups and government agencies in Thailand, Cambodia, Indonesia, Malaysia, Philippines, and Vietnam	Apr-Dec 2022
Vixen Panda	China	Taurus	Iranian and Qatar governments and legal networks	Mar-Jul 2022
Static Kitten	Iran	Purple Tulip - Espionage and IP theft	US, UAE, Qatar, India, Central and Eastern Europe	2021, and whole of 2022, ongoing
Vixen Panda – b	China	Better together	FIFA World Cup and associated infrastructure	Jan-Nov 2022
Gamaredon	Russia	Trident	Ukrainian and NATO targets	
APT 29	Russia		Targets across Europe and NATO	Throughout 2022
Turla	Russia		Diplomatic intel from Eastern European countries	

Percentage of attacks logged/detected



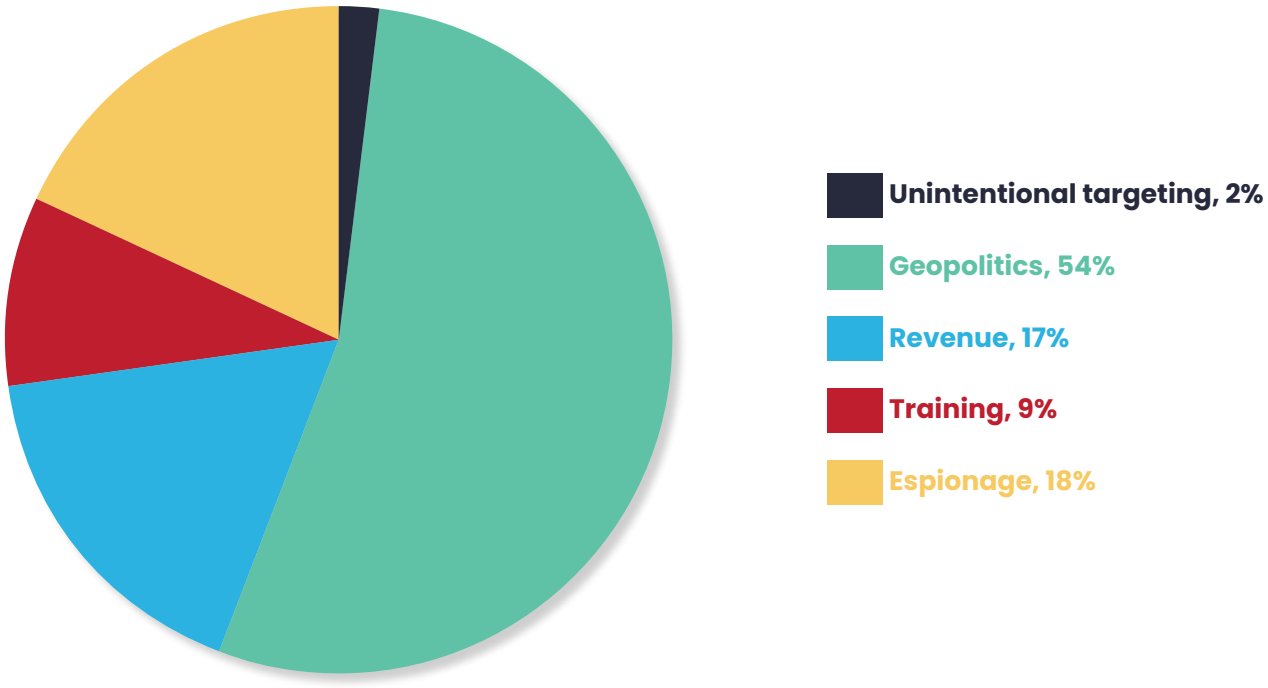
Industrial espionage

APT groups are also targeting large defense vendors, manufacturers, utility firms, and connected supply chains. Attacks on such entities go well beyond the core motive of disruption and are usually oriented toward stealing data and confidential IP from the target organizations. In such instances, the reconnaissance phase lasts well over the norm of 25-40 days and extends in some instances into over 400 days. During this phase, the surveillance is mounted by a range of APT agents who diligently track the target network and actions of key personnel.

The scanning phase usually gets extended as the hackers try and map the network, connection hierarchies, assets, applications, processes, controls, and credential dumps. If these activities are not done within the time allocated, hackers often escalate the task to senior members of the APT group and the new individuals start their task afresh trying to wrap up the project within a fresh deadline.

In the case of the Chinese attacks on Taiwan during the visit of U.S. House of Representatives Speaker Nancy Pelosi, the snooping attacks were ongoing as early as Jan 2019. Chinese APT 27 and 41 were at various times keeping a watch over Taiwanese cyberspace while occasionally surfacing to carry out large attacks such as those carried out on-chip manufacturers and oil firms in May 2020.
Taiwan was also attacked as part of an attack on Hong Kong pro-democracy activists in 2019.
Sectrio's threat research team monitored over 70,000 conversations between February and December 2022 to among other things identify the motivations for a cyber strike. During this duration, we also analyzed the command and control structure of APT groups and identify how individual members are given specific tasks across channels such as Telegram and paid after the execution of such tasks as well.

Motivations for APT-affiliated hackers to hack specific targets



Before the pandemic set in, hackers and non-North Korean APT teams were not operating with revenue goals. During the pandemic, covet funding to APT groups dried up and this led to many APT groups seeking ransom payments from their targets. Thus, their victims (most of whom were strategic targets) had to deal with the loss of data and money and for all practical purposes[which was eventually sold to multiple buyers], this data was also stored by these very hackers for retargeting.

There were also instances of APT groups targeting ending up targeting unintentional victims. In one instance, a retailer in Indonesia was targeted instead of a government agency by a Chinese APT. Such instances are far and few as APT teams have perfected the art of being specific with their targeting.
Unlike non-state threat actors, APT groups often sell data through proxies to a highly limited audience. North Korean Lazarus uses Telegram extensively to target buyers while Russian APT groups operate through sales proxies and affiliates who sell the data through their contacts.

When it comes to the communication hierarchy, North Korean APT hackers operate through commands given directly to them through a single handler. In the case of Chinese, Iranian, and Russian APT actors, multiple handlers manage hackers in parallel. This is because the hackers are often engaged in multiple projects at the same time and are reporting to various handlers separately for each of those projects.

Russian APT activity

Russian APT groups went after a diverse spectrum of targets in 2022. This included government bodies, oil and gas companies including pipelines, ports, large cargo movers, and even scientific institutions. Russian groups affiliated with the FSB and various security agencies in Russia targeted these agencies through a mix of phishing and spear phishing using malicious attachments, template injection, and spurious apps to load malware on compromised systems.

Trainee hackers from Russian APT also defaced many government websites belonging to various countries in the assessment year. A coordinated misinformation campaign was also run by agencies (supported by Russian APT groups) masquerading as think tanks.

Several Russian APT groups also targeted Ukrainian and Georgian citizens directly using harvested mail IDS and emails bearing war-related messaging. Such messages lured recipients into clicking links with multi-payload malware loaders. The APT group involved (APT 29) also used such emails to deploy backdoor malware to track victims' devices as they moved across Ukraine to map their movement. Devices that were located near known Ukrainian army bases or areas housing Ukrainian troops were targeted by precision artillery shelling in some instances.

Russian APT group Callisto AKA SEABORGIUM was tasked with tracking logistics companies and entities involved in moving equipment and weapons inside Ukraine. It was also asked to hack into companies

Weaponizing resumés

Russian APT groups used an old and proven technique to enter systems and networks of interest in 2022. The quality of these documents indicates the commissioning of a professional resumé writing or polishing agency to ensure they beat Applicant Tracking Systems and/or human checkers enroute their destination.

Surprisingly, among hackers, CISOs are among the least preferred profiles for sending resumés. The most preferred profiles include product heads, legal and privacy heads, sales heads and procurement heads.

The idea of using a resumé rigged with a malware loader was first used by North Korean Lazarus during its attack on an entertainment major last decade. Russian groups took it to another level by identifying and responding to job ads posted on forums using a rigged resumé. They were able to breach at least 3 targets in the process. Rigged resumé are also popping up in South America where they were first discovered in an attack on a Chilean ATM connectivity provider.

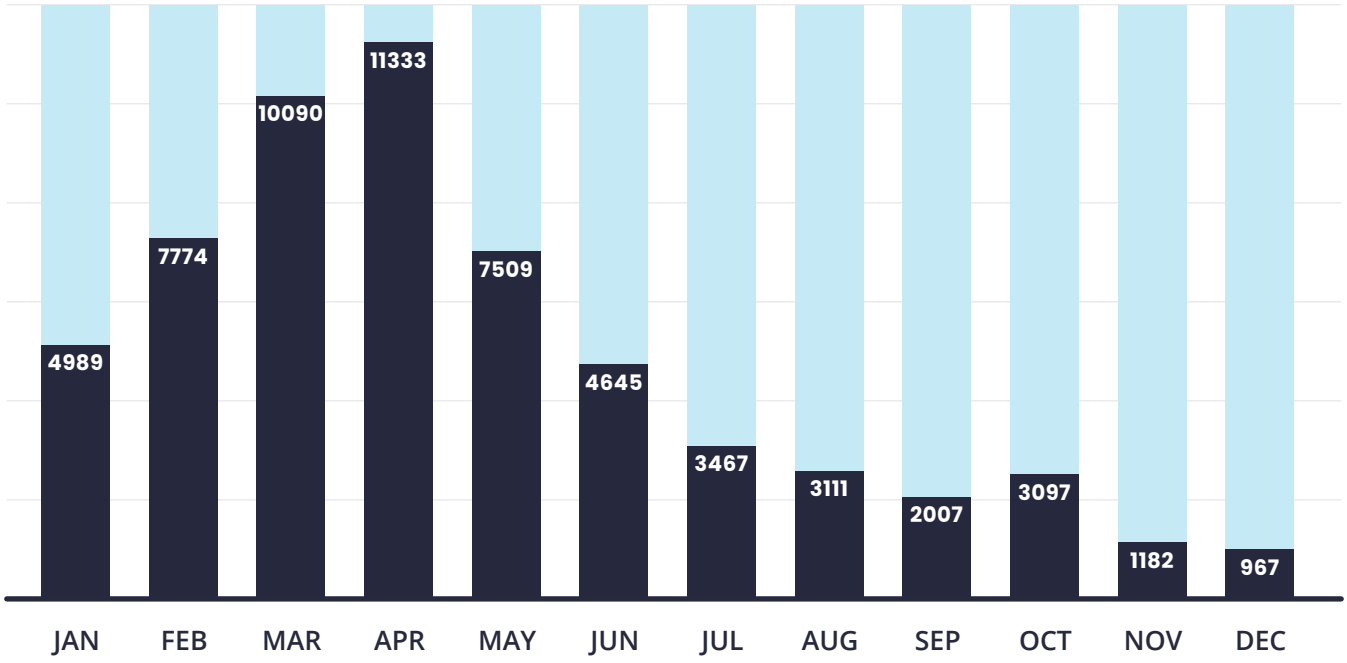
Table: Sectors targeted by Russian APT groups

Sectors	Percentage of overall attacks logged
Diplomatic missions and European\transatlantic regional grouping**	12
Oil and gas companies	13
Financial institutions	09
Manufacturers	09
Defense establishments	04
Space tech/aerospace	01
Others	52

*** as per phishing emails and chatter intercepted*

- Russian APT activity peaked in April 2022. The collective footprint of these hackers has been shrinking since then. This is because these groups are now focusing on targeted attacks while responding to specific geopolitical triggers (unlike the first quarter of 2022 when they went after many targets simultaneously. Russian APT groups have also been targeted by Chinese APT groups as well.
-
- Highlights of Russian APT activity in 2022
- Russian APT groups are now acting out through proxies
- Clear signs of a consolidation emerging among key players
- Russian APT groups were themselves targeted among others by Chinese APT players
- While the group's footprint is reducing, its capability to strike remains intact
- Core Russian APT groups are now focusing on highly focused operations
- They are also making attempts to monetize their attacks and target crypto wallets

Russian APT footprint in 2022



Chinese APT activity

Chinese hackers took over many of the spaces vacated by some Russian APT groups and private hackers in 2022. Chinese groups dominated most of the year through sheer brute force and persistence. The total number of attacks attributed to Chinese APT groups rose by 277 percent in 2022. Chinese hackers targeted fewer countries than Russian hackers but carried out more attacks and breach attempts in 2022. Unlike 2021, when Chinese APT activity was traced to 11 cities across China, in 2022, Chinese APT teams were traced back to just 5 cities.

Almost all Chinese APT groups focus on cyber espionage. A few of them such as APT 41 are however used for offense operations to harass victim organizations as per the directions of some departments within the Chinese state. These groups also target other APT groups globally to pilfer tools, data, and strategies and to test various tactics.

Chinese APT groups were active across the globe and were operating with specific strategies to target countries and businesses. In addition to industrial espionage, these groups also focused on pharma companies and diplomatic cable interception. Establishing persistence (through payload obfuscation) on target workstations via OS services to sideload backdoors is a favored tactic among these groups. They also use compressed formats for data collection and transmission from the victim's network.

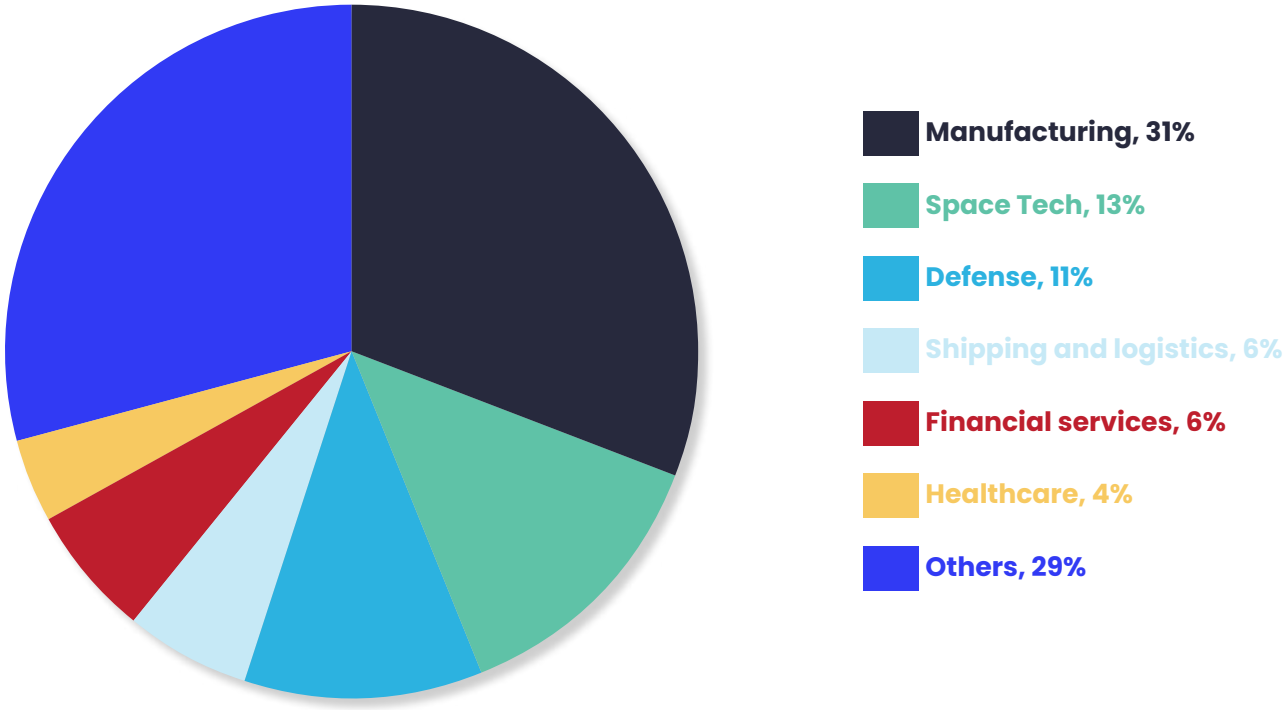
In one instance recorded in Europe, APT 29 affiliated hackers leveraged vulnerabilities in a widely used ERP system to deploy a payload that came with digitally-signed kernel-level rootkits augmented with a multi-stage infection chain that is activated in phases to keep its operational signature low.

