SECTRIO

www.sectrio.com

The Global Threat Landscape Report 2022

A Sectrio Threat Research Labs Initiative

DATA COLLECTION AND RESEARCH METHODOLOGY

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in over 70 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
- 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 Subex. The network includes over 6000 physical and virtual devices covering over 400 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.

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 advisories

Key findings are published by us every quarter to enable businesses, decision-makers, academicians, students, CISOs, and others 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.

2021: THE YEAR OF RANSOMWARE AND LARGESCALE CYBERATTACKS

On July 4th, hacker group Revil asked for one of the largest ransoms ever demanded. The group asked for $70 million to deliver the universal decryptor key to victims of a major breach. While this ransom was not paid, it does bring the scope and scale of hacker activity into perspective. Hackers are getting bold and brazen in their efforts to not just exploit gaps in the security architecture but also to create new gaps to put businesses under pressure.

Just a year ago we had warned about the next phase of the pandemic era cyberattacks. We had predicted that the next wave of attacks would target businesses by extensively going after unpublished vulnerabilities through multi-modal reconnaissance. As subsequent events have shown, these attacks started as early as February 2021 with a large automotive manufacturer.

The Colonial Pipeline attack which surfaced in May 2021 was also not an out-of-the-blue attack. Hackers were studying critical infrastructure targets across the US for almost half a decade now. With the rapid and unsecured expansion in threat surfaces, such events will now turn commonplace unless several measures are put in place to address this specific challenge.

EXPANSION IN TRADITIONAL AND NON-TRADITIONAL ATTACK SURFACES

Cyberattacks grew in sophistication and scale in 2021. The number of large breaches increased significantly from 1 a month to 4 this year. With more digital assets moving outside the traditional business infrastructure management zones, security teams were tasked with protecting traditional and new surface areas that have cropped up within their network. They also had to keep up with the new digital transformation, automation, and workforce management technologies some of which were untested at scale.

One of the earliest gaps that emerged from this growth was the misuse of user credentials. Access and identify management measures were quickly overrun by sophisticated hackers. This is a challenge even on air-gapped networks. Even businesses running multi-factor authentication were not sparred due to the lack of optimal configuration of their identity management systems and networks. Identify, privilege, and directory information is being sought out actively by commercial and state-backed hackers.

Managing machine identities at various levels has also provided enough security concerns. With the widespread use of APIs, services that were traditionally rigid and restrictive by default have now become open and flexible from an ease of use and access standpoint. Attackers can use unauthenticated and unmonitored services and leak data or manipulate outcomes to facilitate kinetic attacks. A supply chain angle to this problem has also become apparent.

EVOLUTION IN SOCIAL ENGINEERING ATTACKS

Social engineering seems to be emerging as a preferred means for attackers who are investing more time and attention in surrounding their target person or persons across cyberspace with phishing and whaling attacks. Social media tools morphed phone calls and emails are the preferred tools in this case. Sectrio also came across hackers who were selling sophisticated multi-channel phishing kits.

A typical level one phishing kit contains a custom assembled (or procured) code and resources packed in an archive file. Such kits are available for sale and exchange across the Dark Web and other forums. The codes and resources within these kits can be rapidly deployed on web services or VMs to facilitate phishing attacks at a very large scale.

In the case of a custom phishing kit, even social media and other credentials of target individuals are added to the base data. Such kits are made to order and often deployed to target large businesses, governments, or even persons of interest by APT actors. During our research, we came across kits that vary significantly based on the targets and geographies.

- **Level one commercial kit:** available widely, designed to collect data from the victim's files. These often contain just a few files written in basic machine language or even HTML.
- **Level two kit:** these contain codes and logic that are designed to trick the victim by offering or rather creating content based on their inputs or usage. These kits can morph into a fake website or document that will induce the victim to download and open for the attack to commence
- **Level 3 kit:** when deployed, these codes help highjack inbound messages and OTPs in the victim's device. Based on the sophistication, the victim’s device may be hijacked to either suppress the messages or delete them after forwarding
- **Level 4 (custom built):** these are kits that are made to order. They contain a range of personally identifiable information belonging to multiple targets in an organization, access credentials, financial information, and details required to trick the victim into revealing more details or to steal critical information

These kits contain specially made code and logic to present dynamic content to the victim, based on input. This can be in the form of presenting a fake consumer banking login page based on previous input or presenting logos of their company based on their email address.

The typical cost of a phishing kit:

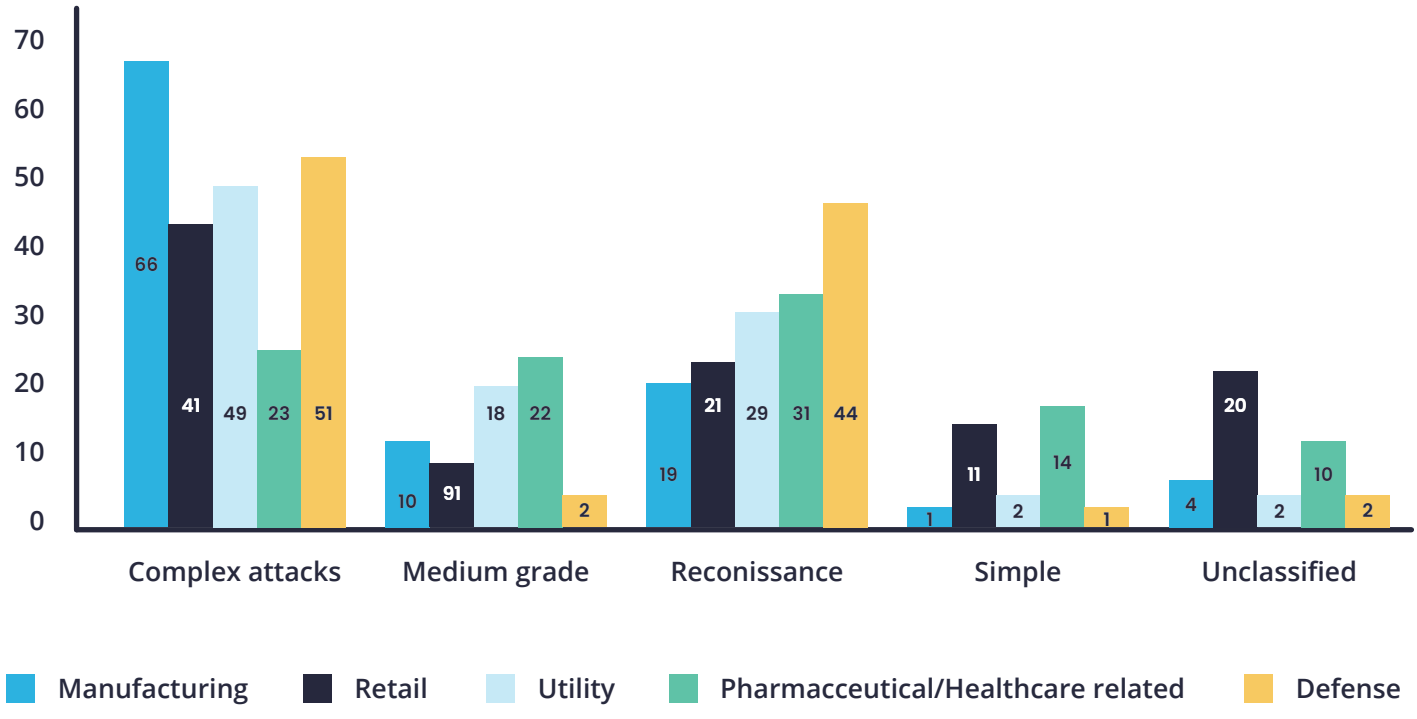
Phishing kits will vary dramatically in cost based on the complexity and capability of the kit. Simple kits containing only a few files of PHP code can cost anywhere between 10-100 USD to purchase. More complex kits which may require backend databases, integrate third-party APIs, have built-in “anti-bot” or evasion techniques, or even use licensing terms, may cost in excess of several hundred dollars.

TARGET: SUPPLY CHAINS

In their attempt to continue to create large-scale disruption, hackers went after supply chains like never before. Sectrio studied 137 supply chains attacks across the globe of which:

- 47 percent could be traced back to known APT groups
- 11 percent came from suspect APT groups or affiliated enablers
- Independent hackers and those working for unaffiliated groups were behind the rest of the attacks
- Vaccine supply lines covering active pharmaceutical ingredients (APIs) were targeted extensively.