IP theft by Chinese APT groups is an ongoing concern and the problem got worse in 2022. A unique challenge with Chinese APT groups involves cleaning their tracks after the mission is completed. Thus if data concerning Intellectual Property is stolen by Chinese APT actors, the victim may not even come to know of the theft till a competing product or service appears in the market with similar characteristics and value proposition.

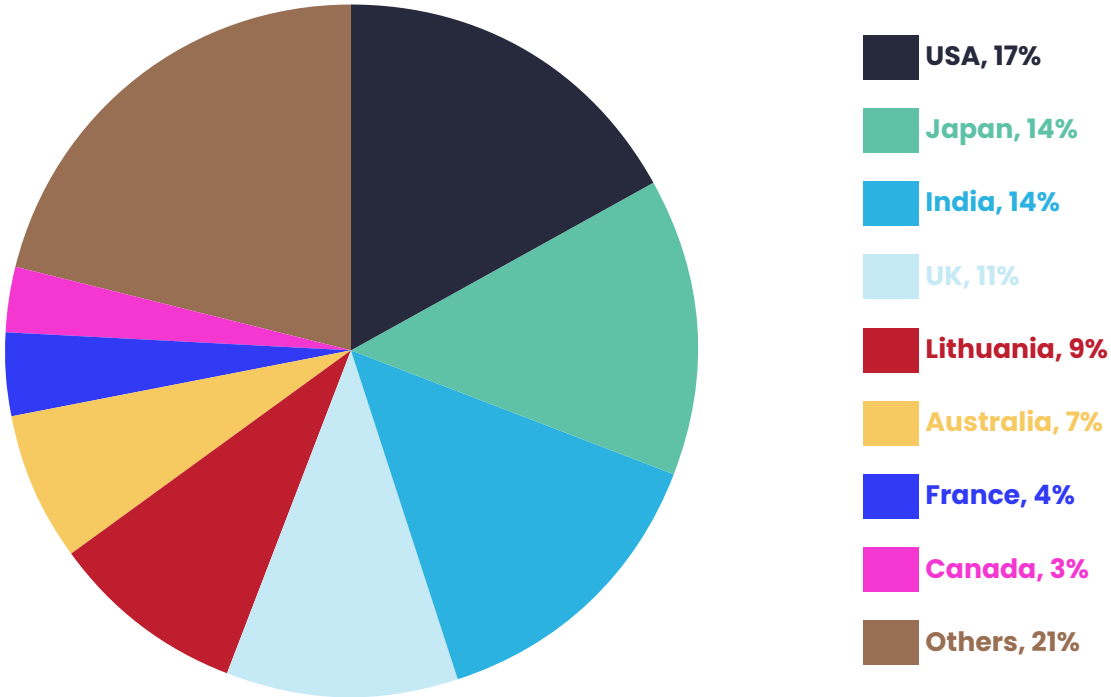
One of the most active APT groups from the Chinese APT assembly line is APT 41. APT 41 works to breach hardened and tough-to-attack targets. In addition to it's growing footprint in India, South East Asia, and North America, the group also maintains constant surveillance in cyberspace across countries. Spear phishing, sniffing, water holes, listening, RATs, and backdoors are all favored APT 41 tactics. It does also opt for communication chain attacks when needed to exfiltrate data.

The group has been known to attack government targets and monetize its attacks through third-parties. The funds so generated are used by the group to train its hackers and also to build new tools. APT 41 is also known to maintain a pool of reward money to pay top-performing hackers.

Chinese APT Targets



Target Countries



The Chinese Intelligence conveyer belt

In the second half of 2022, China moved up a notch to become the country harboring the most active APT groups in the world. Cyberattacks from China have picked up both in volume and quality in the last 9 months. In addition to diplomatic cables and Intellectual Property, Chinese APT groups also went after defense vendors, healthcare providers treating (or holding records of) politically important persons, and infrastructure connected with critical manufacturing facilities.

Chinese intelligence operates at four levels viz., data gathering, validation, analysis, and deployment. Various enablers are involved at each stage. In recent times, China has paid extraordinary attention to data validation by recruiting more information sources to cross-check the information already on record. It has also figured out ways to hack into non-traditional sources of data to assess the quality and significance of information already collected. The validation used to happen at two facilities located in Eastern China. Now, however, China's Ministry of State Security (MSS) has started commandeering private sector companies to help in refining collected data to derive intelligence value. This includes firms with big data analysis capabilities and those with proven and working AI models to determine the link between unconnected data sets and the validation of raw data by looking for pre-established patterns of authenticity.

Intelligence data processing occurs at huge scales in China. Thanks to the availability of facilities commandeered from private enterprises, China doesn't have to invest in building these facilities in-house and spend time, resources, and energy in recruiting manpower and maintaining them. This frees up a big chunk of manpower to focus on upstream intelligence-gathering activities.

Every event of significance is validated from multiple independent data sources to confirm its strategic utility. For instance, if an asset of interest is moved across locations, then this movement can be confirmed by not just tapping into different sources of intelligence data but also looking for post-event indicators residing in petabytes of collected data. Such bits of intelligence are priceless from a strategic decision-making standpoint.

Private sector participation in intelligence data processing is encouraged by the Chinese government. Some of the private companies participating in this effort do receive some form of discrete funding or non-monetary and tax benefits from the MSS or the Chinese government. Those that don't readily agree are coaxed and forced to participate.

Why is China investing in newer methods of intelligence data collection?

With the establishment of a huge capacity for crunching raw intelligence, China ran into a problem in the early half of the last decade. It had to figure out a way to keep these facilities churning. China then started to look for new sources of intelligence information to continue utilizing the established capacity. China is aware that any break in data collection, validation, or analysis could lead to a partial degradation of intelligence processing capabilities in the long term. Thus the entire intelligence information assembly line is kept active with information and datasets fed at regular intervals. This is why China needs to constantly harvest information across HUMINT and SIGINT channels.

Further, China is also testing newer military hardware that performs optimally under certain atmospheric and local weather conditions. With greater awareness of atmospheric conditions and other regional factors including accurate

views of strategic military installations, China can afford to work with more operational insights to better plan and execute the use of military hardware, systems, and personnel in the event of a formal/informal declaration of hostilities.

This also offers a strategic advantage in times of geo-political crisis, trade negotiations or confrontation such information gives a clear advantage to the country involved. It can even help factor in a potential response from an adversary.

Given this backdrop, we expect China to stay invested in expanding its intelligence-gathering capabilities and facilities. Such efforts will also be augmented with other means as the raw data processing and refining capabilities improve. The growing capabilities of Chinese APT groups in cyberspace is another undisputable evidence that points to the adoption of this approach by China. With its increasing appetite for intelligence data, this trend will define China's approach toward cyberspace and beyond in the days to come.

Lockbit RAAS and its disruptive impact on the threat environment

LockBit is a highly autonomous series of ransomware designed to block access to systems. It is self-propagating and the groups that use this ransomware use a double extortion model, in which its associates exfiltrate data from victim organizations at level one and then threaten to disclose it online. The data itself is sold irrespective of the ransom payment. LockBit 2.0 tries to breach networks primarily through purchased access, unpatched vulnerabilities, insider access, and zero-day exploits.

The LockBit ransomware gang started emerging on the radar around August 2019. It started as a ransomware-as-a-service (RaaS) and the Lockbit gang that was promoting the operation gave support on Russian-language hacking forums while running a multi-stage campaign to recruit more hackers.

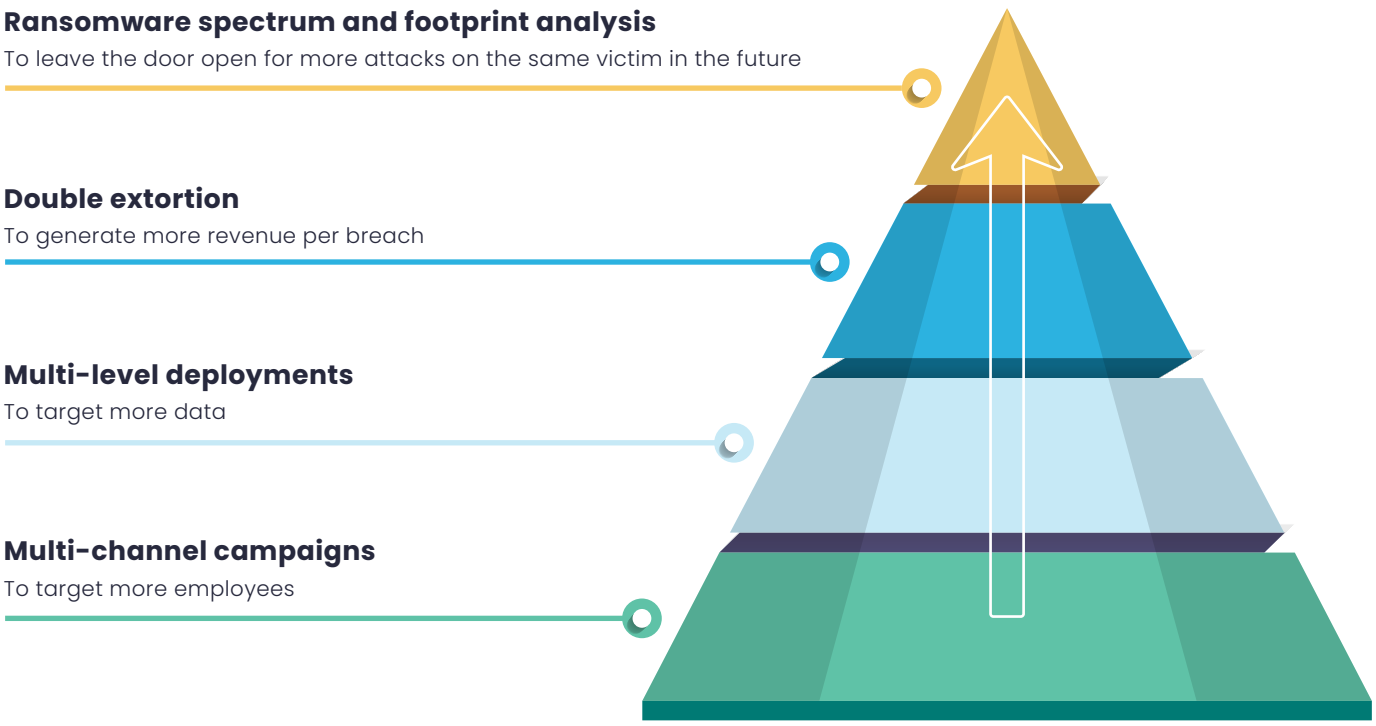
Just two years later LockBit launched LockBit 2.0 RaaS on their data leak site. This was after ransomware actors were banned from posting on existing cybercrime forums.
A typical attack begins with the victim's device being infected and the files being encrypted with a jumbled extension. The process of data encryption is done at a rapid speed with multiple tasks being done in parallel. The infection becomes apparent with the wallpaper of the victim's machine is changed to a ransom note. In case the ransom is not paid on time, the victim's data is then put up for sale on the Dark Web and other forums.

When LockBit 3.0 was launched in June, the group touted it as the most powerful encryptor ever built. The launch also led to a 17 percent rise in cyber incidents directly linked to the encryptor. The new variant brought in new features such as more payment options across cryptocurrencies, new monetization options, and more means to recover or destroy data as per the outcome of negotiations with the victim.

With LockBit 3.0, the group also launched a new bug bounty program to let security researchers and hackers find flaws in the gang's projects and infrastructure hosted on the dark web. LockBit creators have also developed an automatic data exfiltration tool called StealBit to improve the whole process.

Understanding the Lockbit ransom model

- Unlike previous ransomware groups, Lockbit creators have almost perfected an operational model that is sustainable and creates more opportunities for revenue in the short term and long term. Here are a few innovations brought about by Lockbit that other groups are now copying and aping:
-
- The recruitment of affiliates is on a revenue share model that is highly skewed in favor of the interests of the affiliate. The group can levy an affiliate commission between 15-30 percent of the ransom collected for every successful breach. This is way less than the industry norm of almost 50-70 percent collected by other ransomware groups from their affiliates.
- The group has netted so many affiliates that now it is finding it difficult to keep a tab on their activities. In December, a LockBit member attacked a children's hospital in Canada and the group had to step in to disown the attack and the affiliate and provide a free encryptor to the hospital.
- Lockbit is today the single biggest ransomware group out there. Its fingerprint was detected in as many as 27 percent of all attacks studied by our researchers.
- Lockbit has outsourced the research and development work to gangs such as Mzar who work in the background to fine-tune the ransomware.
- It also runs an open bug bounty program to reward researchers who find bugs in the ransomware
- Lockbit affiliates work closely with some APT groups as well.



The Lockbit operational model components

Ransomware spectrum and footprint analysis

Ransom Group	Instances
Clop	06
Conti	06
Lockbit	27
Darkside	09
Revil	11
Black basta	09
Blackcat	07
Conti -B/^ Karakurt	11
Others	14

Sample size: *1647 attacks studied by Sectrio's threat researchers*
^ Data for 2022 before the group shut operations

Lockbit Group has also figured out a method to detect which affiliate is behind a specific attack. There are slight code-level variations in the core ransomware handed over to affiliates. This also helps the group evade evasions or attempts to use the ransomware without the knowledge or permission of the group.

The Lockbit ecosystem today includes affiliates, payment enablers, target seekers, reconnaissance planners, and executors, and lure setters. Each of these agents is either directly recruited by Lockbit or are on the rolls of the affiliates. Once a target is shortlisted, the chain of actions is triggered till the ransom is obtained and distributed among the agents, the affiliates, and the group. The whole operation is more streamlined and less prone to disruption as compared to other ransomware groups such as Blackcat.

According to back-of-the-envelope calculations and data from footprint analysis, over 70 groups are affiliated with Lockbit. A majority of these affiliations are from groups that are also working with other ransomware groups as well but there are almost 37 groups that working exclusively with Lockbit as of Dec 30th 2022. Lockbit's affiliates are tiered according to various factors.

Lockbit affiliate tiers

Parameter	Tiers
Previous instances of successful breaches	Unknown
Previous affiliation with Conti or other well-known ransom groups	Tier 1
History of developing malware independently	Tier 1
Revenue	Unknown
Number of Members	Unknown
Desired State affiliations	Tier 1
Operations in key countries	Unknown

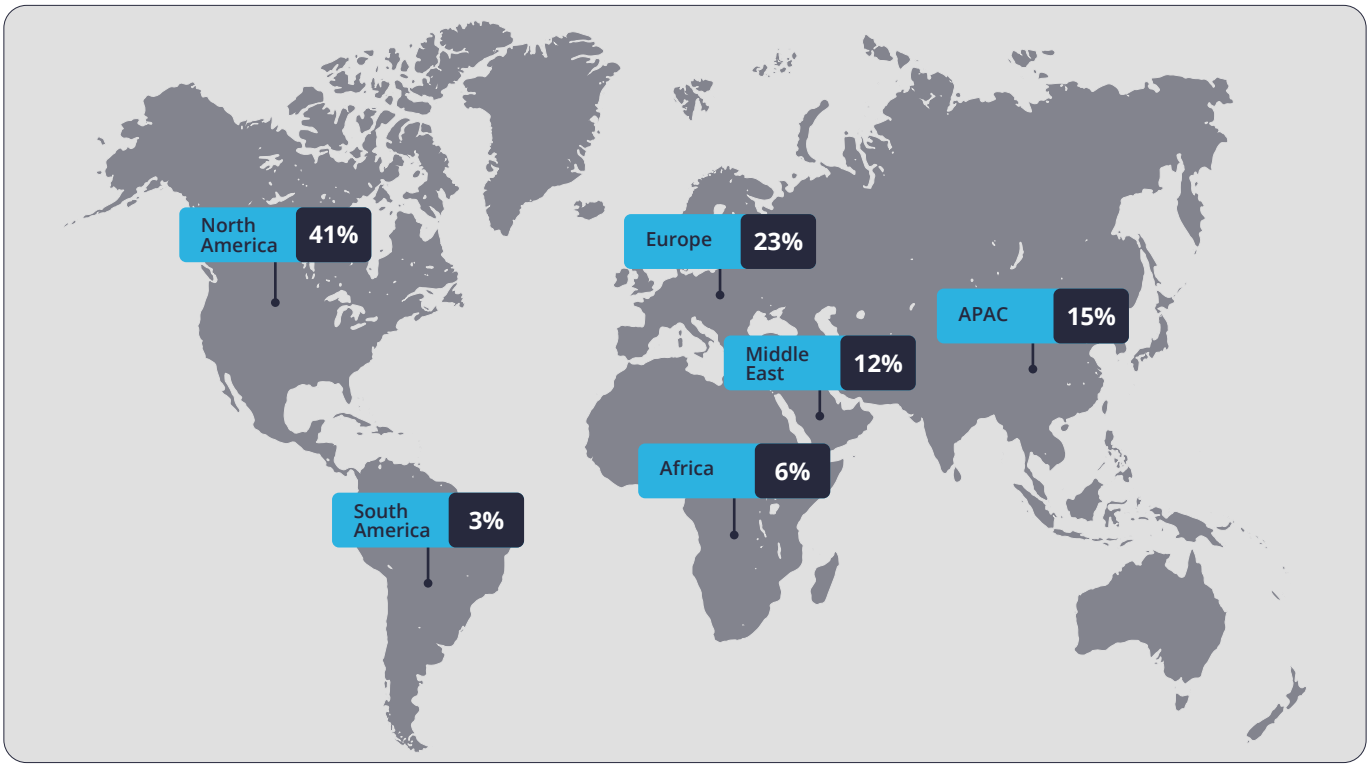
These tiers are changed based on the level of revenue that these groups are bringing to Lockbit.

At least 3 Lockbit affiliate groups are also working closely with hacktivist groups to target specific corporations for large-scale disruption of operations.

Black Basta

The Black Basta ransomware-as-a-service (RaaS) was first spotted in the wild in early 2022. The group behind Black Basta works with extremely short malware development and launch cycles. It works in a targeted manner and the level of discipline that it's affiliated actors have shown indicates the backing or at the very least some form of influence of an APT actor. Black Basta detections remain low as the group follows a highly targeted approach when it comes to selecting victims. The group has expanded its arsenal by inducting Quackbot trojan, Black Basta will be one of the main groups to track in 2023.

Geographical distribution of cyberattack on IoT and OT in 2022



Which countries are getting attacked and why?

Geopolitical instability and active APT players set the narrative for cyberattacks in 2022. Attacks on Ukraine, the US, the UK, India, UAE, Lithuania, France, and South Korea had strong geopolitical undertones. While the targets are diverse, as far origin of cyberattacks (including scans) goes, as many as 51 percent of all attacks were traced back to China. Russia came in second followed by North Korea. For this assessment, we have only considered cyberattacks that could be clearly attributed to an APT actor. In cases of ambiguity or where the origin was not clear, we have tagged those attacks to 'others'. Others does not include countries that accounted for less than 4 percent of the overall attacks logged.

OT-specific attacks were targeted at countries with a significant industrial footprint and those possessing a large OT-powered critical infrastructure landscape. While hackers operate more democratically when it comes to scans, they use more discretion when it comes to escalating the scanning into a full-fledged attack. There could be many reasons for this. As per our analysis, most of the scans on OT networks are now automated and conducted using automated tools. During these scans, hackers use port scanning and network vulnerability scanning tools to identify security gaps to exploit.

Public networks and IP obfuscation is commonly used to hide tracks.

The chain of events often follows the below sequence.

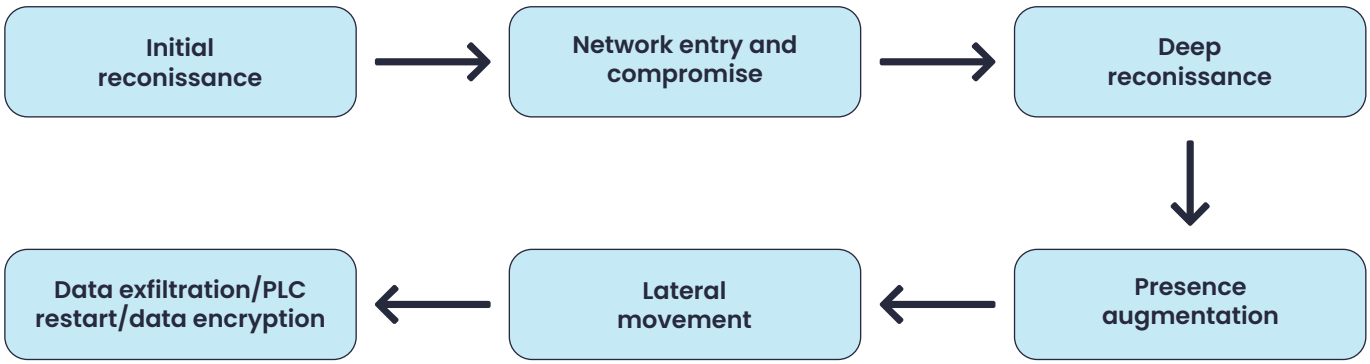


Table: Percentage of attacks tagged to the countries of origin

Country of origin with less room for error in attribution	Tiers
China	41
Russia	21
North Korea	13
Iran	04
Pakistan	04
Others	09

- China also accounts for the maximum number of active APT groups. As many as 11 groups including loosely affiliated actors belonging to China were tracked by Sectrio's threat research team in 2022. The definition of an active APT threat actor covers the following parameters:
- Has been active for at least 2 quarters (consecutive or otherwise) in the assessment year [highly active]
- The group should involve actors engaged in targeting and/or scouting for potential targets
- Any APT actor that has shown some form of activity in 90 days at a stretch is considered active
- Those APT actors that traded data or resources at least once in the year are also considered as active
- In the case of APT groups that shared their resources with another group, the group that received the services of the hacker was considered active (with a score of one). While the APT group that shared the resource was considered active for half a count (or .5). Two instances of half counts add up to full activity while if a group gets only half a count throughout the year is considered inactive.

Table: top countries of origin for APT actors

Country	Number of APT groups (active)
China	11
North Korea	01
Iran	02
Pakistan	04
Others	50

In case of non-APT actors, we logged cyberattacks from groups operating from a wide range of countries.

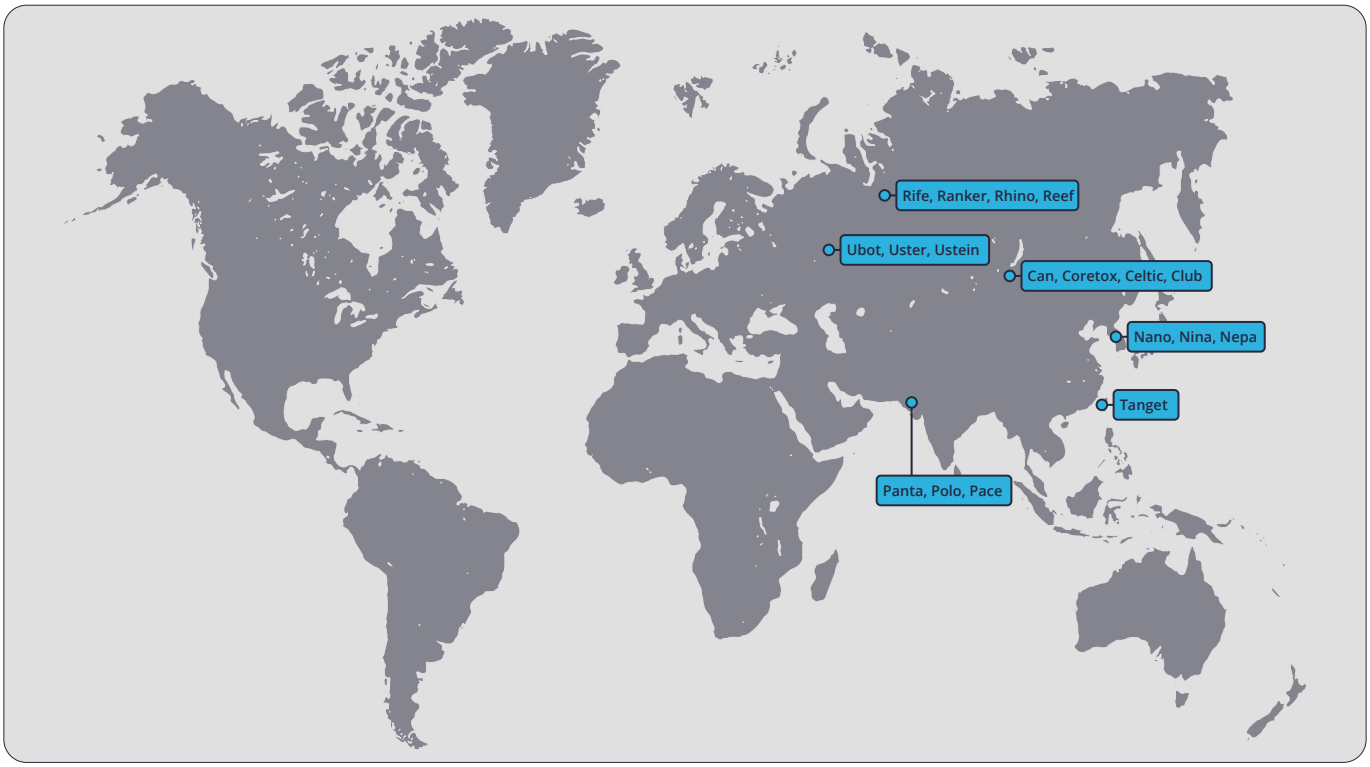
Table: What is being attacked and why?

Sector	Target	Why?
Manufacturing	Safety systems, IIoT deployments, shop floor controllers, HMIs, monitoring systems,	Data theft, ransom, large-scale disruption, geopolitical factors
Healthcare	Internet of Medical Things devices, high-value health care machines that run on legacy systems	Patient data theft, ransom, lack of adequate cybersecurity measures
Defense	Communication systems, controllers, theater and situation monitoring hardware, weapon systems	Data theft, intelligence, data on movement and use of weapon systems, injection of laterally moving malware to infect the entire chain of command structure inactive and cold combat zones
Pharmaceutical/ drug manufacturers	Assembly lines, data	Disruption of vaccination manufacture and manufacture of critical drugs
Smart cities	IoT deployments including devices and platforms, command and control centers last-mile connected devices (may or may not be part of a large IoT deployment such as standalone pollution monitoring devices)	Citizen data, long-term targeting,
Utilities	HMIs, control systems at various levels, monitoring systems	Geo-politics, ransom, data theft, manipulation of bills, and revenue diversion
Oil and gas	Upstream, midstream, and downstream assets, control systems, HMIs, LORA, and short-range connectivity-based networks	Primarily geopolitics
Maritime	Ships, navigation and communication equipment, offshore OT installations connected with cargo management	Ransom

The link between cyberattacks and inflation in select countries

State sponsored threat actors are targeting food production across major agro-economies. Simultaneously they are also targeting oil and gas producers and renewable energy producers and nuclear power plants. While on the surface these may not seem linked, when one connects the dots in terms of the way the sectors are targeted, a pattern emerges. Such attacks are designed to increase the prices of essential goods and services at one level that leads to an overall rise in inflation. Most of the attacks we have seen in 2022 are targeting those very sectors that have a direct impact on inflation. From oil pipelines to small agricultural farms, there is an attempt to create conditions for uncontrolled inflation by calibrating the attacks in time to target specific enterprises within sectors.

Key APT cluster under observation



The rising cost of ransom

The cost of ransom continued its upward trajectory for the third consecutive year. In 2021, the average cost of recovering a GB of encrypted data stood at USD 50,000. Even if the businesses that fell victim ended up paying the ransom, some of them did not get their data back. Some of them found their data being released on the Dark Web and other places.

Table 2:
Cost per GB of data as demanded by hackers and what was paid by the victim businesses^

Year	The approximate ransom demanded by hackers per GB (Demand) (USD)	Cost per GB (Paid by the victim organization)	Sample size* (Number of incidents)
2016	4975	4900	23
2017	7600	7000	26
2018	10,000	9000	35
2019	14,567	12000	41
2020	27,340	22,045	49
2021	50,000	39,000	51
2022	54,990	49,044	82

* Number of incidents studied where the information was sufficient to arrive at the ransom numbers
^ The ransom demand varies according to the threat actor, size of the data, victim, and complexity of the malware used

While the rise in ransom demand per GB may seem less, what is concerning is the rise in the number of incidents. The number of incidents refers to incidents for which we have a full set of data available and we were able to validate at least some part of the information from more than one source. Due to the increase in the number of hackers associated with groups like Lockbit (which ran a recruitment campaign on Telegram in the first half of 2022), the number of active hacker groups has grown and so have the attacks. New groups or even affiliates charge less ransom as compared to established players who often have to sustain large operations and wage bills.
The large increase in incidents are also due to many instances of healthcare and academic institutions reporting cyberattacks. The ransom demand placed by hackers to institutions from these two sectors is significantly less when compared to sectors such as oil and gas and manufacturing.

In over 85 percent of breaches cases from the healthcare and education sectors that we studied in 2022, the negotiations between the victims and hackers were conducted directly without the involvement of negotiators who often take a commission from the ransom collected. In the absence of negotiators (who are often professionals who are not in the direct rolls of the hackers),

Attacks on sectors

The significant rise in attacks on healthcare is not surprising. After the attacks on UK NHS in 2017, many hackers started taking more interest in this sector. Small and medium healthcare providers whose data was encrypted ended up paying ransoms to free their data (sometimes multiple times) and many of these attacks are yet to be shared with the patients affected, regulators and governments, and citizens alike as many of these incidents are still under wraps.

The rise in attacks on the utility sector is primarily driven by a huge rise in attacks in this sector in Europe where renewable energy projects and transmission infrastructure was scanned and attacked extensively.