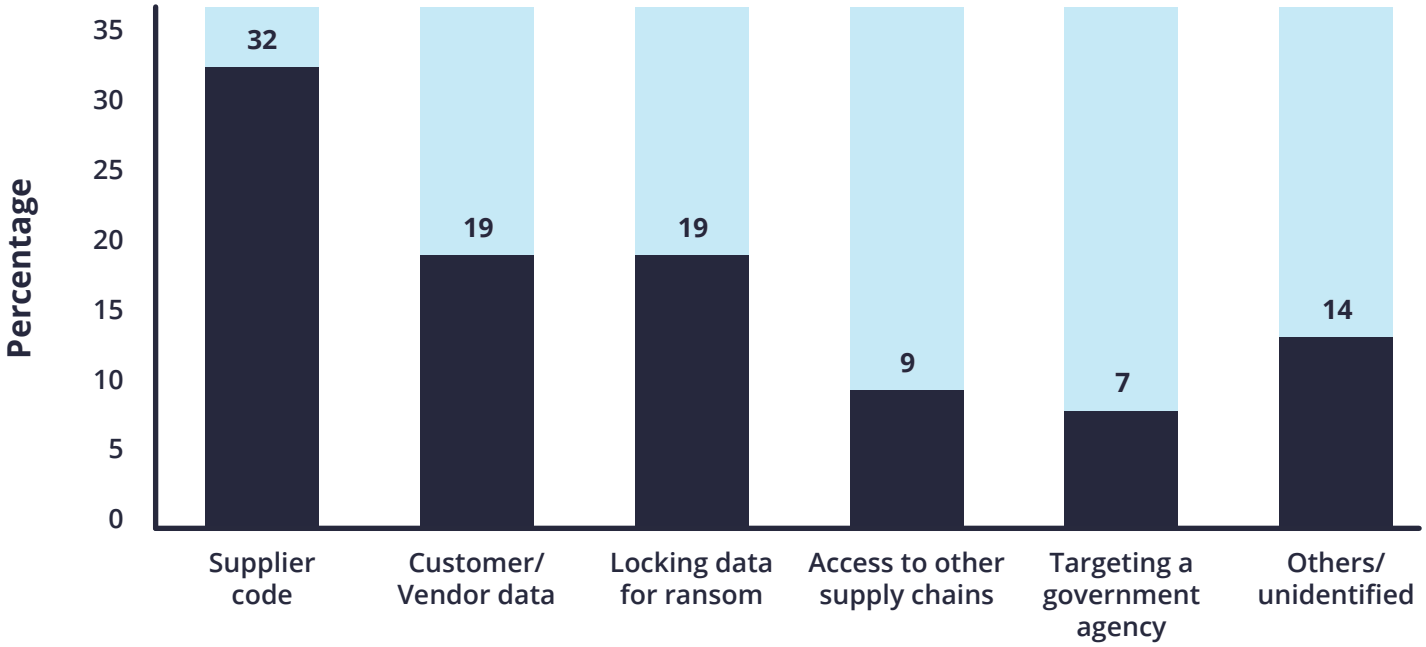
Manufacturing, retail, and utility supply chains were targeted the most. Within manufacturing, those related to large-scale manufacturing of white goods, automobiles, defense hardware, and farm equipment were the ones targeted the most by hackers. In the case of every supply chain attack, multiple vendor chains and even sub-vendors were targeted (in the case of businesses with long tails).



Reconnaissance attacks continue to rise across supply chains. Hackers are maintaining a high level of interest in attacking and studying supply chains. There could be adversarial groups that are focused on exclusively attacking supply chains as such high levels of interest can (ideally) only be sustained through focused efforts.

TABLE: MOTIVATIONS FOR SUPPLY CHAIN ATTACKS

Supply chain attack motives/targets and percentage of attacks recorded



Supply chains present a moving target to hackers which could also be a reason why they are being studied extensively by them. New vendors get added, new processes are adopted, and the length of chains also varies based on various parameters. In the 137 supply chain attacks that we studied, we could identify many motives. Supplier code and customer data were the top motivations that drove hackers to target supply chains. In the case of defense entities, hackers wanted to move laterally across the chain to access upstream and downstream organizations to finally target government agencies. In the retail vertical, hackers wanted to access the financial transaction data of customers and businesses while in the maritime space, hackers were tracking cargo of interest across the seas.

Supply chain poisoning is now a major concern

Supply chain poisoning refers to how a code level infection is added in software, components used in the development of software, or firmware supplied to businesses and government.

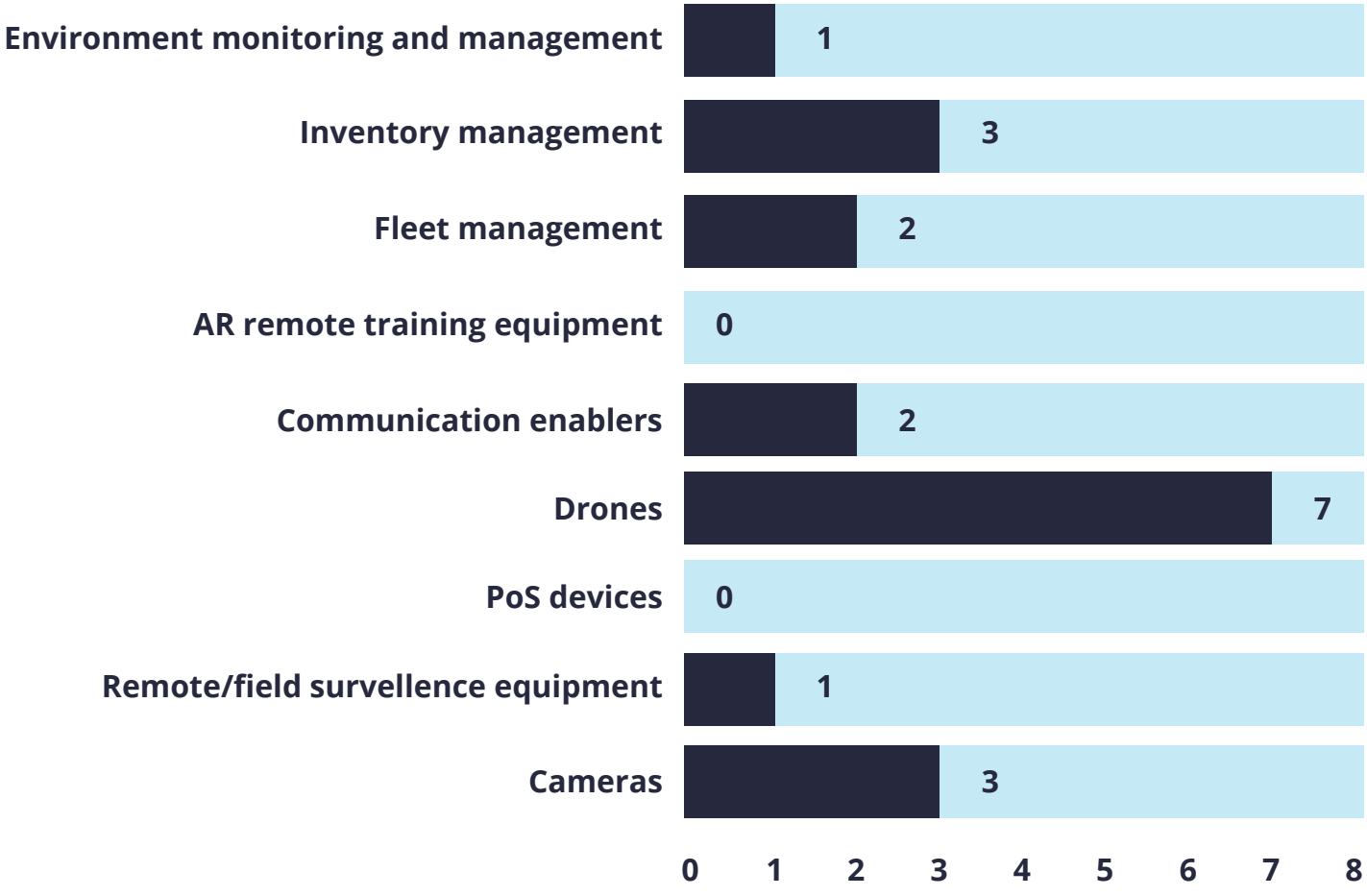
The defense sector was most impacted by supply chain poisoning in 2021. Random military hardware including drones, communication equipment, controllers, surveillance hardware switchgear, inspected and scanned by our research team revealed the presence of suspicious foreign contaminants and signs of digital infection.

Dimensions of Supply Chain poisoning

- Supply chain poisoning and contamination and trojanising input lines remains a source of concern
- Critical projects could be compromised at will by hacker groups
- Core system and infrastructure can be rendered inoperable or inaccessible during times of crisis to degrade the quality of response
- Laterally moving malware could target other businesses as well as other critical infrastructure components

Supply chain poisoning in the defense sector is being triggered from different source points spread across the chain. This includes all the points mentioned in para one of this section. There were also signs of post-procurement infection in some hardware.

Table: percentage of supply chain infections recorded across various categories of devices studied



Smart cities came second in the list of sectors impacted by supply chain poisoning with cameras and environment monitoring equipment showing signs of infection and digital tampering.

HACKERS ARE USING REPLY-CHAIN PHISHING TO TARGET BUSINESSES AND DIGITAL INFRASTRUCTURE

What is reply-chain phishing?

Reply-chain phishing is used by hackers to insert themselves in legitimate conversations through compromised accounts. Unlike spear-phishing where hackers use fake email addresses that sound similar to legitimate ones in reply-chain phishing, emails are sent from hacked email accounts belonging to legitimate users. The credentials are obtained through various means. Once the hackers access the email account, they study email threads and identify those with the maximum likelihood of netting victims.

The hacker then sends an email as a reply to one of the mails in a thread with a malicious URL disguised as a legitimate one. Recipients may inadvertently click on the link and install or download malware that can then spread across the network. IoT and OT-specific malware is also being spread this way.