Increasing attacks on key sectors

Sector	Trend
Healthcare	85 ↑
Energy	81 ↑
Manufacturing	71 ↑
Critical infrastructure excluding energy/utilities and oil and gas pipeline and infra	66 ↑
Oil and gas	66 ↑
Education	61 ↑
Banking and Finance	44 ↑
Defense	39 ↑
Retail	33 ↑
Smart devices	31 ↑
Others including agriculture, public safety, unspecified projects, and telematics projects not falling under the above categories	42 ↑

Top countries of origin of cyberattacks

Country	Percentage
China	21
North Korea	07
Iran	04
Russia	05
Ukraine	03
Others	27

Most attacked countries in cyberspace

While the center of gravity for cyberattacks continued to remain around North America, attacks on Europe did rise significantly. A significant proportion of these attacks were directed against energy and oil and gas infrastructure in the region. In addition, media houses and government agencies, and not-for-profit institutions also reported a rise in cyberattacks. Overall, hackers have tried to bring more institutions on their radar in 2022 to monetize more of their attacks. This again is due to the addition of newer threat players affiliated with groups like Lockbit.

Most attacked countries

Country	Rank
USA	01
India	02
United Kingdom	03
Canada	04
France	05
Ukraine	06
Germany	07
Australia	08
UAE	09
Singapore	10

Most attacked countries on a per capita basis

To explore another dimension of the impact of cyberattacks on various countries, we decided to bring the population of countries into the picture. This number is arrived at by considering the number of cyberattacks logged per citizen of that country. Based on the population source Worldometer, Ukraine comes as the number one country on this parameter.

Table: Countries drawing maximum number of cyberattacks on a per capita basis

Country	Rank
Ukraine	01
Lithuania	02
Finland	03
Israel	04
Taiwan	05
Belarus	06
Sweden	07
Chile	08
Oman	09
Estonia	10

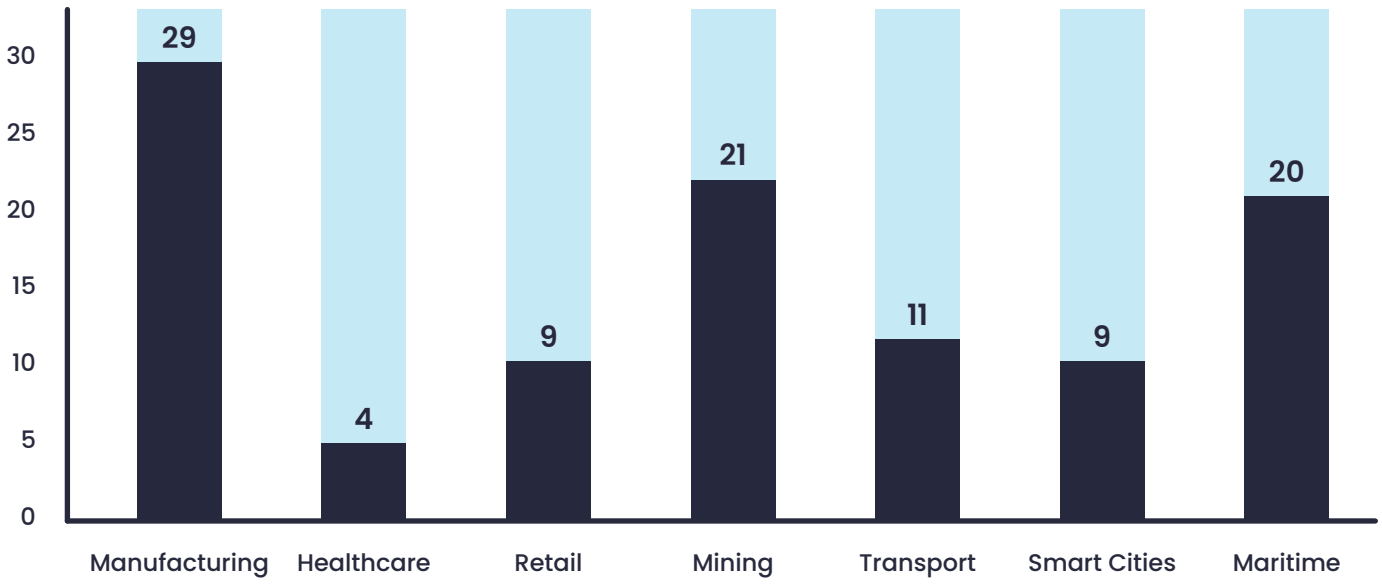
Population source: Worldometer, 2023 data

Cities drawing the maximum cyberattacks

If any evidence was needed to understand the influence of geopolitics in cyberspace, then one just has to parse the list of the most-attacked cities in the world. Many East European cities made their debut in the top 10 list in 2022. Most of these cities drew attacks from Russian, Chinese, and Iranian APTs. Over 60 percent of attacks on Vilnius were traced to Chinese APT players. There is no evidence to prove that these attacks were carried out in collaboration by these APT groups but we can say with a high degree of certainty that these attacks were clearly motivated by geo-political considerations.

City	Rank in 2022	Rank in 2021
New York	01	03
Kiev	02	06
Tokyo	03	-
Talin\Prague	04	-
New Delhi	05	05
Vilnius	06	-
Dubai	07	07
Oslo	08	-
London	09	02
Washington D.C	10	01

Days taken to monetize a cyberattack in 2022



Time to monetize

This is another telling statistic. The time taken to monetize a cyberattack is the lowest in the healthcare sector. This is because many healthcare institutions are pressurized to give ransom quickly so that the patients and those requiring urgent medical attention do not have to be kept away from any required intervention. Smart cities and projects falling in that domain is another sector where the time to pay the ransom is less as data of citizens or citizen services are at risk.

Overall, we saw a small dip (less than one percent) in the time taken to pay ransoms across the board. This means that hackers are now monetizing their cyberattacks faster.

Days took to discover a cyberattack rises

From an average of under 180 days in 2021, this number has gone to 220 days now. If one looks purely at reconnaissance scans, then the number could be even higher as are not noticed or are ignored post-detection and not taken up for analysis.

Average time to transfer data to C&C servers (lab \ virtual environment)

Nature of data	Average observed Transfer window/frequency of communication with C&C
Credentials \ proprietary \ IP based \ confidential	2-4 hours post-injection of data
Network analytics info	8 hour 20 minutes or more
Normal/routine traffic	9 hours or more
From trojanized firmware	24 hours or more

Malware (including variants) sample size for the test: 15000
Target sectors: manufacturing, telcos, healthcare, smart cities, defense, shipping and utilities

The average price of sophisticated malware fell in 2022. This could be because of the easy availability of malware variants from groups such as Lockbit.

The cost of reconnaissance tools fell significantly as many APT players and others made these accessible for free.

Key traits in malware detected around the world (sample size 7796 unique malware)

Trait	Trait detection rates (in percentage)	Geographic distribution or focus	Verticals targeted
Persistence	High 58 Med 32 Low 10	North America, Western Europe, and SE Asia	Manufacturing and critical infrastructure projects
High levels of stealth	76	Global	Defense, healthcare-connected vehicles, and manufacturing
Faster deployment	81	Global	Almost all verticals
Crypto mining	29	All except Latin America	Smart cities and manufacturing
High network mobility plus Lateral movement	65	Global	Manufacturing, smart cities, Defence, telecom

Malware sources

In 2022, many unidentified sources of malware were added to the mix of sources. Due to this, we were unable to clearly identify the sources of such malware in circulation. This indicates three things.

- Most of the sophisticated malware comes from countries that are either engaged in a conflict or are involved in some way. We saw this in Ukraine and Armenia.
- Enablers and level two actors are obfuscating the header information and other properties to hide their origin. We were however able to detect their presence through proprietary technology used by our research team that detects even the stealthiest malware out there.
- Hackers want to cover their tracks all the way
- Undiscovered malware forums are trading in complex malware

State-backed APT actors remained active throughout 2022. The high-profile attacks (and even the low-profile but critical ones) on gas pipelines, utility infrastructure, and project management software, and other applications indicate an attempt by them to create pathways to open networks to deploy malware and for long-term snooping and network access.

Within critical infrastructure, availability is a key parameter of operational significance. With many OT environments running legacy systems that lack vulnerability assessments and patches as also access management and controls have increased. The maturity of security programs needs to be improved and the protection of cyber-physical systems needs to be elevated as an immediate priority.

Operational technology (OT) availability and uptime are the primary concerns within the critical infrastructure sector. Taking down a critical system for maintenance could result in a power outage or a loss of access to drinking water. Therefore, many OT environments are running legacy systems that lag vulnerability patches and other updates.

The enablers are also acting as third-party conduits facilitating the exchange of sophisticated malware, vulnerability information, and stolen data are also enabling the exchange of malware between friendly APT groups to maintain a level of plausible deniability and distance.

Malware origin

Possible Source	Percentage detected
Dark web	25
Procured via malware forums	18
Mixed	09
Military-grade	03
Academic\research labs	03
Unknown	42

At one of our research labs, we were able to segregate malware based on observed traits, deep content inspection, multi-layer inspection and analysis, and code slicing. Using dual sandboxing and some of our proprietary techniques, we were also able to do a behavior analysis and stealth evaluation. While the properties of malware keep changing, the baseline trait that all malware share is stealth and persistence.

This year saw the release of a huge cache of malware developed in what seems to be academic or research facilities. This is because many of these malware had code inserts and traits that do not belong to any known malware labs we have seen in the past. Malware development is sometimes a complex process with many actors collaborating and sharing inputs. Sometimes, malware developers also build their malware on a base code developed by labs in academic institutions or facilities belonging to government agencies.

Top Ports attacked

Port	Attacks in million
23 -Telnet	700
445 - SMB	305
22 SSH	297
1433 MSSQL	380
3306 MySQL	559
80 - HTTP	680
7547 - CWMP	45
25 - SMTP	87
20 FTP	98
Others	16

Types of attacks and frequency

Types	Percentage occurrence
Integrity violation with malicious code Injection	21
Brute force attacks	11
Phishing emails	1/week/org
Privilege abuse	08
DoS and variants	11
Simple reconnaissance	05
Persistent reconnaissance	18
Port/asset scan/TCP dump (specific recon)	10
Firmware downgrade attempts (corrosion)	07
Crypto mining/jacking	09

CISO sentiment in 2022

Between April and June 2022, Sectrio conducted its first Annual CISO Peer Survey. The objective was to understand the security, budgeting, manpower, operational and strategic challenges that CISOs were facing and how CISOs were addressing these challenges. The findings of the survey were captured in the form of a comprehensive report. This report covered specific aspects related to:

- The biggest security, manpower, skilling, and risk management challenges the CISOs are dealing with today.
- Disruptive industrial trends and tech acquisition roadmap CISOs are tracking for the next 12 months.
- Pain points that CISOs are working on such as lack of network visibility stressed manpower, and a deteriorating threat environment.
- Insights on how are CISOs leveraging their existing tech landscape to secure the IT-OT-IoT convergence and digital transformation outcomes.

Key findings of the survey

- 41 percent of CISOs feel they have a fully operational and relevant dashboard that delivers all the information they need.
- 55 percent are finding it difficult to prioritize security alerts.
- 70 percent are overwhelmed by false positives
- 65 percent do not have the right tools to deal with emerging threats.
- 59 percent feel the threat environment had deteriorated in the last 12 months
- Over 90 percent reported at least one major cyber incident in the last 18 months

These responses help us in developing a deeper understanding of the context in which the global threat landscape is evolving and the responses from businesses that are shaping and influencing this evolution. We would urge you to read this report here[5].

Over to the regions.

North America

Cyberattacks on North American enterprises and government agencies continue to rise. In 2022, we saw a 267 percent rise in attacks across sectors. Manufacturing, healthcare, critical infrastructure (utilities and water treatment), start-ups and oil and gas were the most impacted sectors in the region. Businesses hosting complex environments with a mix of IT-OT and OT-IT and IoT were most impacted by this surge in attacks. The US continues to be the most attacked country in the world attracting almost 9 percent of all cyberattacks.

North America dominates the digital transformation market globally. It is today home to the maximum number of digital transformation projects according to multiple studies. On the threat front, the US continues to be the center of attention drawing scans and attacks from a range of countries. US networks are probed by APT and non-APT groups from Iran, North Korea, China, Russia, and even nations that are not known to host hackers or APT actors.

Such a high volume of attacks focused on a few sectors does magnify the potential for a breach. There have been instances of overlapping attacks wherein, a payload deployment attempt by a hacker group was followed by a similar attempt using either a whole new malware or a variant by another hacker group.

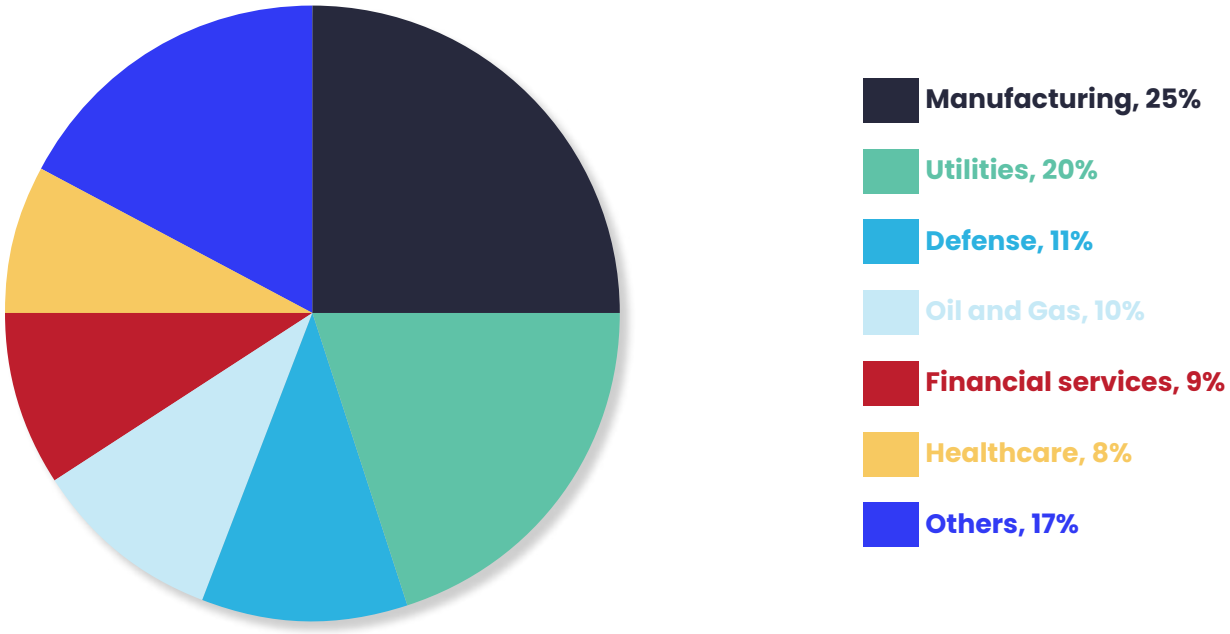
In the case of US businesses, info-stealing malware has been used to augment data stolen from social media outlets such as Twitter to create a breach profile for employees working in sensitive locations and roles. Such profiles and exfiltrated credential data are then fed into AI tools that then work to churn out potential access credentials. A business email compromise is commonly caused this way.

Key facilities in the region are under constant surveillance by hacker groups globally. In the oil and gas sector, a separate unit of the GRU (code-named **слo** within GRU) has been stalking oil and gas facilities including refineries, pipelines, and offshore oil facilities. **слo** operates with some of the highest known levels of persistence with an average session lasting 310 days at a stretch.

A payload deployed by **слo** in February 2022 in an offshore rig near Louisiana caused a partial shutdown of the facility.