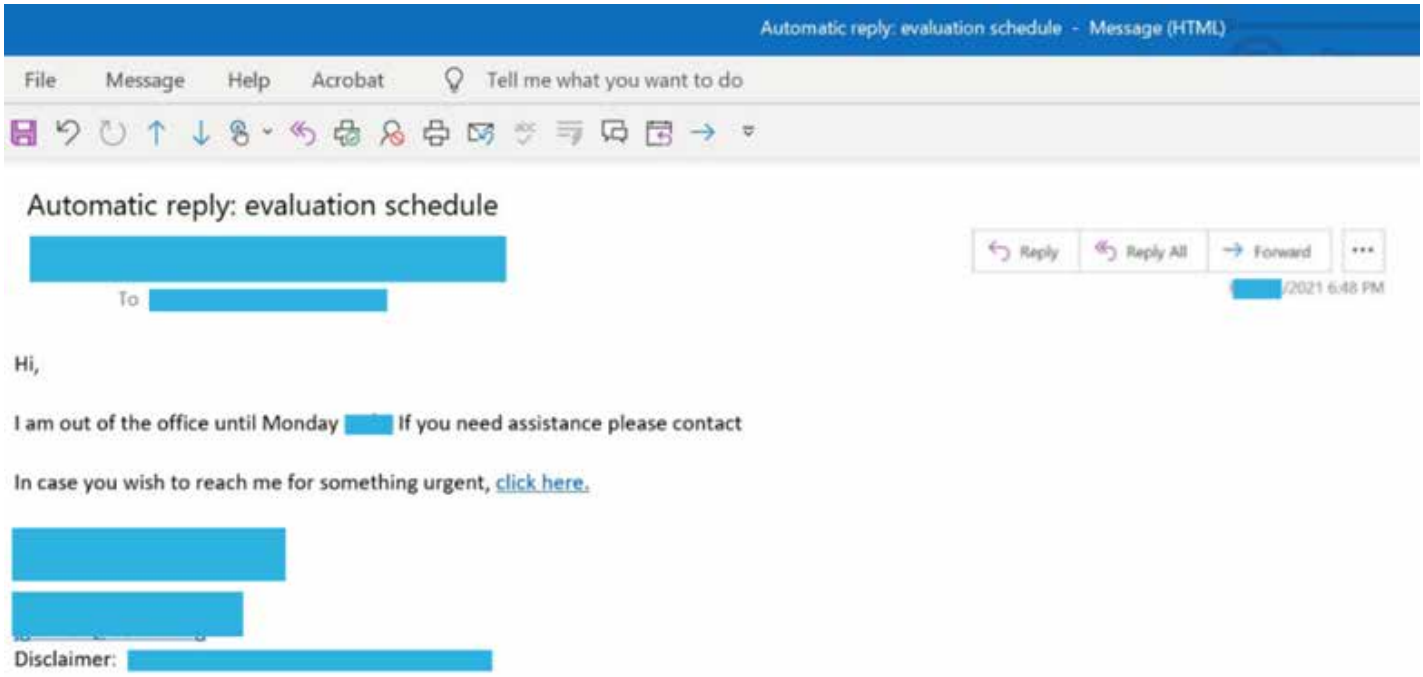
We came across multiple instances of reply-chain phishing in North America during the Thanksgiving holiday season. Because of the inherent possibility of a breach of credibility and trust, we feel that this will become a significant cybersecurity problem in the days to come.

Crowdsourcing a cyberattack

Hackers tried out several new tactics in 2021. One of which involved recruiting a web of hackers to conduct pointless reconissance scans of the target network. During these scans, neither is any data collected nor is any payload deployed. But such attacks are designed to keep cybersecurity teams busy chasing non-existent cyberattacks by generating a flurry of alerts. This keeps the SOC team busy and generates SOC fatigue to tire down security teams while hackers plan their next move which could be an attack that could slip through as the teams battle noise and fatigue.

Such attacks can be prevented by preventing hackers from building a connection to your network and devices before they can initiate the scan.

Sample reply phishing attack intercepted by Sectrio



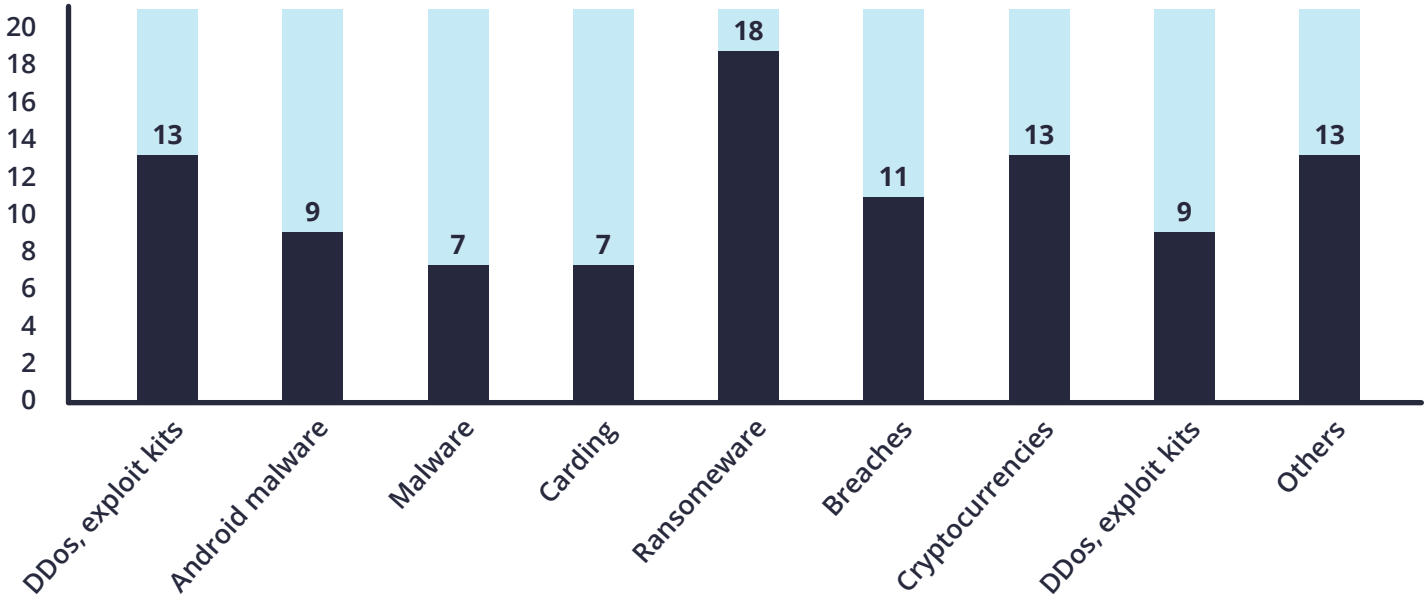
IMPACT OF DARK WEB ON CYBERSECURITY

Dark Web is casting a wider shadow on the threat landscape surrounding businesses across the globe. The gap between surface web and Dark Web in terms of leaked data, malware cracked software, ransom content, etc. widened in 2021. This means that much of the information found on the Dark Web is not there on the surface web or on forums that are akin to a grey area in between the two.

Pre-cyberattack signs are now appearing more frequently on the Dark Web through the language used is now more cryptic than ever. Hackers are exchanging coded information on new targets as well as data dumps belonging to existing victims. The use of Dark Web resources to communicate ransom notes is also growing. All this means that Dark Web continues to hold a big say in how cyberattacks are conceptualized and executed.

While the use of private messaging platforms is growing, hackers are still relying on the Dark Web in parts to identify victims and conduct a cyberattack. Many packs are being sold on the Dark Web for rookie hackers and those with basic knowledge of hacking. Such 'kits' have been turning up in many breaches we have seen in the last 3 years and are widely available across the Dark Web under different names. Some of these packs were disguised exploit kits as well designed to trick the would-be hacker.

Percentage occurance of keywords in Dark Web dicussions



Type of pack	Cost in USD
Ransomware with source code	50
Basic ransomware	15 to 76
Hacker start-up kit	14
Dangerous malware pack 2021 edition	21
RAT tools	5 to 45
VPN breach pack	15 to 100
Ultra-dangerous malware suite	12
Avengers whaling phishing kit	7
Ultimate password cracking pack with instructions, demo, and help	10
Must have DDoS kit	10

The impact of the Dark Web on cybersecurity can be broken into three aspects:

- **Data sink:** Dark Web continues to be a dumping ground for plenty of stolen data. Such data is then accessed by other hackers to conduct secondary attacks.
- **Source for further attacks:** in addition to the above, the Dark Web has also become a source for understanding if your business could be on the radar of hackers or not. If discussions are happening on a company on the Dark Web, then chances are that a cyberattack is imminent or at least in the works.

- **Source for collaboration and monetization:** hackers are still relying on Dark Web to some extent to monetize their work. This is not just limited to selling stolen data and malware but also in offering tips of the trade to rookie hackers and anyone interested.

Thus, it is essential to keep an eye on the Dark Web to understand how the threat environment is evolving. Its impact on the cybersecurity posture of businesses and government is not going to go away any time soon.

BLEEDING DATA: MORE DEAD DROPS, MORE DATA LOSS

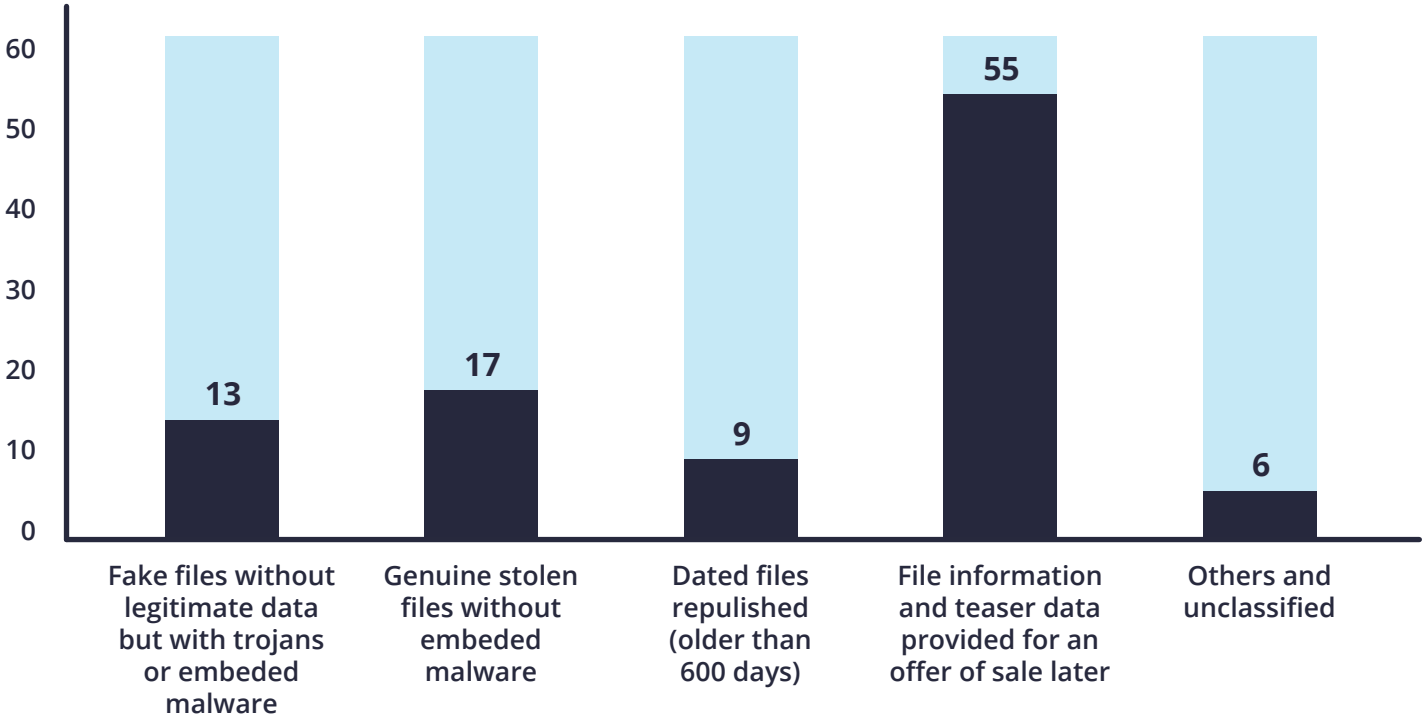
Wikipedia defines a dead drop or dead letter box as a method of espionage tradecraft used to pass items or information between two individuals using a secret location. In cyberspace, however, a variant of this tradecraft has emerged in the last few years. This involves rogue insiders in organizations dumping valuable data including credentials, network information, or even ways to bypass security measures in online forums or the Dark Web. They expect hackers to find and use this data to target their current or former organizations as a means of exacting revenge or settling scores as the case may be.

We are encountering many such data dumps across forums now. In the last few months, the number of such drops encountered by our research team has risen steadily enough to warrant concern and action. Insiders are compromising even highly confidential information belonging to employees such as pitch decks, pricing documents, and meeting minutes. From the shop floor, production schedules, device information (including patch status in some instances), machinery information, default system control passwords for remote devices, and more are compromised.

For purpose of this study, we took into account new data that was not connected to any hackers or hacker groups or was put out for sale or barter. This was data that was collected and dumped by individuals or groups without any intention of monetizing the data. Monetizing could mean that there is a monetary motivation involved. In the case of dead drops in cyberspace, however, the most common motivation is revenge. But some other groups and individuals are selling such data as well. Sometimes such data is also booby-trapped with malware to lure new victims who could be other hackers or businesses who procure such data.

More than the loss of data, it is the exploitation of such data that should worry businesses. It also represents the failure of data protection measures at many levels. Such drops are also making it easier for hackers to breach networks and systems encrypt data and demand ransom for its release.

Percentage detection of various types of data in dead drops

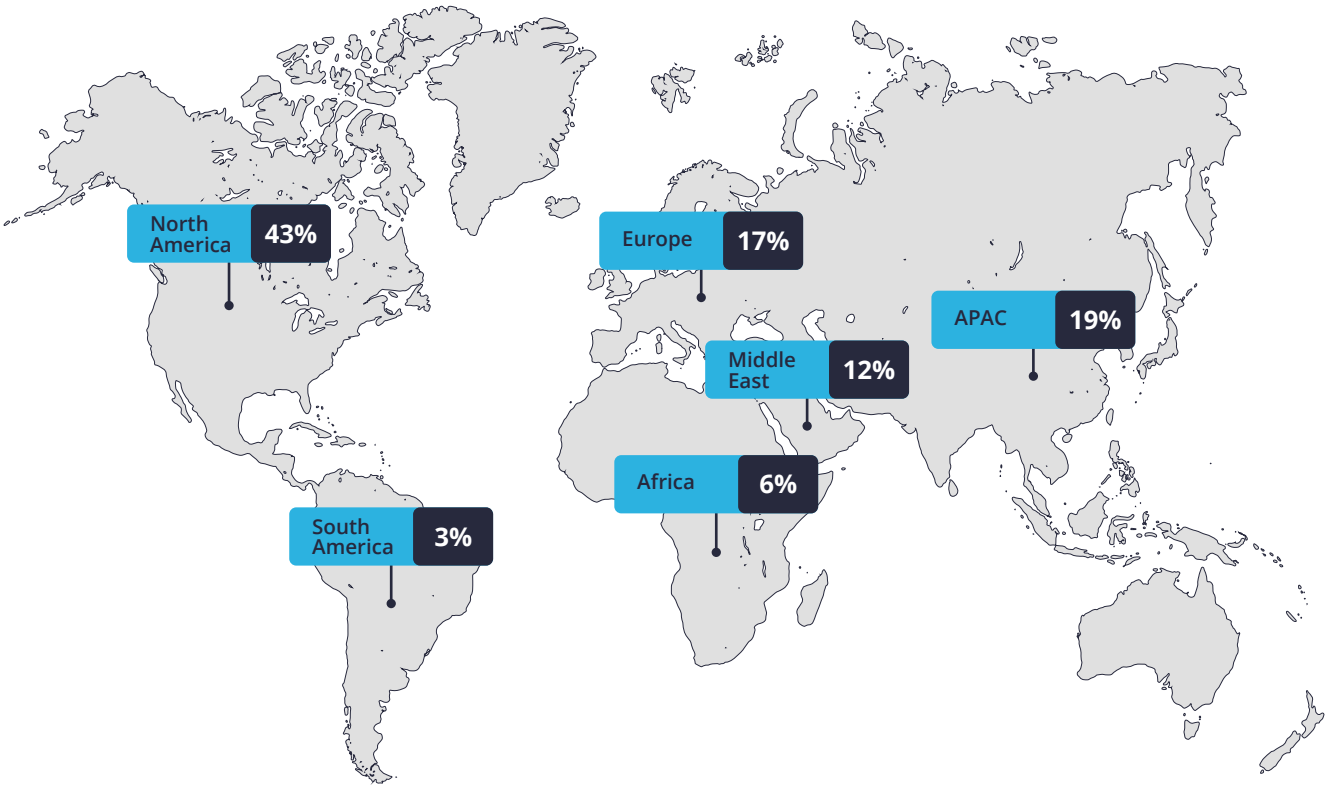


Cybersecurity highlights of 2021

- Supply chain attacks targeting large-scale disruption occurred throughout the year. We observed a near 100 percent rise in multi-modal attacks on critical supply chains.
- The number of high-value breaches reported rises by 81 percent
- New APT groups reported from South East Asia and South America
- The Center of gravity as far as global cyberattacks are concerned is still around North America because of the huge volume of cyberattacks targeting the US and Canada
- Attacks on critical infrastructure spread across manufacturing, defense, oil and gas, electric power grids, health care, utilities, communications, transportation, education, banking, and finance log a significant rise in cyberattacks (330 percent)
- Growth in dead drops: data dumps encountered a rise of 59 percent over 2020
- Reply phishing emerges as the third most used mode of phishing
- Control system targeting has improved in sophistication. Hackers have now developed a better understanding of these systems to exploit weaknesses
- Many instances of the use of AI in hacking were reported in 2021. New models of attack automation, post-attack data transfer, data sink creation and data poisoning were recorded
- Published instances of ransom payment rose 190 percent over 2020
- Secondary attacks using data stolen from previous attacks rise by a staggering 600 percent

- Instances of crypto-malware infecting new projects rise
- The gap between surface web and Dark Web in terms of leaked data, malware cracked software, ransom content, etc. widened in 2021.

Geographical distribution of cyberattacks on IoT and OT in 2021



Which countries are getting attacked and why?

With many geopolitical hotspots in the Middle East, South East Asia and Eastern Europe warming up in 2021, cyberattacks from these regions rose in 2021. Many of these attacks also spilled over into other regions engulfing countries and businesses unconnected with the original set of actors. APT groups were also being deployed by a few nation-states to generate revenue through ransom. We have seen this trend picking momentum in the post-pandemic period.

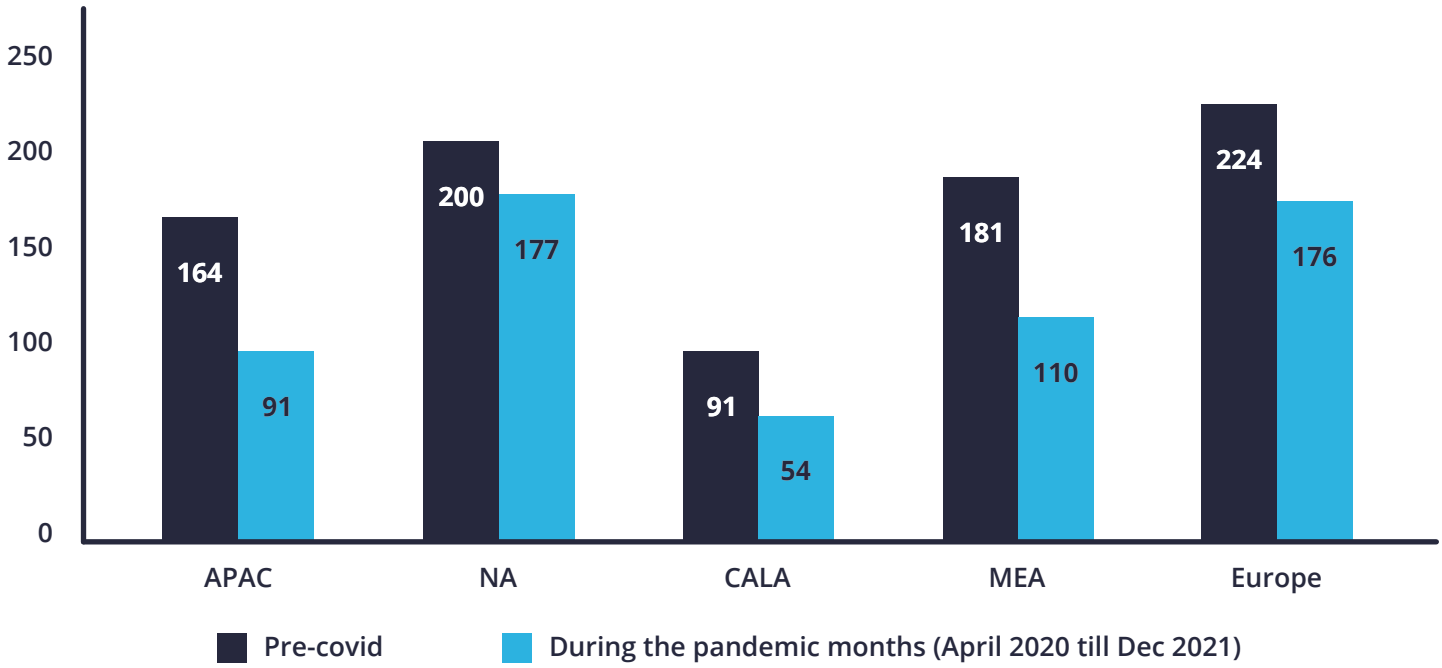
The number of reported instances of cyberattacks is far lower in almost every country studied by us. The difference between these two data points viz., the number of actual attacks Vs those that are reported is the highest in countries such as India, Mexico, South Korea, Finland, Oman, and Spain. It is the lowest in Japan, and a few other countries. We came across data belonging to companies that had never reported a cyberattack this year online. Those companies were promptly informed but we are yet to hear from them.