In the manufacturing sector, cyberattacks are primarily targeted at facilities running multiple OT systems across locations. This includes facilities that have a mix of legacy and new OT systems and a hint of IIoT as well. Overall, the motivation behind these attacks is purely ransom. A Lockbit encryptor with North America-specific updates to target specific installations in the region was also located in the wild by our threat research team. With the onboarding of many former Conti hackers many of whom have targeted North American businesses extensively in the past, Lockbit now has good insights into the infrastructure it is targeting in North America.

Sectors drawing Cyberattacks in North America



Manufacturing continues to account for a significant share of cyberattacks. In addition to inherent vulnerabilities in industrial networks hosted by many manufacturers in North America, the increasing complexity of asset interactions and legacy factors are together contributing to this sector becoming a soft target for hackers.

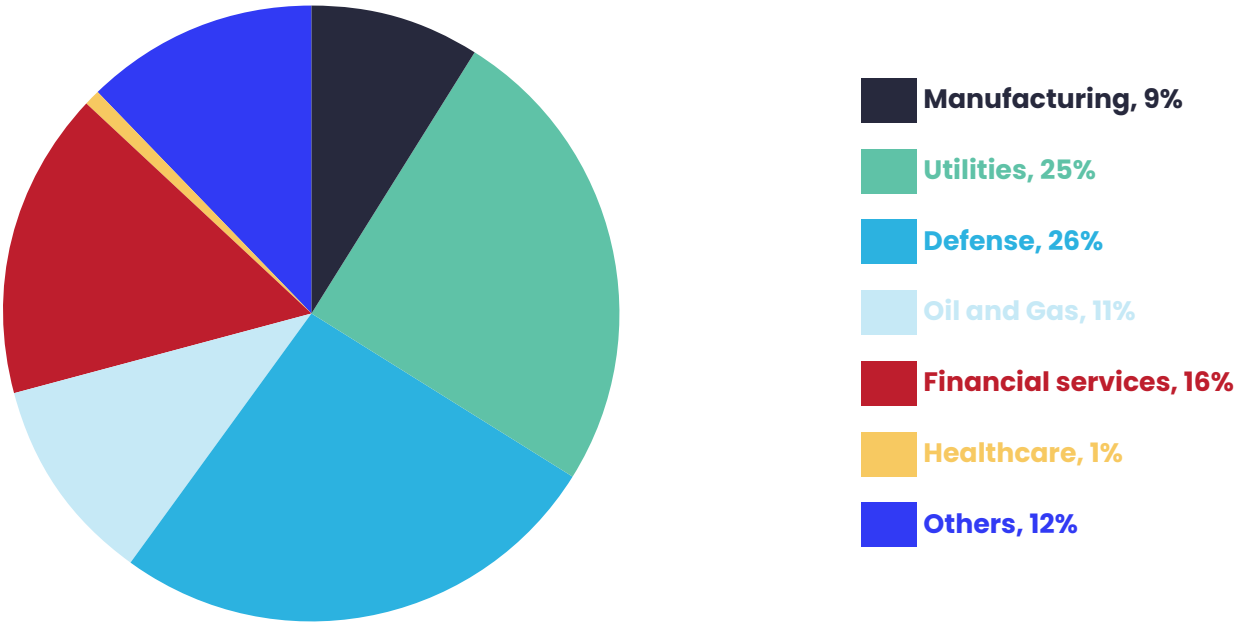
As per our 2022 CISO survey, North American manufacturers have started expanding their investments in Industry 4.0 across the board. This has added a new wrinkle to the asset complexity challenge mentioned earlier. While 43 percent of manufacturers were investing in some form of asset rationalization and infrastructure through practices such as vendor consolidation and legacy system replacement, the sheer volume and diversity of assets that need urgent attention is turning the task of infrastructure rationalization into a herculean task. This factor is having a major say in the way manufacturing assets are defended in cyberspace.

The sector is also under pressure from extended supply chains. Post-Covid-19, many North American manufacturers diversified their input sources. A few established vendors were replaced by new ones as manufacturers tried to stabilize their supply chains and production. The entry of new players brought in new challenges as some of the new suppliers did not follow robust cybersecurity practices and their products deployed in the infrastructure of North American manufacturers served as conduits for entry of scans and malicious payloads.

While manufacturing companies are facing quantitatively superior cyberattacks, the utility sector is dealing with cyberattacks that are qualitatively superior. This sector faces a direct threat from nation-state actors, hacktivists, and organized cybercriminal gangs. The aging grid infrastructure in North America is contributing significantly to the security challenge. Elements of the overall grid infrastructure are exposed to the internet at various points.

The US General Accounting Office (GAO)[6] notes that the grid distribution systems—which carry electricity from transmission systems to consumers—" have grown more vulnerable, in part because their operational technology increasingly allows remote access and connections to business networks. This could allow threat actors to access those systems and potentially disrupt operations."

Percentage of sophisticated attacks



In addition, there are three clear threats to the power infrastructure in North America these include:

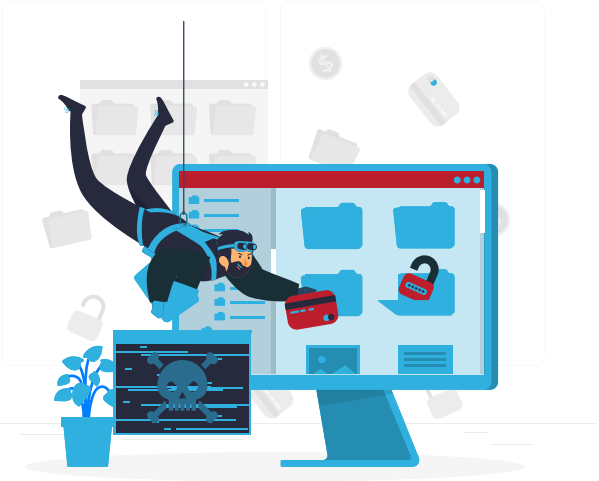
Involuntary botnets: when electronic devices connected to the internet are hijacked by malicious threat actors, they can then use these devices to launch DDoS attacks or even modify the power consumption pattern to put additional load on the grid.

Industrial Control Systems: use of legacy systems and lack of visibility into core operations involving such devices has created a security gap in the power infrastructure. Devices that use traditional protocols can present a significant threat surface area to an attacker who can then selectively shut down key control elements to create a massive disruption

Timing-based operations: at a grid level the utility infrastructure is dependent on accurate timing to monitor and control generation, transmission, load management and distribution. If these dependencies are exploited, then a grid-level event could occur. Hackers have already gathered plenty of information on the power infrastructure in North America. Such information can be used during times of geopolitical discord or can even be sold to adversarial nations and entities by these very hackers.

The power sector in North America needs urgent security attention.

Another sector that is drawing the attention of hackers in North America is defense and aerospace. With the presence of a huge defense-industrial complex in the region, hackers with varying levels of affiliation are targeting defense and aerospace firms in North America. North Korea, China, and Iran are the three countries contributing the maximum cyber attention to the region's defense installations.



Impact of the Ukraine war on North American cyberspace

In March 2022, while the conflict in Ukraine intensified, the Chinese APTs group and a possible affiliate stepped up their cyber reconnaissance missions inside North America. At the same time, several Russian groups were also logged trying to target multiple institutions and networks including those belonging to academic institutions in US and Canada. In Mexico, several focused manufacturing businesses and oil companies came under the radar of Russian, Chinese, and Iranian hackers.

Chinese groups in fact tried to spoof some of the attacks to pass them off as originating in Russia. Russian hackers in turn attacked many businesses especially those connected with defense supply chains using multiple variants of Wiper malware that wipes out data instead of encrypting it. Such attacks picked up momentum in early 2022 but soon petered out as ransomware-dominated attacks became mainstream again.

Networks of several Mexican companies were used as launchpads to target US and Canada. Some forms of tunneling and IP obfuscation cannot be ruled out as well to trick cyber forensic analysts and investigators to conclude that these attacks were being carried out from within Mexico. In the case of spear phishing campaigns, we found the same tactic being used as several spoofed email IDs used in these campaigns belonged to companies based in Mexico.

The Colonial Pipeline attack continues to haunt critical infrastructure and beyond.

In many ways, the Colonial Pipeline incident was easily among the most disruptive cyberattack on US soil. It also showcased the many shortcomings in the way businesses manage their cybersecurity needs and underscored the need to improve many facets of institutional cyber risk and security management practices. By shutting down the entire pipeline, the company showed that it didn't know which part of its infrastructure was impacted and how the impact could be contained.

Through this incident alone, the hackers were able to showcase their ability to disrupt critical infrastructure at will. While a slew of energy companies were attacked by hackers in 2021 across North America, the problem is not restricted to the energy sector alone. Even businesses in segments like healthcare, manufacturing, utilities, shipping, and defense were targeted by hackers

The hackers went by a tested playbook to target companies and the most common factor among the targeted companies were:

- Lack of visibility into operations across the infrastructure
- Lack of cyber attack deflection capability
- In most companies, security teams were understaffed or didn't have the capability or quality threat intelligence to detect the attacks early
- While compliance is a driving factor for improving risk management methods, many businesses left parts of their infrastructure out of the purview of complex mandates
- Overworked SOC teams: in some instances, the SOC teams had not adopted frameworks such as the MITRE attack framework, IEC 62443 and Zero Trust. This led to the SOC and cybersecurity teams being burdened with lots of false positives to analyze
- Lack of automated threat hunting
- Facilities having OT were dealing with another set of problems
    - OT security is not audited and no reports are created or studied
    - OT devices were not being inventoried
    - The patching schedule was ad hoc and dictated by the availability of spare time
    - OT was left unmonitored

Ransomware and APT actors active in the region

This table outlines the frequency of detection of the footprint of the most common threat actors in the world in North American networks. In 2022, many ransom payments were negotiated directly by the hacker groups themselves. This could be attributed to many instances of payment disputes that arose in early 2021. Additionally, many ransom negotiation groups had also hiked up their commissions as the ransom demand increased.

Group	Percent Occurrence
Lockbit	27
Blackcat	13
Killnet	9
Lapsu$	08
Lazarus	08
APT 41	07
APT 28	03
Others	25

South and Central America

This region witnessed a 60 percent (year-on-year) rise in attacks. All sectors tracked by us in the region reported a rise in inbound attacks. South America is steadfastly climbing the charts to become a lucrative region for APT hackers and there are multiple reasons for this including:

- Interest in commodity production and trade in the region
- The growing digitization and adoption of technology across sectors
- Some of the non-APT actors seem to be visiting the region as we discovered many times in 2022 when we found out that 3 major Lockbit affiliated hacker groups had visited the same city in Brazil at different times before March 2022
- Hackers are able to replicate their attacks at scale in the region
- Cyberespionage
- There are Portuguese and Spanish speaking APT groups as understood from the codes we uncovered in the malware used
- Integration of manufacturers in the region with global supply chains

As geopolitical fault lines globally and in the region expand, newer APT actors will emerge in the region and these actors will exhibit more or similar behaviors as compared to their counterparts in other parts of the world. APT actors in the region have not been studied in depth so far. They have evaded closer analysis at many points in time. Thus from the shadows of inattention from threat researchers and cyber defenders, many regional APT groups have emerged that are now defining or rather redefining the contours of the threat landscape in the region.

With increasing cyberattacks in the region, it is essential to understand other specific factors that are contributing actively to this trend. Manufacturing, mining, agriculture, and forestry[7] are among the key contributors to the region's GDP. Brazil is the largest country in the region both in terms of size, GDP, and diversification of economic output. With the region working towards greater integration with global supply chains, there is a clear impetus for higher adoption of technology and its deployment for creating value-added products that feed into these supply chains.

Oil production in the region is dominated by Argentina, Brazil, Colombia, Mexico, and Venezuela[8]. Guyana is increasing its oil output to become a leading global player[9,10]. All these countries are home to extensive and diversified facilities for the exploration, extraction, and transport of oil within and outside the region.

This region has received plenty of cyber attention from hacker groups based in China and Russia.

Most of the information exfiltrated concerns:

- Data on extraction and processing of minerals and petroleum products
- Information on purchases and potential purchases of commodities
- Data on software deployed on shop floors
- Data on maritime trade
- Information on lawmakers and influencers

Most attacked countries in the region

Country	Percentage of attacks
Brazil	14
Peru	13
Argentina	11
Uruguay	10
Columbia	07
Chile	05
Ecuador	05
Bolivia	03
Others	32

In terms of volume, Brazil accounts for the biggest percentage of attacks logged in the region. These attacks target a range of verticals including aerospace, defense, maritime, oil and gas, and financial services. Since Brazil's economy is more diversified, it gets a range of attacks across verticals and draws the attention of bad actors who do not target other countries. For instance, Brazil is attacked by a Croatian threat actor Blue Spring which is exclusively after Brazilian aerospace.

Table: Most attacked sectors

Sector	Percentage
Manufacturing	27
Oil and gas	19
Financial services	15
Government	10
Healthcare	09

The IP and process information theft, integration of supply chains, and easy extortion of ransom are driving factors for the cyberattacks on the manufacturing sector.

The oil and gas sector in Argentina, Brazil, Colombia, Mexico, and Venezuela is among the most targeted sectors in the world (it is the second most targeted sector in the region). When one looks exclusively at the oil and gas sector alone, Venezuela gets the 4th rank after UAE, Saudi Arabia, Kuwait, and Iran. This is a telling statistic as it reveals the sectoral preferences of hackers. Bad actors after monetary goals often find the oil and gas sector more lucrative especially when it comes to dealing with sensitive data and higher volumes of ransom. Listed oil and gas companies also deal with price-sensitive information – the disclosure of which could influence stock price movement on stock exchanges and consequently the profits made by equity and commodity traders. It wouldn't take a stretch of the imagination to consider that bad actors are monetizing stolen data in multiple ways and the stock markets may be presenting one such avenue.

North Korean Lazarus has been active in the region since 2015. In 2019, they infiltrated the networks of a company that interconnects the ATM infrastructure of all Chilean banks. Chile and Brazil have been in the crosshairs of Lazarus since a while and based on information obtained from chatter, Lazarus maintains a high level of interest in the whole region. In addition to periodic snooping, Lazarus also seems to have recruited allies in the region.

Regional APTs

In 2013, the Russian GRU trained the cyber offense wing of a major South American country giving rise to what could potentially be the first APT actor of the region. As of today, there are at least 5 APT groups operational in the region. It is hard to trace their lineage but we can say with a fair bit of certainty that the operations of these groups are fairly limited and that a bulk of the cyberattacks in the region come from China, North Korea, Russia and Iran.

Common traits of regional APT players

- Fairly lengthy periods of reconnaissance scans
- While most are motivated by some of financial gain (48 percent), 31 percent of attacks are motivated by the need to steal data for various reasons followed by the need to snoop (11 percent)
- Attacks on governments and embassies, financial systems are done using the most sophisticated malware
- Public malware codes have been used extensively to build RATs
- Some APT players are also used to attack hacktivist groups and protest groups

Europe

Countries in Europe attracted attacks across sectors. The region reported a 310 percent rise in cyberattacks during 2022. 4 regional trends impacted cyberspace in the region in 2022:

- The Russo-Ukrainian conflict
- The rising prices of commodities globally
- Rise of generative AI
- Post-pandemic realignment of threat actors and groups

The war in Ukraine was a tectonic event at various levels. It impacted the overall security fabric of the region in addition to impacting security in cyberspace. Cyberattacks across Eastern Europe rose at never before seen rates and due to the rising cyber incidents, many enterprises ended up losing revenue and data.