In some countries, reconnaissance attacks have been going on undetected for a while. Hacker groups have collected GBs of data on targets. This data is being used to target them at a time chosen by the hackers. This is also the reason why start-ups often get hacked after several rounds of funding are over or they bring out an IPO. The hackers would have been stalking the networks of such start-ups since their early days while diligently keeping a tab on them digitally waiting for an opportune moment to strike.

In the case of manufacturing plants and oil and gas entities, hackers typically gain access through new projects that use untested and unsecured applications and devices. We have seen many instances of hackers attacking parts of manufacturing plants or even entire locations using this method.

Distracted employees clicking suspicious links is another way in which hackers are targeting businesses.

Average number of reconissance days



While healthcare and manufacturing attracted the maximum number of attacks in 2020, attacks on oil and gas installations rose steadily in the first half of 2021 (the assessment period). With the demand for petroleum products rising, refineries and oil wells started increasing production in a phased manner in 2021.

Table 1: What is being attacked and why?

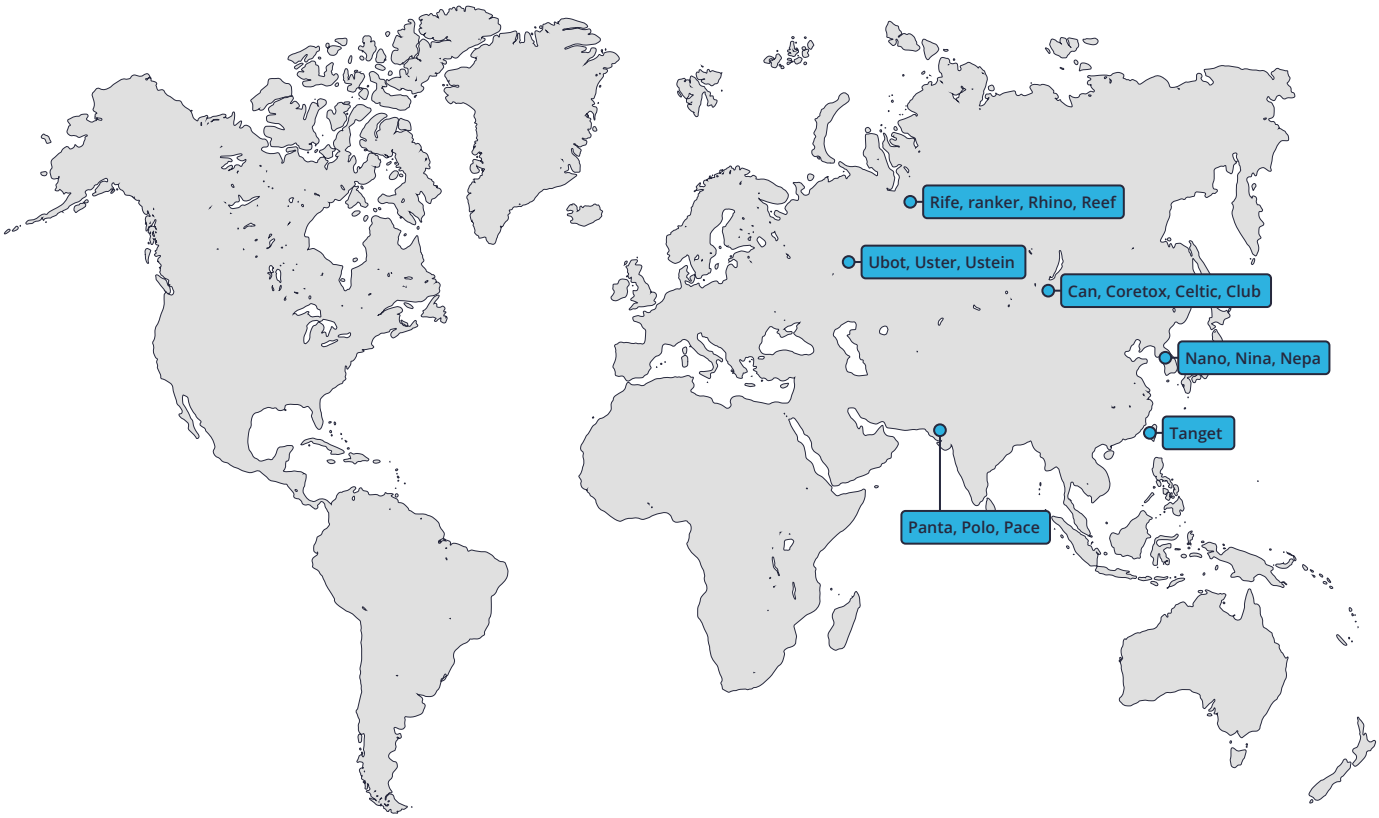
Sector	Target	Why?
Manufacturing	Safety systems, IIoT deployments, shop floor controllers, HMIs, monitoring systems,	Data theft, ransom, large scale disruption, geopolitical factors
Healthcare	Internet of Medical Things devices, high-value health care machines that run on legacy systems	Patient data 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

Demand for petroleum products in economies that have now opened up for business at the very least partially (such as the United States) is touching record levels, according to Forbes. Such a rise in demand and the increase in production levels led to the sector climbing it's way back to the top 3 most attacked sectors globally. We are expecting this rise to continue as the sector is still grappling with an unsecured digital footprint and a converged tech environment.

Utilities and smart cities that were in the top 5 last year, continue to attract a huge volume of cyberattacks.

Key APT clusters under observation



THE RISING COST OF RANSOM

The cost of ransom continued its upward trajectory for the third consecutive year. In the first half of 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*
2016	4975	4900	23 incidents
2017	7600	7000	26 incidents

2018	10,000	9000	35 incidents
2019	14,567	12000	41 incidents
2020	27,340	22,045	49 incidents
2021	50,000	39,000	51 incidents

*** 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

REvil and DarkSide commanded the maximum ransom per attack while Babuk and Avaddon, DoppelPaymer, HelloKitty, and Evil Corp were the other groups that placed a ransom demand of anywhere between 40-60,000 USD per GB in 2021. In many instances, a ransom demand of over 20,000 USD per GB involves the use of complex malware and crypto loaders.

Breakaway APT groups such as those belonging to two clusters whose respective operational epicenters have been mapped to Irkutsk in Russia and Sinŭiju in North Korea have been found to use sophisticated military/defense-grade malware that could be stolen or donated by advanced state-backed cyber offense labs. In such instances, the ransom demand is often very high and it can be said with a high degree of certainty that such malware bring revenue for these actors and labs and maybe even other state intermediaries.

THE RISING COST OF RANSOM

Increasing attacks on key sectors

Sector	Trend
Healthcare	97 ↑
Manufacturing	76 ↑
Critical infrastructure	71 ↑
Banking and finance	61 ↑
Smart cities	44 ↑
Defense	39 ↑

Retail	37 ↑
Smart home devices	35 ↑
Others including agriculture, public safety, unspecified projects, and telematics projects not falling under the above categories	45 ↑

TOP COUNTRIES OF ORIGIN OF CYBERATTACKS

Country	Percentage
China	21
North Korea	7
Iran	4
Russia	5
Ukraine	3
Unknown	27

CITIES DRAWING THE MAXIMUM CYBERATTACKS

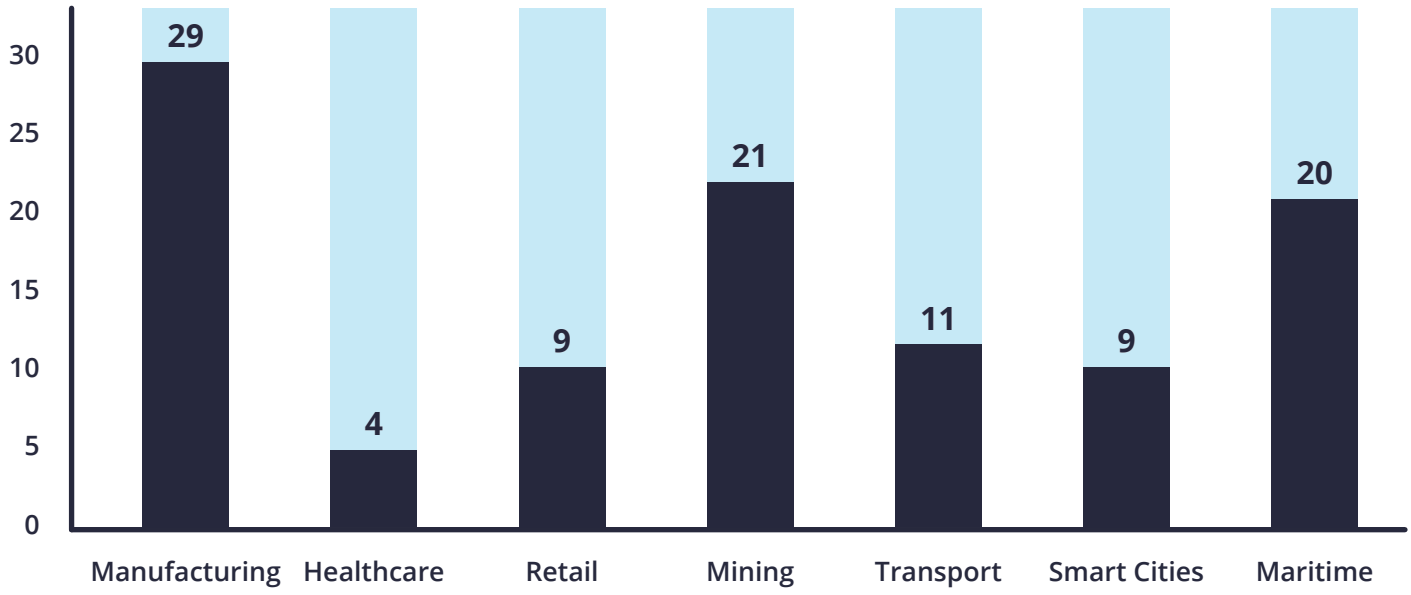
Due to the Covid-19 themed attacks that were relatively more successful as compared to the others, the composition of the list of the top cities that were attacked the most underwent a massive change in 2020. Here are the top 10 cities that were attacked most often in 2021:

City	Rank in H12021	Rank in 2020
Washington D.C	1	1
London	2	2
New York	3	3
Hanoi	4	11
New Delhi	5	5
Kiev	6	7

Dubai	7	10
Sydney	8	8
Madrid	9	9
Singapore	10	4

All the cities listed above and those that were part of the top 10 in 2019 but are now out of this list such as Seoul for instance have registered a significant increase in 2020 as well. But the cities that are part of the 2020 list were attacked at a much higher rate in 2020 propelling them to the top 10.

Days taken to monetize a cyber attack in 2021



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 2 percent average dip in the time taken to pay ransoms across the board. This means that hackers are now monetizing their cyberattacks faster.

Days taken to discover a cyberattack rises

In 2019, there was a slight dip in the number of days taken to detect and address a cyber attack. In 2020 however, this number rose to 165. In 2021, this number has gone up to an all-time high of 190. Since most employees were working from home throughout the first half of the year on unmonitored networks, security analysts found it difficult to access employee equipment for forensic analysis to identify signs of a breach.

> **"A year down the line, security teams are still finding it difficult to manage remote assets"**

With employee devices operating from unmonitored environments, the chances of such devices getting infected with dangerous malware grow significantly. Such devices may also contribute to

Cybercriminals are targeting sectors such as financial services, healthcare, oil and gas and manufacturing using diversified and sophisticated botnets. They are also deploying bad bot methods to increase the speed of attacks on these sectors. This is why we are seeing a huge increase in the volume of traffic originating from these botnets. Common methods for botnet use include: remote account take over, privilege mining, distributed denial of service, and attacks on exposed intranet-based applications and other internal platforms.

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

Malware (including variants) sample size for the test: 18000
Target sectors: manufacturing, telcos, smart cities, defense, shipping and utilities

The average price of sophisticated malware held steady in 2021. This could be because of muted demand or hackers reusing malware to create variants with the help of part-time malware developers.

The cost of reconnaissance malware came up down a bit as most hackers were going after monetization rather than data collection or snooping

Launchpads

The number of Malware launchpads I.e., botnet constellations that provide surfaces for the release of malware into cyberspace registered a rise this year. Increasingly, such surfaces and farms are moving closer to urban areas and major cities. Servers and connected devices in some businesses and academic institutions may have been highjacked by hackers are being used to launch malware and cyberattacks on specific targets and the larger cyberspace in general.

The increase in launchpads points to the diversification of cyber-attacks as also the large-scale 'addition' of infrastructure to facilitate an increase in cyberattacks. We can come to this conclusion by studying the traffic patterns including command and control interactions and persistent and dynamic connections related to these botnets some of whom are using sophisticated obfuscations techniques that are tough to decipher.

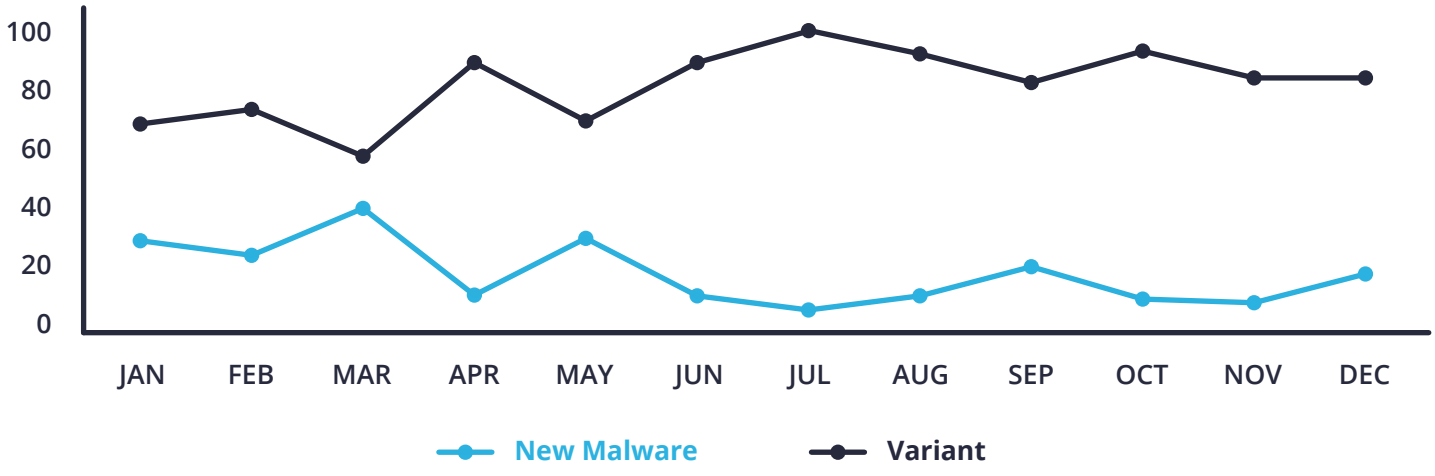
Highjacked botnets show similar patterns in traffic generated except when it comes to communications between these botnets and their botmasters. However, there are some similarities in command and control communications across botnet families in some cases even those managed by different botmasters.

Diversity

In terms of malware diversity, in H12021, we saw several new malware variants released by malicious actors. Top targets include utilities, manufacturers, maritime, and healthcare institutions.

Poorly secured remote protocol access and shared remote protocol access credentials helped hackers compromise more network assets while the use of endpoints with little or no security in the early stages of projects involving the Internet of Things allowed hackers to gain control over infrastructure and deploy remote access trojan to sustain access and control over networks well beyond the project tenure. This is a trend we have been observing since 2018.

New malware Vs variants (percentage detection)



The dip in new malware detection in the second quarter of 2020 is consistent with similar patterns we have seen in the last two years. June and July are months the months where most malware variants are released while the same period also shows the least numbers of new malware.

Key traits in malware detected around the world (sample size 12700 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 2021, 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.
- One that the 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 that there.
- Hackers want to cover their tracks all the way
- There are undiscovered malware forums trading in complex malware

State-backed APT actors became quite active globally around March 2021 and continued their activities till late November. 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 create disruption.

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, stolen data are also enabling the exchange of malware between friendly APT groups to maintain a level of plausible deniability and distance.

MALWARE SOURCES

Possible Source	Percentage detected
Dark web	25
Procured via malware forums	18
Mixed	9
Military-grade	3
Academic\research labs	3
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 a labs in academic institutions or facilities belonging to government agencies.

PORTS ATTACKED

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	8

DoS and variants	11
Simple reconnaissance	5
Persistent reconnaissance	18
Port/asset scan/TCP dump (specific recon)	10
Firmware downgrade attempts (corrosion)	7
Crypto mining/jacking	9

Red alert

Based on the testing done by our threat research and penetration testing teams in 2021, we came across many critical components that could easily be penetrated to facilitate a cyber attack.

- An installer file for asset location management can be used to penetrate offshore and nearshore assets belonging to oil exploration and maritime companies
- Phishing emails disguised as an emergency alert from a regional regulator
- Anti-virus applications and rigid firewalls are not enough to protect equipment related to safety and chemical and ore processing in mining and mineral handling plants.
- Utility plants and transmission equipment have several weak points that could be exploited including HMI systems, equipment management sensors

During one of our assessment tests, the test rigs' operation technology (OT) networks were penetrated using a software installation file for dynamic positioning and workstation charts. This indicates the ease with which devices and systems could be breached. The prevalence of large-scale unreported or unacknowledged vulnerabilities has added to the problem. Such vulnerabilities slow down response mechanisms and have a trickle-down effect on limiting the impact of a breach and putting systems back online.

REGIONAL TRENDS

North America

Ransom payments rise in proportion to the growth in OT and IoT-focused cyberattacks

The US continued to be the most attacked country in cyberspace in 2021. While such a huge number of cyberattacks may have a lot to do with the diversity of businesses that operate here as well as the country being a favorite target of APT groups, the impact of most cyberattacks could have been minimized by adopting a basic level of hygiene.

In many ways the Colonial Pipeline incident that was among the most disruptive cyberattack on US soil also showcased 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
- 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 aggravated the problem
- 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

MINES IN NORTH AMERICA COULD BE TARGETED IN 2022

Based on the data collected from our honeypot, hackers are conducting recce drives across many sectors in North America. These include oil and gas, manufacturing, retail, defense, energy and utilities, they are also on the lookout for new targets. The widespread use of OT, partial adoption of automation, and use of new and unhardened IoT and IT devices could impact sectors such as mining and shipping. As per our analysis, mining companies may already be targeted to some extent while the attacks on shipping and freight management companies are now growing.

Hackers could also target new businesses in segments such as connected vehicles, renewable energy, and retail supply chains. These are priority segments for hackers who use such attacks to mature their breach tactics and to gain media attention.