To understand the impact of the Ukraine conflict on European cyberspace, we need to see the changes that have come to bear since the conflict began in February 2022. These changes can be studied by analyzing these parameters:

- The volume of sophisticated cyberattacks
- Quality of attacks and target deviations
- Failed intrusion attempts
- Sectors targeted.
- Motivations

Other than these, we must bring the magnifying glass on attacks on high value targets like NATO stations and bases, large oil and gas infrastructure, government agencies and think tanks, and armed forces belonging to countries in the region. Of higher interest will be the attacks on targets that are directly or indirectly linked to war.

The volume of sophisticated attacks

Type of attacks	2021	2022
DDoS	2,22,000	3,98,000
Brute force	1,00,900	2,45,000
MiTM	56,099	89,001
SQL injection	37,300	41,508
Ad-based targeting	7000 plus ad instances	Over 10,000 ad instances
Phishing	17,00,667	33,98,834
Device hijack	1,29,000	3,10,000
Scans	56,43,420	74,20,939
Others	5,44,988	7,55,000

The number of phishing attacks in the region almost doubled in 2022. During the same period, the quality of intrusion attempts also saw a significant improvement. While in 2020 and 2021, most payload deployment attempts were via phishing, in 2022, hackers invested more energy in deploying lures after studying the behavior of their targets online to get them to engage with infected sites without having to send emails or targeted SMSs. Instead, hackers used content on third-party platforms and paid ads to get their targets to engage.

Such a direct mode of targeting eliminates many X factors and increases the chances of success for the hacker. While the numbers may seem low when compared to phishing, our threat research team believes that more of these may have gone undetected across forums and other gated online communities. Russian and Chinese APT groups such as APT 29 and APT 41 are now switching to an AD and targeted approach to reach potential victims.

Where are the cyber threats to Europe coming from?

Country of origin	Main actors	Percentage
Russian	APT 29, SEABORGIUM	29
China	APT 41	22
Iran	APT 35, Static Kitten	09
Pakistan	Transparent Tribe/Mythic Leopard	05
North Korea	Lazarus	03
Others		32

Most attacked countries

Country	Rank
United Kingdom	01
France	02
Ukraine	03
Germany	04
Finland	05

France and the UK are drawing a huge volume of sophisticated attacks on their manufacturing infrastructure linked to defense. While Ukraine is in the third position, attacks on Ukraine rose by as much as 566 percent in 2022 which is unprecedented. Ukraine, Lithuania, and Finland top the list of most attacked nations in Europe on a per capita basis.

What is getting attacked?

Sector	Percentage of overall attacks logged
Utilities	16
Manufacturing	12
Oil and gas	09
Defense facilities and supply chains	07
Critical infrastructure other than the above	06
Healthcare	05
Education	05
Others	40

Germany and UK house many facilities connected with NATO. During the annual Operation Hedgehog conducted by NATO in May, all participating countries reported a rise in phishing emails and attacks as well. While the attacks in May were not intense it was certainly of a higher quality with the involvement of multi-payload malware and wiper malware families targeting institutions as diverse as oil and gas refiners and weather monitoring stations.

There were also some early signs of collaboration in some manner between APT groups from Russia and China. In many cases post a breach, there were signs of snooping by a Russian APT group in case the breach was effected by a Chinese actor and vice versa. The link could however be circumstantial, but such instances are now occurring too frequently to dismiss such a link exclusively on an incidental basis.

Threat actors from Iran and Pakistan were also found snooping in the networks belonging to government bodies, NATO, research bodies, and think tanks. Threat actors from both countries tried exfiltrating data from their targets to servers based in South-East Asian countries and they were then downloaded on personal drives and carried back to their respective countries. This was an attempt at obfuscating the last mile details to prevent the original threat actors and countries from being exposed. Sectrio has confirmed the existence of such a circuitous journey for stolen data from multiple credible sources.

Attacks on Ukraine

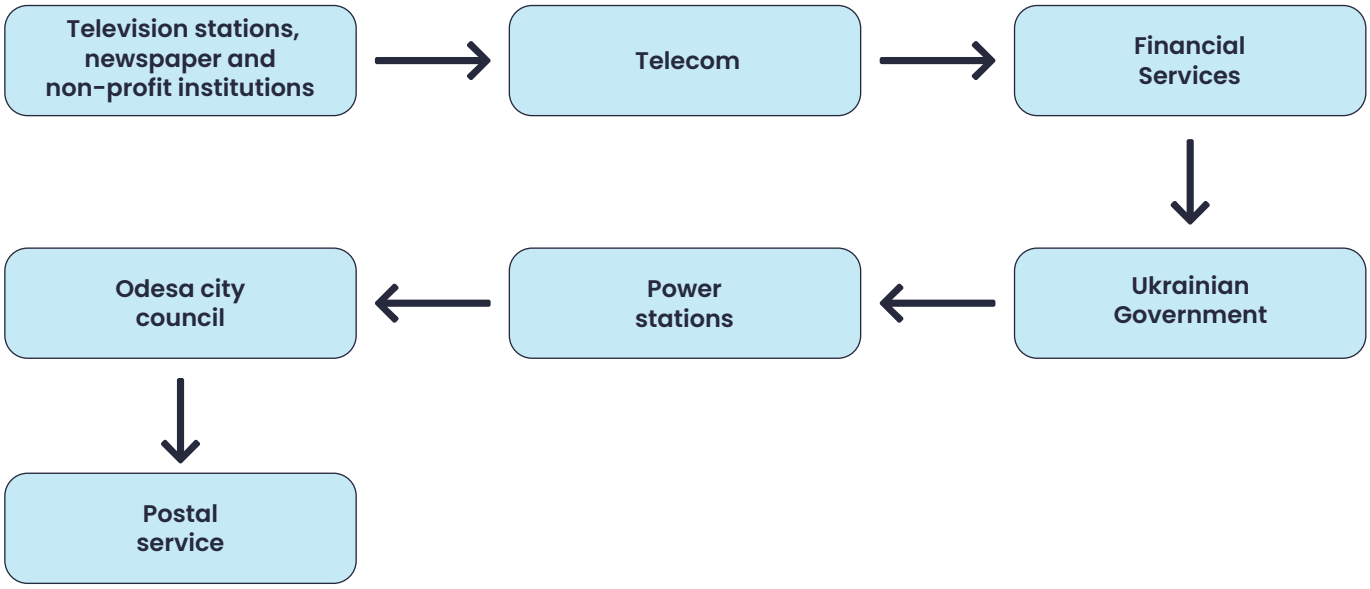
After the attacks on the Ukrainian energy sector in 2015, Ukraine was subject to multiple attacks in the 2016-2022 period. Hackers had extensively used the NotPetyamalware liberally to target nuclear power plants, public institutions, banks, not-for-profit agencies, postal services, newspapers, critical infrastructure, and businesses. Even the Chornobyl power plant was not spared. In most instances, drives were directly impacted and rendered unusable. While these attacks were part of a wider global campaign, Ukraine was singled out for a more intense wave of attacks.

Between 2018 and 2021, hackers went after critical infrastructure in Ukraine with security services and water plants being exclusively targeted. In each attack, hackers exfiltrated data and left residual snooping loiterware on multiple devices to enable future access to core systems. The hackers were certainly preparing the ground for more widespread attacks in the future and that is exactly what transpired in 2022.

In previous editions of the Threat Landscape Report, we have studied the evolution of attacks in Ukraine in detail. We would like to draw your attention to specific research published in 2020 and 2022 which spoke about how hackers were using cyberspace in Ukraine as a testing ground for testing new variants of malware. In 2022, Russian hackers using a rudimentary playbook went about attacking multiple institutional pillars of Ukrainian society starting Feb 2022. While many of these attacks were repelled some did manage to get through disrupting operations and shutting down many institutions in their wake.

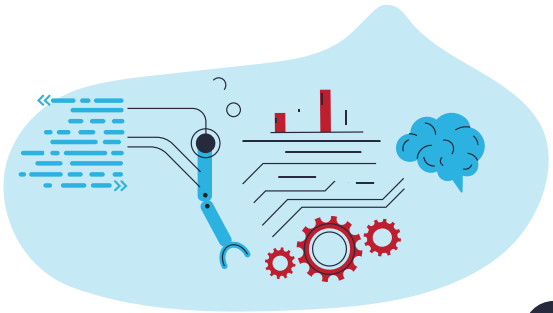
Deepfakes have also been unleashed along with some of these attacks to increase the impact of breaches. In one notable instance, in the second half of March 2022, Russian hackers launched a concerted effort to target television stations in UK and Ukraine. CaddyWiper was the malware in this case. A fake video was also circulated showing Ukrainian President Zelensky asking Ukrainians to surrender. The hackers were certainly working with a plan targeting key institutions to disconnect Ukrainian citizens from vital services to create a sense of panic and fear in phases.

The sequence of attacks on Ukraine



- **Vectors:** CaddyWiper and Marsinfo stealer

- **Tactics:** the first leg of the hybrid warfare launched by Russian hackers involved information which is why sources of information were targeted first. In the second phase, telecom infrastructure was targeted to disperse malware to the maximum number of systems in cyberspace. Using telecom infrastructure and targeted phishing, the financial services sector is then targeted to disrupt the payments infrastructure to block access to funds. In the next phase, the government itself along with critical infrastructure is targeted to tie down the government machinery (all this is happening while the government is trying to make sense of the deteriorating threat environment slowing down the quality and timeliness of a response).
- While the cyberattacks on Ukraine failed to create the desired impact it has still added a few chapters to the playbooks that hackers will use in the near and far terms. They are many takeaways for defenders and hackers from the whole episode. Here are some of the key takeaways for security planners:
- While cyberattacks may emerge from out of the blue, no major attack can happen without years of probing, hacking, and data exfiltration. It is this chain that has to be broken. Unless measures are taken to harden infrastructure or periodically bring in changes in the infrastructure that eliminate old practices and/or components, it will be difficult to avoid breaches that result from such attacks.
- Knowing the intention of cyber adversaries is important to understand the tactics and methods they may use.
- If one can learn from past mistakes to improve security and bring in a culture that values security and is invested in it at all levels, cyberattacks can be prevented to a large extent
- A war zone will attract attention from all kinds of APT groups
- With AI, hackers can also game responses, architectural specifics, and other attributes of the infrastructure you are trying to protect. Such games can improve targeting and bring forth better outcomes for the adversary. However, by breaking the chain and rendering exfiltrated datasets unusable, hackers can be prevented from succeeding



The axis of cyberattacks in Europe

Most cyberattacks within Europe have concentrated within a radius of approximately 700 miles from Ukraine away from Russia (North, South, and Western Europe). This zone doesn't just log the maximum attacks but some of the hijacked assets in this area are serving as a conduit to enable further cyberattacks on Ukraine and the Baltic countries. Finland lies just outside this zone. This landmass in this area falls within what we call Zone 1.

Zone two is the zone that lies outside this zone stretching up to approximately 1600 miles from Ukraine this region also faces attacks but the volume is much lesser than that of Zone 1. While the vectors and tactics are more or less common, the degree of hacker interest is what makes this region stand out.

This axis clearly indicates that Ukraine is more or less at the center of cyber attention as far as hackers go. While geographical distances don't matter as far as cyberspace is concerned, the existence of such an axis indicates high levels of hacker interest in these countries because of the proximity to the war zone. At various points of time in 2022, unusual patterns of internet traffic were observed in countries falling within zone 1. These patterns were linked to ongoing cyberattacks and intrusion attempts logged across Europe.

Top Zone 1 countries and the volume of associated cyberattacks

Country	Volume
Ukraine	Around 14 percent
Finland	08
Lithuania	07
Estonia	07
Latvia	05

Cumulatively these countries account for over 50 percent of all cyberattacks on Europe. In terms of per capita attacks as well, these countries draw nearly as many attacks per person as Kuwait. Which is in itself a telling statistic.

Common tactics, techniques, and procedures used by hackers in Europe

Cyberattacks in Europe grew significantly in 2022. Hackers deployed many TTPs in Europe first before they were deployed elsewhere. Let's now look at some of the most common TTPs used by hackers in Europe in 2022.

- Large-scale spear-phishing campaigns
- Persistent and focused attacks on specific targets
- Stealthy, long-term scans and reconnaissance
- Attacks on personal devices and routers to sniff traffic
- Modified use of tools and techniques from previous attacks
- Information hoarding (data is not released)
- Password spraying
- Credential harvesting
- ICS shutdowns

Chinese APT groups also increased their footprint in the region in 2022. Some of these groups such as Goblin Panda which is among the most active Chinese APT groups restarted their operations in Europe in 2022. This group is notorious for its ability to target air-gapped systems to deploy RATs targeted government bodies, tech companies, manufacturing entities, and start-ups. By using similar tactics and even malware in some cases.

Among institutions, media agencies and television stations were repeatedly hacked into along with not-for-profit bodies. All such attacks had one thing in common. Russian and Chinese APT groups were taking turns attacking them. A television station in Kiev was attacked by a Chinese actor hours after it was attacked by Russian APT 28. The hackers followed a scorched earth policy to obliterate data without exfiltrating any information.

Espionage operations

A Russian identified as SEABORGIUM maintained a level of vigil across the region. While focusing on weapons and troop locations, it also snooped on NATO bases across Europe. Across the region, critical infrastructure was attacked with intensity and persistence to gather every ounce of data available. Such data was then filtered using data mining structures and expansive cloud infrastructure.

In late August, the Balkan republic of Montenegro faced an unprecedented wave of attacks. The digital infrastructure connected with public services in the country went offline after ransomware encrypted data residing on multiple servers. While the country was dealing with these attacks, Finland, Romania, and Estonia also reported attacks across sectors. These

brazen attacks represent years of probing, data exfiltration, incident, and threat response analysis, and system behavior modeling across systems and geographies. As we have seen in the case of Ukraine, the level of specificity and the ability to time these attacks to specific geo-political and geo-economic triggers indicates a very high level of planning and sophistication.

Asia-Pacific and Oceania

Few countries in this region have started attracting a huge chunk of the overall volume of cyberattacks logged across the globe. Sectors such as utilities, smart city projects, financial services, manufacturing, and regional critical infrastructure are being targeted by players within and outside the region.

Rapid digitization without paying adequate attention to security is taking its toll on businesses across sectors in the region. In order to understand the undercurrents defining security trends here, one needs to go back a few years.

From 2011 onwards the adoption of CCTV cameras grew exponentially in the region. Even now, according to various estimates, the segment is expected to continue to grow well into the next decade. Such a massive adoption of CCTV cameras has created a significant security challenge in APAC.

Sectrio's threat research team has continued to see a steep rise in botnet traffic from networks connected with security cameras. In some instances, even the control centers connected with such cameras seem to have been breached. Such cameras have also provided hackers an easy entry into the IT, OT, and IoT networks of businesses in the region and if one were to go by past trends, it becomes even more apparent that many businesses are yet to realize that their networks have been compromised. Such compromises are proving to be the proverbial Achilles Heel for corporate and government entities in the region.

Some businesses that were worrying about the recurring attacks on their systems and OT shutdowns should now look at two aspects of their operations:

- Infected CCTV cameras still connected to corporate networks
- OT networks that are openly accessible from other networks

The geopolitical fault lines that have come to define the cybersecurity threat landscape in Europe have cast their shadows in APAC and Oceania. Such an impact is more apparent in countries such as Australia, India, Vietnam, and Singapore. In countries such as Malaysia, Thailand, Indonesia, and others, sub-regional factors were at play wherein local hackers dominated the threat landscape. Other than the factors mentioned earlier, the easy availability of malware and the extensive use of variants to beat signature-based threat detection engines is also rampant.