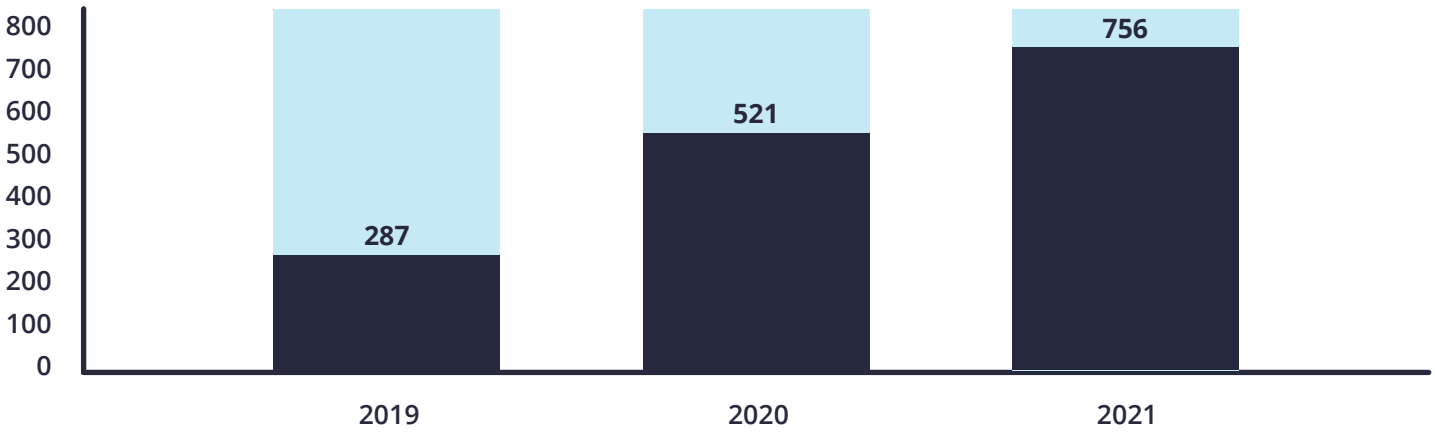
What are hackers after in North America?

- Consumer services
- Large business interests and dominant players
- Supply chains
- New businesses
- Government contractors and vendors
- Power grids and related infrastructure

Supply chains are presenting hackers with a moving and lucrative target. In addition to large-scale disruption, such attacks also offer more return on investment. In addition, there are other factors that make supply chains a favorite for hackers:

- The opportunity to strike businesses from multiple entry points
- Once infected, malware can move across the connected infrastructure crossing not just organizational but even political boundaries
- The entry of start-ups with high valuation and risk appetite but with low appetite or patience rather bring systems online in a foolproof way after a cyber incident. This means that these companies may be more susceptible to paying a ransom to get things back on track faster
- Workflows, responsibilities, and systems are not aligned towards cybersecurity imperatives today
- Hackers may also be aware of zero-day vulnerabilities across vendors that are yet to be discovered

Repoted cyber incidents in North America



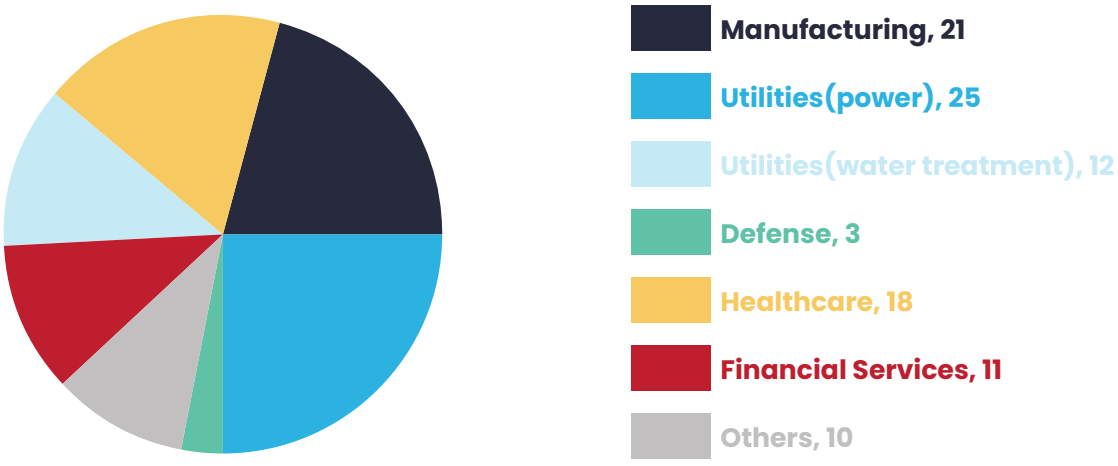
Limited visibility is a problem

While IT systems have been targeted by hackers for a while, utility firms and manufacturers, and other operators of facilities that use OT have reasons to worry. Sectrio's research team has found that many companies using OT had limited visibility into their OT devices linked to their industrial networks. This prevented them from framing a clearer picture of their physical and digital assets. Further, many companies are also not paying any attention to detecting and addressing vulnerabilities.

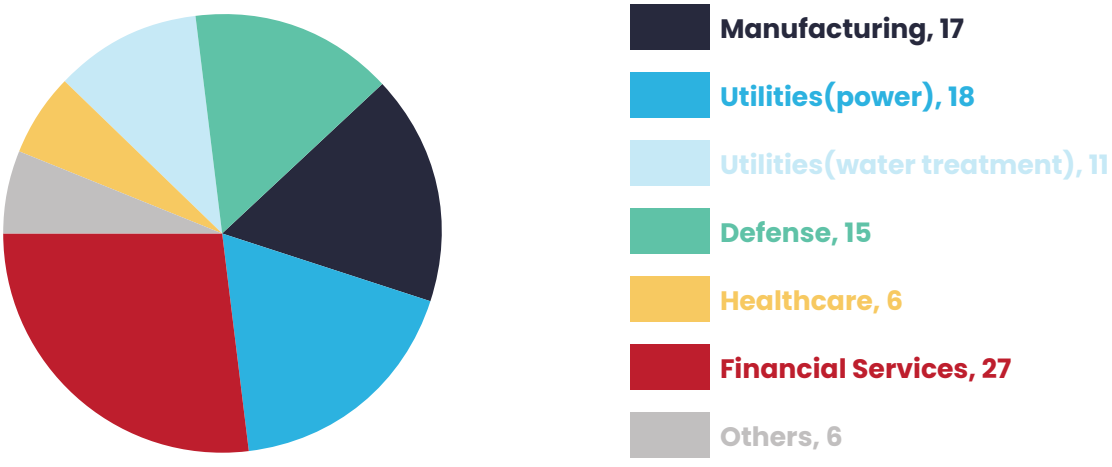
Such challenges are leading to delayed response times and a lack of a precise and timed response to a cyberattack. Shutting down the whole system in response to a cyberattack demonstrates a lack of visibility into assets and a lack of precise response mechanisms that when triggered can contain and limit the impact of a cyberattack. Hackers are making note of such shortcomings and working towards exploiting them. If the system affords enough visibility, shutting down a whole pipeline wouldn't have been an option worth considering, let alone executing.

CHART: MOST ATTACKED SECTORS IN NORTH AMERICA

Percentage attacks logged



Percentage of sophisticated attacks logged



New environments, old challenges

While investments in IT security have grown, OT cybersecurity investments and attention are still lagging. Businesses hosting complex hybrid environments with IT, OT, and the Internet of Things are now understanding the importance of ramping up their cybersecurity measures to align them with the complexity involved in securing such environments. Such businesses are closer to a massive cyber disruption than they can imagine.

- Some businesses have upgraded their OT environments by adding new devices. Such devices are however invisible to standard off-the-shelf vulnerability scanners.
- OT vulnerability scans are not done frequently and many businesses fail to fall back on a more disciplined approach that requires regular scans and remediation
- The ever-evolving threat landscape throws up new threats including malware that evade detection
- Visibility into threat surfaces is not adequate. Some of the solutions used by businesses are prone to misconfiguration and new vulnerabilities.
- OT security teams are often less empowered than their IT counterparts and if the same security team is handling both IT and OT cybersecurity, OT doesn't get as much attention as it should

Such gaps in addressing OT cybersecurity leave the room wide open for hackers or other adversarial entities to exploit.

Malware classes detected in the region

Class	Percentage detection (2020)	Percentage detection (H12021)
Crypto mining	17	20
Ransomware	21	33
Predatory	2	1
Defence-grade	2	1
Mission-based (uniquely engineered)	5	2
Modular malware	5	3
Reconnaissance	40	34
Others	8	6

Differences in cyberattacks logged in East coast and the West coast

Parameter	East coast	West coast
Type of attacks	Reconnaissance	Targeted attacks
Sectors	Chiefly critical infrastructure, oil, and gas	Telcos, shipping
Malware attributes	Highly persistent	Less persistence but stealthier and with staggered deployment patterns
Attack window	Early mornings	Early mornings and late evenings
Key cites targeted	Atlanta, Boston, Detroit, Washington DC, and New York	San Francisco, Seattle, Los Angeles, San Diego, San Jose

The US retained the tag of being the most targeted nation in the world in 2021. US registered a 71 percent increase in attacks over 2020. US cities also bagged the top 4 slots in the list of most targeted cities in North America. The top 5 cities include Washington DC, New York, Seattle, San Francisco, and Toronto. Malware-laden traffic was coming into North American cities from across the globe. A majority of this traffic could be traced to APT hotspots.

Possible botnet traffic emerging from within the US was also logged by our honeypots. This could be the outcome of devices operating in unmonitored environments being hacked into and used to route malware-laden traffic into other networks in the chain.