Taiwan and India continue to be ranked high on the list of the most attacked nations in APAC. The attacks on Taiwan have been traced to countries in the region and beyond. Iran, Russia, and China together account for almost 60 percent of all attacks logged in the region and this comes as no surprise. But what is indeed baffling is the extent of infiltration that Chinese threat actors have managed to achieve in India and Taiwan.

Asia-Pacific is home to nearly 40 APT players. At any given point in time, as many as 10 of them are active (involved in attacks or breach attempts) while another 5 are in probing mode or mapping exploits. These numbers vary based on factors such as geopolitical triggers, availability of new malware/exploit, and even the time of the year.

Most attacked countries in the region

Country	Percentage of attacks
India	15
Taiwan	14
LithuAustraliaania	12
Vietnam	11
Indonesia	09
Thailand	09
Japan	08
Others	22

When it comes to inbound cyberattacks, India and Taiwan are almost neck to neck. Taiwan receives a huge volume of direct cyberattacks from mainland China. Most of the qualitative attacks are directed toward critical infrastructure including power grids and army bases. The low-grade high volume attacks are targeted toward retail stores, smart home devices, CCTV cameras, and home routers.

Taiwan's manufacturing infrastructure especially those connected with high-end manufacturing is also logging a huge volume of cyberattacks. Many of these attacks occur in diffused formats at various times of the day and are designed to probe various networks connected with these facilities.

Specific regional tactics

Chinese APT 41 is quite active in India, Australia, and Taiwan. In these 3 countries, it runs reconnaissance campaigns extending to months at a stretch. On gaining a foothold in a network, an affiliated hacker deploys a multi-loader malware often with hatches for hosting malware payloads designed to cater to objectives such as prolonged snooping, data exfiltration, privilege modification, network hopping (lateral movement), and firmware embedding. APT 41 has been discovered lurking in many networks in the region. The data exfiltrated by it never makes it to any forum or hacker data sites.

APT 41 is the flagship hacker group of China and its expanding and sometimes uncontested presence in the region presents significant threats to regional security. Lazarus is another group that is active in many parts of APAC including India (primary targets: financial services and government), Australia (financial services and commodities), Japan (financial services, entertainment), Taiwan (Government, manufacturing), and Malaysia (financial services).

Table: Most attacked sectors in the region

Sector	Percentage
Manufacturing	27
Defense	22
Government	17
Oil and gas	11
Financial services	12
Maritime and logistics	07
Healthcare	04

The reason for increasing attacks in APAC has been covered in detail before. Now let's look at why certain sectors are drawing more attacks.

Many manufacturing firms in APAC deploy legacy systems, relies less on patching discipline, don't customize workflows to a level where it becomes difficult to target them, uses common passwords with multiple admins, and run OT-linked networks that are accessible from anywhere. The time to patch systems is also very high in APAC and all of these factors contribute to the sector becoming an easy target for hackers. Sectors such as oil and gas, utilities, and maritime to some extent also suffer from similar problems.

Lazarus and its regional affiliates and many small-time hackers are responsible for most of the attacks on the financial services sector (organized and unorganized). Lazarus targets systems linked to financial institutions and wallets that are less secure and contain significant amounts of money or NFTs. Lazarus' affiliates also operate under various names such as Crypt Punk and Rx factor. Both of whom have been implicated in multiple instances of NFT theft in APAC. These groups are nothing but smokescreens for Lazarus to operate with a semblance of plausible deniability.

India

India is among the most attacked countries in the world for the last 4 years. This year, the country received cyber attention from state and non-state hacker groups based in North Korea, China, Iran, Russia, and Pakistan. The only set of actors who maintain a persistent vigil in Indian cyberspace belongs to China which is presently involved in exfiltrating huge volumes of data from India. Such data is being used to run the intelligence conveyer belts mentioned earlier. Such data is also validated using intelligence gathered from the field. Such data is collected by the planned intrusion of Chinese forces across land and air frontiers.

Through such data, China tries to maintain a high level of situational awareness of its adversaries and their capabilities. While the cyber and physical intrusions into India are nowhere close to that of China in Taiwan, the quality of attacks does indicate a cause for concern. The attacks on Indian power infrastructure that have been ongoing since 2010 continue to escalate. The attacks on the power infrastructure in various states are all part of a coordinated effort to initiate and sustain a high level of reconnaissance activity in Indian strategic cyberspace.

The volume of cyberattacks in India registered a 96 percent growth in 2022. The sectors that are under the scanner of hackers include healthcare,

manufacturing, government, defense, public sector enterprises, and oil and gas. These are sectors of strategic national interest. In each of these sectors, hackers are working towards a mix of objectives.

Table: Strategy and objectives behind the targeted sectors

Sector	Strategy and objective
Manufacturing	Exfiltrate production information and process IP. Identify and examine the scope for exploiting the data
Defense	Gathering information on troop movement and deployment, hardware capability, defense procurement, infrastructure expansion in border areas, production in ordinance factories
Public sector enterprises	Vendor data for potential opportunities, landscape mapping, intrusion into core networks for maintaining a long-term presence
Power and utilities	Maintain an ability to disrupt the normal functioning of plants and distribution infrastructure
Oil and gas	Gathering data on production, infiltration into core and critical systems and networks, enable maintaining an ability to shut down key systems, gather info on key personnel
Healthcare	Gather information on the health status of key decision-makers
Government	Exfiltrating information
Conglomerates	Data on investments in domestic and overseas projects

APT 41 is the most active and evolved threat actor in India. This group blends intelligence operations with random data exfiltration (as was the case in AIIMS) to confuse any attempts to decipher attack motives. As per the information available and deciphered by our threat researchers, China's MSS has divided Indian cyberspace into 14 zones. All APT groups maintained by MSS follow the same zoning when it comes to choosing their targets in India.

Zone one: includes all frontline defense-related networks, ballistic defense sites, sea-going assets

Zone two: digital assets connected with Indian decision-makers in their official and personal capacities

Zone three: utility superstructures including grids, water treatment plants, and ports

Zone four: financial super assets such as stock exchanges and big banks

Zone five: telecom and communication highways and submarine cable landing stations

Zone six: connected remotely accessible infrastructure in towns near the border

Zone seven: healthcare organizations with exposure to decision-makers or influential persons

Zone eight: IP-rich enterprises and start-ups

Zone nine: foreign MNCs with supply chain access to OECD countries

Zone ten: aerospace assets independent of Zone one but with significant commercial value

Zone 11: networks connected to hydrogeographic systems and weather monitoring

Zone 12: strategic assets linked to or based in Andaman and Nicobar Islands

Zone 13: data centers

Zone 14: digital assets linked to disaster management

Each zone is dealt with differently when it comes to probing and creating a breach. The time for reconnaissance exploits targeted, amount of data exfiltrated and threat actors assigned by MSS vary according to the zone. APT 41 often appears in attacks on Zone 7 and above.

In addition to Chinese APT groups, Iranian APT 34, Russian APT 28, and Pakistani Transparent Tribe have also been discovered in Indian networks. APT 34 is often associated with highly specific geopolitical triggers involving Iran's neighbors. In the aftermath of the Russo-Ukraine war, for nearly a month, many APT actors retreated from Indian cyberspace. Lazarus and APT 41 however were still around.

Independent threat actors operating with leased malware are also active in Indian cyberspace. Most of these actors target enterprises running on OT and IoT.

Scale of data theft

Data exfiltrated from Indian systems and networks are among the biggest datasets that are up for sale on the Dark Web and other forums. A typical data dump could involve anywhere from 200 records all the way to 10,00,000 records. The prices range from as less as 0.5 cents a record all the way to $10.

Most of the data has been exfiltrated from app-based service providers. Such data is relatively cheap to procure. Data from conglomerates and large enterprises is however costly and hard to procure. Such data is available for sale none the less.

In addition to credentials, direct access to networks belonging to large enterprises is also up for sale. This includes details of open ports and static IP ranges for targeting.

Percentage attacks of various types

Type	Percentage occurrence*	Mapped to (IP ranges in _ number of countries
VPN exploit	11	02
Website SQL injection	02	03
Connected device manipulation (remote)	07	02
Workstation RAT injection/scans	14	02
Device patch altering	09	03
Spearphishing	09	Masked
Watering hole attack using fake sites	04	03
Data exfiltration through rogue devices and twining	02	01
Phased DDoS (inbound)	06	02
Brute force email compromise	06	02
Safety instrumentation modification	04	02
Code injection attempts	11	02
Reconissance (long term)	15	02
*As a total of the overall attacks logged	100	

Compromise attempts logged (Severe instances only) in the manufacturing sector in India (Sept-Dec 2022)

Nature of malware detected in this sector (Sept-Dec 2022)

Type	Occurrence
Downloaders (Bughatch, Bumblebee, and variants)	10
Cryptominers	03
Lockbit 3.0 Variant	07
Scanners and RAT precursors	11
Sophisticated ransomware (Cuba group, Bumble bee, and above)	31
Unknown malware being tested/AI-based malware	19
RAT	19

Target systems

Top target systems in inbound attacks	Percent
PLCs	18
Generic IT	17
SCADA workstations	19
Firmware	04
Processes related to software	04
Safety instrumented systems	02
Thermostat	06
Mill control	04
Cyber-physical monitoring systems	09
Production management systems	05
Output control	02
Unspecified HMI systems	03
ERP	02
Unknown	05

The AIIMS attack: breaching the healthcare frontier.

- India's All India Institute of Medical Sciences, Delhi faced a cyberattack on November 23, paralyzing its servers. According to various sources, up to 1.3 GB of data was encrypted. The encryption was a smokescreen created by a Chinese APT actor. This was done to hide the real purpose of the attack which was to exfiltrate healthcare records of senior decision makers in the Indian government. Few other healthcare providers were also attacked in the following days just to give the impression that the attacks were carried out at random. We believe this attack has generated a playbook for other Chinese APT groups to follow. More such attacks across the globe could be expected in the near future
- Our threat research team has drawn the following inferences after studying the attack and its aftermath.
- Personal email ids and passwords belonging to key AIIMS personnel were already exposed in previous breaches and were openly available on the Dark Web. Almost all the personal email addresses linked to key personnel mentioned on the AIIMS website are appearing on multiple breach DBs. Some of the personal password link to procurement websites which indicate the use of these accounts for official procurement transactions. It is therefore possible that some of these passwords were reused for accessing official email accounts. These compromised credentials could have provided the hackers more avenues to study network usage and associated vulnerabilities and vulnerable apps to hack into.
- Using the stolen credentials from data dumps, hackers could have gained access to the files and data stored on the cloud or on machines belonging to employees (including folders where crucial information and sometimes even passwords could have been saved by employees.
- Based on the above information, it is possible that the hackers were shadowing the institute including its 40 physical servers and 100 virtual servers for some time, stealing data or accessing parts of its networks for some time.
- The stolen data could potentially include health data belonging to VVIPs which could provide state-backed hackers and their sponsors' access to important information on the health profile of key decision-makers.
- The hackers seem to be using the ransom as a façade to deceive investigators. It is possible that the hackers were after the health records of key people and are using the ransom as a pretext to hide their true motives.
    - No sample data (stolen or exfiltrated) has been released after a breach. Hackers often release sample data and use pressure-building tactics to put added pressure on the victim. We have not seen this happening so far.
    - The ransom demand works out to about INR 200 or 2.45 USD per affected record which seems to be quite less. Lazarus which was behind the Wannacry attack in 2017 could have potentially netted USD 60000000 from the attack [at the rate of USD 300 per machine affected based on the initial ransom demand]
    - Data encryption could also help mask the tracks of the hacker, especially if they are an APT group to prevent attribution.
- The Healthcare sector in India uses legacy systems quite liberally and because these systems are no longer updated, they cannot support the installation of anti-malware measures. Such systems are sitting ducks when it comes to cyberattacks. In some instances they may be running key functions in others they house patient or asset information
- The accessed databases contain PII

Virtual bot farms

In many parts of APAC, many elements of critical infrastructure have been subject to incessant probing from a wide range of IPs. APT elements and independent threat actors are targeting these nations using the digital infrastructure of other countries. Such attacks are routed through cyber loops running across the telecom infrastructure of the conduit countries where digital twins of real IoT devices are used to generate infected bot traffic.

These bot farms are not even real as in they don't even have real devices. Such virtual bot farms are easy to establish and run. They are monitored by using AI which eliminates the need for manual monitoring. Such farms can be turned on and off easily and even moved to new IP sets for hosting at a minute's notice. They can evade detection for a long time unless they are located using specific tools. This is a very unique use case for digital twins.

Middle East and Africa

- Volatility in the threat environment trigged by bad actors increasing their activity in the region defined the major cyber events manifested as a result of this trend. The role of cyberspace as a battleground continues to expand as bad actors ramp up their game in the search for new targets to exploit and data to harvest.
- The number of cyberattacks aimed at causing a kinetic impact rose by almost 188 percent in 2022. The implications of such a rise will be felt in 2023 when many attacks may breach the kinetic threshold and display a visible impact resulting in outcomes that will not be acceptable.
- Hackers have clearly moved goals to target physical disruption that than the virtual one they were targeting till 2022. The other cyber security major trends that we recorded in the region include:
- The emergence of three new APT actors in the region.
- Utilities and manufacturing were the most targeted sectors across the Middle East
- 69 percent of all attacks had geopolitical undertones. The rest were predominantly motivated by monetary considerations
- Chinese and Iranian APT activity in the region touches an all-time high
- Oil and gas is a sector that is under the radar of bad actors globally and ME is no exception in this regard
- About 80 percent of all businesses across large and small segments have been scanned in 2022. That is also a new high

The rise in scans and the rise in successful cyberattacks are also linked to the use of ransomware such as Lockbit 3.0 by regional groups and independent actors. The democratization of cyberattacks involving regional threat actors and acquired ransomware has brought a whole new dimension to the challenge of securing businesses in the region.

The attacks on critical infrastructure including ports, telecom networks, water and power plants, and power distribution infrastructure by APT players from within the Middle East and beyond continued on predictable lines. Large-scale disruption was the clear intent and APT actors continue to run scans and maintain a high level of interest in networks connected with critical infrastructure in the Middle East.

Table: What is getting attacked?

Sector	Percentage
Utilities	35
Manufacturing	29
Oil and gas	11
Financial services	06
Government	06
Healthcare	06
Others including Not for Profit bodies	07

Table: Motivation factor for bad actors

Factor	Percentage
Geo-political intent	69
Monetary considerations	15
IP/Data Theft	10
Rogue insider	03
Unknown	03

Table: Top APT groups in the region

Name(s)	Country of origin	Target countries
APT 34 OilRig, Helix Kitten, GreenBug, IRN2	Iran	UAE, Saudi Arabia, Oman
APT 35 Newscaster, Rocket Kitten, Phosphorus, Charming Kitten, Saffron Rose	Iran	The whole of the Middle East
APT 39 – Chafer	Iran	Middle East
APT 41	China	Middle East
APT 28	Russia	UAE, Saudi, and Egypt

Groups from China targeted the data centers belonging to financial services institutions and utility companies extensively in 2022. We believe that these units are being attacked not just for data but also for their strategic value and to exploit the access that these facilities provide to multiple networks and locations. Across 5 attacks that we studied in 2022, we were able to identify attempts to deploy infostealers and loiterware designed to stay hidden on networks to be activated later.

While Oil and Gas ranks number 3 in the list of most attacked sectors, it is a sector that gets the maximum number of sophisticated attacks. These include long-term listening attacks on core networks to sniff data of interest and stealthy movement across networks to ensure persistence and presence in as many networks as possible.

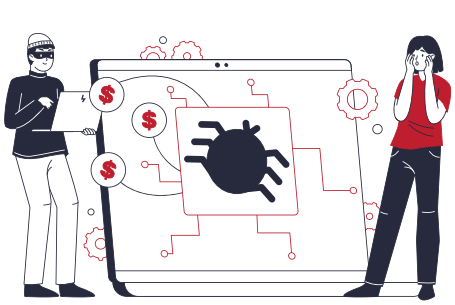
In the case of IoT devices, certain pre-infected ones studied by our threat research team were found to be rigged at the firmware level to enable the deployment of trojans and backdoors. Smart cameras were the most rigged devices followed by smart fire alarms and medical sensors. Vulnerable IoMT devices are one of the reasons the sector is attracting so many attacks. The presence of such backdoors in multiple classes of IoT devices (at random) points to a sustained effort by bad actors to breach IoT projects to gain access to core networks.

The presence of these backdoors at random reduces the chances of their discovery during a random vulnerability assessment. An AI-based threat bot can use these devices to launch cyberattacks that are separated in time and space – this is what we call the sequential botnets which participate in cyber attacks at random intervals with varying IP ranges and thus are hard to detect.

The attacks on intelligent subsystems connected to sensors and data lakes in the region is also rising. This is especially true of projects in the infrastructure sector. In addition to pre-existing backdoors in such systems, many of them are being scanned at regular intervals from various IP ranges. The addition of IoT gateways to critical infrastructure systems including power and power backup systems is also leading to a deterioration in the security posture of the infrastructure associated with them.

Systemic attacks in the region

System	Percentage attacks
IT-OT	40
IT-IoT	19
IIoT	14
IoMT	08
Others	19



Most attacked countries in the region

Country	Rank
UAE	01
Saudi Arabia	02
Oman	03
Kuwait	04
Egypt	05
Nigeria	06
Kenya	07

On percapita basis, Kuwait was the most attacked country in the region. Kuwait drawing a disproportionate volume of attacks is chiefly due to the presence of facilities connected with the oil and gas sector.

Targeted attacks on utilities and oil and gas

Attacks on oil and gas and the utility sector in the region target almost all aspects of operations in these two sectors. Repeated incursions designed to cause sub-kinetic physical disruption in 2020 have now turned into more complex attacks designed to control sub-systems and use that control to unleash mayhem. Many of these attacks were discovered because of sheer carelessness on the part of the hacker. For instance, during one episode, the hacker (Witchetty group AKA APT 10) coded the wrong activation time for the vector to perform file and directory actions possibly due to a time zone difference and the malware was triggered during work hours and the anomalous activity was detected and neutralized. In another case, the C&C server address was wrong.

One is not sure why an actor as mature as APT 10 did these mistakes. But there is certainly a need to rapidly improve security practices in the region else we may see some of these attacks evolve and create more disruption and chaos, especially in the oil and gas sector where such attacks could also be coupled with airborne strikes by drones to create an even bigger impact. In the utility sector, bad actors are working to shut down critical systems and subsystems at will and to time such shutdowns to geopolitical triggers.

The football World Cup and cyberattacks

The Football World Cup hosted by Qatar also led to a rise in cyberattacks and inbound reconnaissance activity. The presence of large number of senior delegates, business and government leaders and tourists proved to be too attractive an opportunity to miss for the hackers. In the lead-up to the event, we logged a steady rise in cyberattacks and inbound phishing emails targeted at the event organizers and smart city and transport projects in Qatar. The attacks have since subsided but the threat has not reduced as the data exfiltrated during these attacks will be put to use to target many entities in the days to come.

Most of these attacks were directed toward workstations across industries. It looks like the bad actors were doing a complete sweep across networks to target as many devices and networks as possible for planting lurkware. Such a pattern of attacks will continue as the region hosts multi-national events. Hackers are clearly seeing these events as an opportunity to expand their operations in the region.

The playbook for such events is still a work in progress for hackers. APT actors from Iran were presumably acting under a directive from some authority to carry out coordinated and uncoordinated attacks.

What can the region look forward to in 2023?

The critical infrastructure in the region is witnessing an unprecedented expansion and the expanded threat surface that results from the phased digitization of projects is expected to continue in 2023. In the energy sector, countries in the Middle East are increasing their investments in green energy projects and hydrogen-based energy projects. In the next half a decade, the transition from traditional fuel sources to those based on non-conventional energy will spur the next wave of evolution of infrastructure-specific malware.

As control systems for such projects will be unique, they will be targeted using specific and built-to-order malware. Even before we get there, we are also seeing a rise in snooping on firms and projects that are in the early stages of conceptual development. Such snooping will intensify in 2023 as hackers seek more information on the specific capabilities of such projects.

The rise in Chinese APT activity is a trend that is here to stay. In 2023, more APT actors will be unleashed by China with multiple objectives. Preventing countries in the region from trading directly or indirectly with Taiwan will be a major factor. A major cyber physical breach leading to a kinetic event could occur this year. This is based on the extrapolation of the last 5 years of data on the impact of cyberattacks on cyber-physical systems in the region. We feel that such attacks could be catastrophic and could cause lasting damage to specific elements of critical infrastructure in the region.

By lasting damage we mean the time to recover from such attacks will easily be in the range of 3-5 years.

References

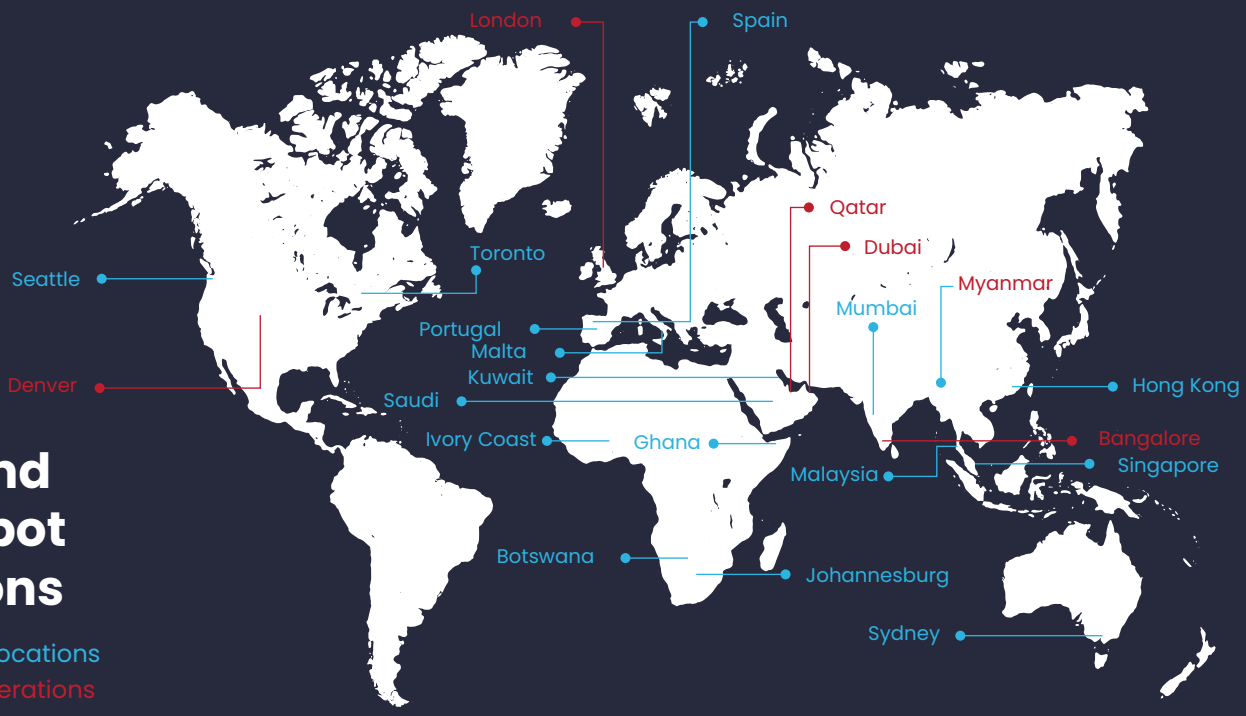
1. https://www.forbes.com/sites/forbestechcouncil/2022/10/21/cyber-insurance-premiums-are-up-and-thats-not-the-only-industry-shakeup/?sh=7dfe241e2290
2. https://www.secureworld.io/industry-news/cyber-insurance-pricing-increase
3. https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698#:~:text=Attribution%20is%20when%20an%20entity,from%20another%20state's%20computer%20networks.
4. https://www.cisa.gov/shields-up
5. https://sectrio.com/ebooks/the-ciso-peer-survey-2022-report/
6. https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks
7. https://en.wikipedia.org/wiki/Economy_of_South_America#:~:text=Now%2C%20major%20economic%20activities%20include,observing%20slowdown%20in%20growth%20rates.
8. https://wedc.org/export/market-intelligence/regions/central-south-america-caribbean/
9. https://www.investopedia.com/articles/investing/101315/biggest-oil-producers-latin-america.asp#:~:text=Argentina%2C%20Brazil%2C%20Colombia%2C%20Mexico,the%20world's%20top%20oil%20producers.
10. https://www.energypolicy.columbia.edu/latin-americas-enduring-new-oil-landscape/

Major cyberattacks in 2022

Date	Attack	Group
01-01-2022	Hackers attacked servers hosting the personal information of over half a million individuals receiving various services from the Red Cross and Red Crescent Movement. The hacked servers contained data related to the organization's Restoring Family Links services, which works to reconnect people separated by war, migration, and violence. The Red Cross took servers offline to stop this suspected attack by a nation-state, although no culprit has definitively been identified.	Unknown
01-02-2022	Malicious threat attackers claim responsibility for the attack at Novartis manufacturing plant. RNA & DNA-based drug technology and test data were stolen directly from the lab environment at Novartis claim the attackers	Industrial Spy
01-02-2022	System failure at Kojima industries in Japan faced a cyberattack causing disruptions and supply chain interruptions. Kojima industries One of the key suppliers of vital parts to the Japanese automaker Toyota Motors. The attack impacted 28 production lines in 14 plants for 4 days.	Unknown
23-03-2022	Italian Railway infrastructure was compromised and hackers may have got control of over 700 km of the railway network.	Russian APT Group
01-04-2022	Costa Rican government was attacked by Conti which took many government agencies offline.	Conti
13-04-2022	Industroyer2 and CaddyWiper malwares were used to target the Ukrainian power grid. CERT-UA claims to have taken preventative measures to foil the attacks on its critical infrastructure.	Russian APT Group
05-05-2022	ACGO fell victim to a cyberattack targetting modern farm machinery which was vulnerable to hacking.	Unknown
01-06-2022	A sophisticated ransomware attack on Yodel impacts logistics and disrupts operations, delaying deliveries across Europe	Unknown
01-06-2022	A broad range of operations, including IoT and OT devices, were brought to a halt in Palermo, Italy. Before the attack the Italian government had received threats by the pro Russian group hacktivist group Killnet	Russian APT Group
01-07-2022	A DDoS attack in July 2022 blocked access to the website of the Lithuanian energy company, Ignitis Group. Pro-Russia group Killnet claimed responsibility.	Russian APT Group
01-08-2022	The Russian "hacktivist" group, People's Cyber Army engages 7.25 million bots in August 2022 to take the Energoatom website down. The attack was part of a Russian psyops campaign to create fear of a nuclear disaster and terrorize Europeans.	Russian APT Group
01-08-2022	In August 2022, the South Staffordshire Water Company reported an attack that caused a network disruption in its internal corporate network and a data loss. A cybercriminal ransomware group threatened to tamper with the water supplied by the company. The criminals demanded payment to not release sensitive files and explain how the network breach happened.	Unknown
01-08-2022	The government of Montenegro's digital IT infrastructure reported an unprecedented cyberattack in August 2022. Certain governmental services and telecommunications experienced disruption, including border crossings and airport operations. The state-owned utility company, EPCG, switched to manual operations as a precautionary measure.	Unknown

Date	Attack	Group
01-06-2022	In July 2022, the Belgian government announced that three Chinese hacker groups, part of the known Chinese Advanced Persistent Threat actors, attacked Belgian public services and military defense forces.	Chinese APT group
01-08-2022	7-11 stores in Denmark close shops after cyberattacks bring down payment & checkout services	Unknown
06-09-2022	UK's top transport group 'Go Ahead' fell victim to a cyberattack when the organization detected unauthorized activity in its transport network infrastructure and is suspected that Telemetry data could have been compromised.	Unknown
13-10-2022	Unusual activity in internal systems at Medibank turns into ransom extortion in return for 200GB worth of customer data	Unknown
01-11-2022	Canada's largest prepared meats and poultry food producer faced outages and disruptions in operations in its manufacturing plants. The total cost of the incident was later revealed to be a massive impact of USD $16M	Unknown
23-11-2022	India's top healthcare institute falls victim to a ransomware attack in late November. Further investigation reveals objective may have been data exfiltration of high priority individuals within the country	Unknown
08-12-2022	A ransomware attack on a top media company, The Guardian in December cripples IT systems & forces Employees to work from home as a result of the attack	Unknown
01-01-2023	The ransomware incident at Atlantic General causes disruptions to critical systems and posed a potential risk to vital services in January as data exfiltration and extortion were believed to be the motive of the attack	Unknown
01-02-2023	A cyberattack impacting healthcare systems are forced to be taken offline and non-emergency processes are suspended at Tallahassee Healthcare memorial.	Unknown
02-03-2023	Sunpharma halts operations due to a major ransomware attack.	Unknown

ABOUT SECTRIO



ISOC and Honeypot Locations

- Honeypot Locations
- Security operations

Sectrio is a division of Subex Digital LLP, a wholly owned subsidiary of Subex Limited. Sectrio is a market and technology leader in the Internet of Things (IoT), Operational Technology (OT) and 5G Cybersecurity segments. We excel in securing the most critical assets, data, networks, supply chains, and device architectures across geographies and scale on a single platform. Sectrio today runs the largest IoT and OT focused threat intelligence gathering facility in the world. To learn more visit: www.sectrio.com

INDIA

Pritech Park-SEZ, Block 9,
4th Floor, B Wing, Survey
No. 51 to 64/4, Outer Ring Road,
Bellandur Village, Varthur Hobli
Bangalore – 560 103

Tel : +91 80 6659 8700
Fax : +91 80 6696 3333

AMERICAS

Westminster:
1499 W. 120th Ave, Ste 210
Westminster, CO 80234

Tel : +1 303 301 6200
Fax : +1 303 301 6201

EUROPE

1st Floor, Rama Apartment,
17 St Ann's Road, Harrow,
Middlesex, HA1, 1JU

Tel : +44 207 8265300
Fax : +44 207 8265352

REGIONAL – MUMBAI

Level 13, R-Tech Park,
Nirlon Knowledge Park,
Goregaon (East),
Mumbai - 400063
India.

Tel : +91-22-4476 4567

MIDDLE EAST & AFRICA

#Office number 722,
Building number 6WA,
Dubai Airport Free Zone
Authority(DAFZA,Dubai
United Arab Emirates

Tel : +9 714 214 6700
Fax : +9 714 214 6714

ASIA PACIFIC

175A Bencoolen Street
#08-03 Burlington Square
Singapore 189650

Tel : +65 6338 1218
Fax: +65 6338 1216