Emerging cybersecurity challenges in the region

- Underreporting of attacks. The amount of data released in public by hackers includes data that belongs to companies that have not declared publicly that they have been breached
- Devices on OT networks are not being scanned frequently to identify vulnerabilities
- Lack of visibility into networks and devices
- The ongoing pandemic has slowed down or impaired the cyber resilience measures planned or deployed by organizations. This has eroded their overall cybersecurity profile and reduced the efficacy of cyber resilience measures.
- High level of APT interest
- Basic cyber hygiene practices are not getting adequate attention

Regional snapshot

- Reported cyber incidents 756 (Sectrio, published figures, regional regulators)
- The highest reported ransom paid $11 Mn (Various sources)
- Highest remoted ransom demand $50/70 Mn (Various sources)
- Ransom recovered: $6 Mn (Forbes, Nov 2021)
- The rise in average ransom demand: 71 percent (Sectrio)
- Hack campaign cycles intercepted: 71 (Sectrio)

Europe

Western Europe continues to attract a disproportionate volume of cyberattacks

The number of rose across Europe rose by 107 percent in 2021. The volume of attacks rose steeply in H1 but fell slightly in the second half of the year The region clearly has many reasons to be worried about this trend. In addition to reconnaissance attacks, hackers moved away from the healthcare sector in 2021 to target traditional segments such as manufacturing, oil, and gas, renewables, retail, and defense. This could imply:

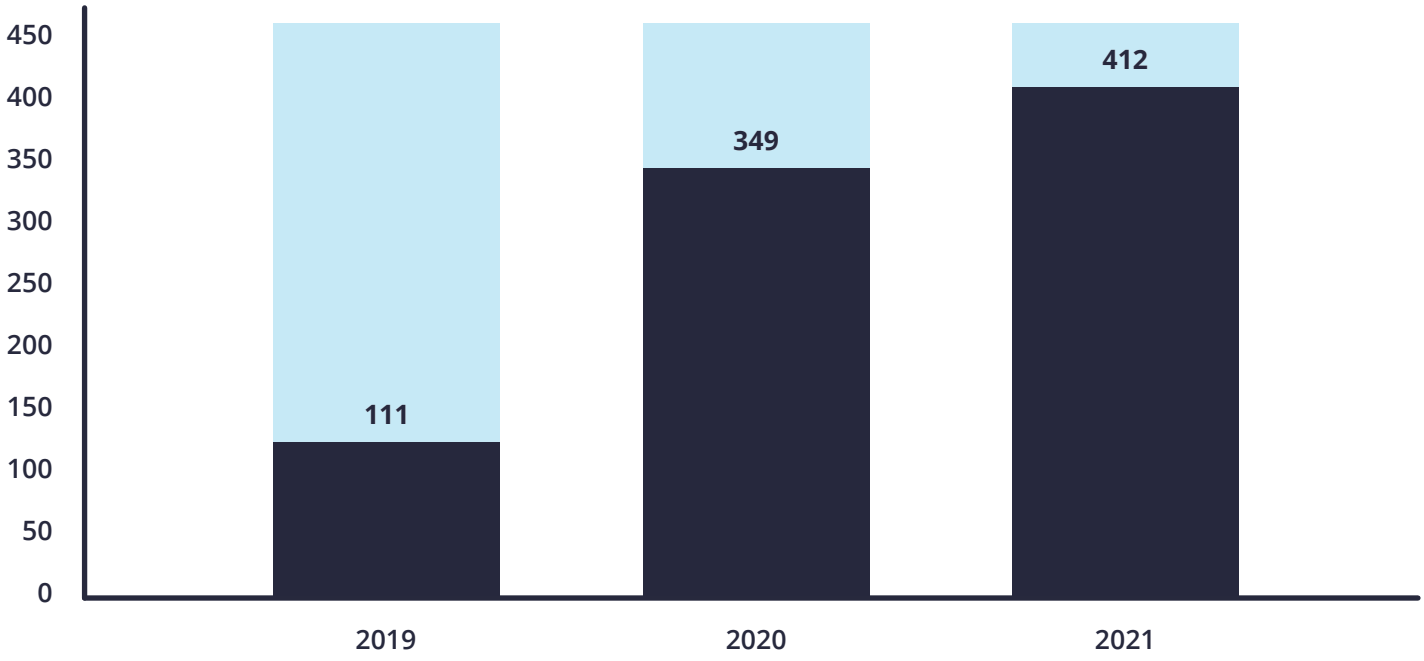
- Hackers were able to monetize attacks on traditional sectors faster
- Traditional sectors were easier targets for hackers
- Unlike North America where we saw extensive reconnaissance attacks being launched before the actual attacks, in Europe, most of the attacks were conducted with very little scanning. This means more attacks in a relatively lesser time period
- More social engineering campaigns were launched in Europe in 2021 than in any other continent. The number of such campaigns intercepted by Sectrio rose nearly 200 percent in 2021

Key trends observed in Europe

- Malware traffic recorded in the region has risen significantly in the last 6 months of 2021
- Britan's exit from European Union has not impacted the volume of cyberattacks recorded there. UK continues to be the most attacked country in Europe.
- The region was impacted extensively by regional geopolitical instability
- Extensive Russian, Chinese and North Korean APT group activity recorded throughout the year
- Attacks on government assets and infrastructure rise significantly
- Overall, cyberattacks across sectors across the continent rose 97 percent in 2021
- Long-tail supply chains that had links outside the continent were relatively less targeted while those within Europe were targeted more

- Healthcare, financial services, manufacturing, utilities, and retail were among the most targeted sectors
- 77 percent increase in pureplay ransomware attacks
- Dridex, Widebot, Qbot and IcedID are among the most frequently encountered malware
- 2022 will be a critical year for supply chain security
- Increased use of network penetration and scanning tools and use of multi-launcher malware led to more breaches and loss of data and eventual ransom payment
- Ransom demands continued months after the attack

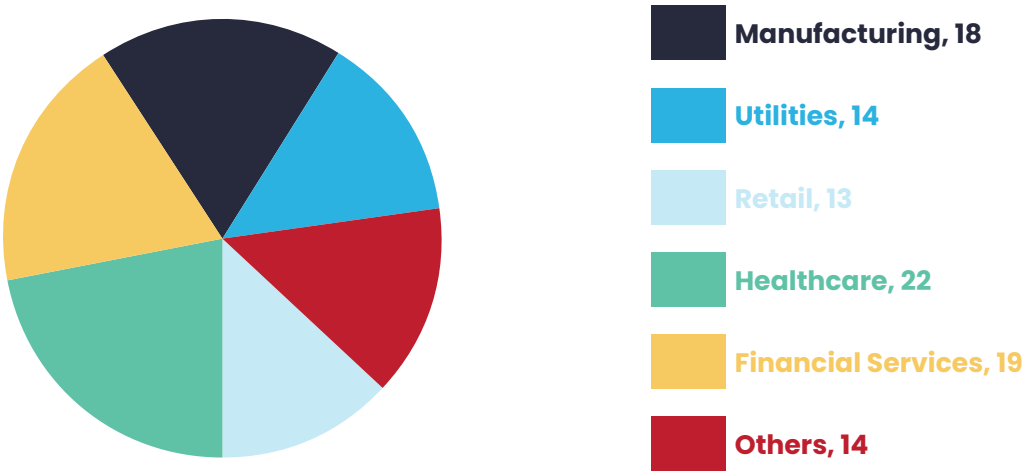
Days taken to monetize a cyber attack in 2021



In addition to a marked increase in the quality of malware detected, in 2021, almost 30 percent of the new malware isolated by us were first detected within the confines of Europe. There seems to be a renewed interest in Europe among hackers most of whom had some level of geopolitical connect. Sectrio's threat team was also able to isolate malware that was not seen anywhere else.

Networks hosting high-end and technologically complex segments such as aircraft manufacturing and space tech were targeted extensively by hackers. Most of the attacks logged came from APT clusters operating from the vicinity of North Korea while the next significant volume of attacks came from IP addresses in Pakistan and Iran.

Percentage attacks logged



According to publicly available information, the cost of a ransomware attack has gone up significantly. This includes costs associated with insurance, loss of revenue, cleanup, and ransom payouts. In terms of the tactics, hackers are trying to go wide and deep in accessing multiple components of the infrastructure being targeted including moving upstream across supply chains.

The number of malicious domains that came up in 2021 also went up by 31 percent in Europe. These domains were used to send phishing emails to recipients across Europe. With the increase in connected devices across the continent, the network traffic went up significantly and so did the proportion of severe attacks and breaches as a percentage of the overall volume of traffic.

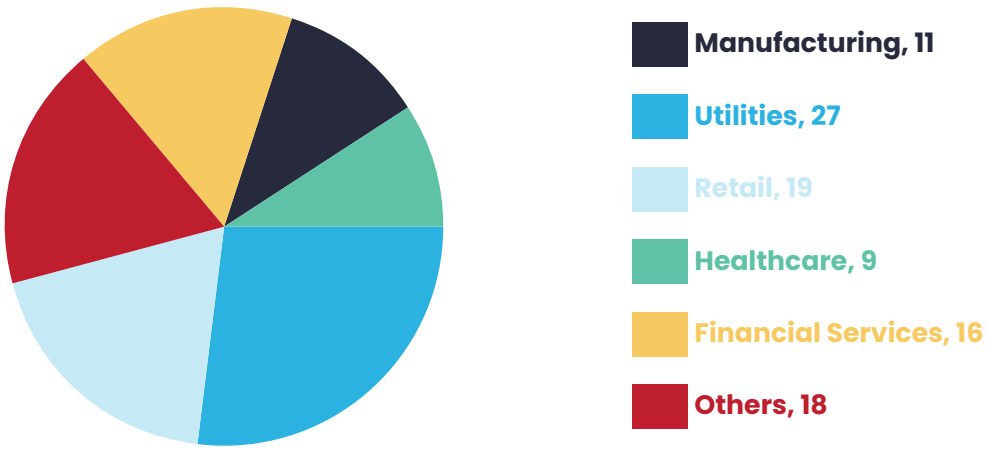
Ruthless efficiency enhancement tactics

Hackers across the world are trying to improve their targeting efficiency and are using several tactics to do so. For instance, the malware load encountered in network traffic streams across Europe has gone up significanmtly in 2021. This means that hackers are now pumping more malware as well as using multi-load launchers to deploy several payloads in one go. This increases the odds in their favor and strains the security teams through detection fatigue caused by increased work load.

Emerging cybersecurity challenges in Europe

- Lack of an economic impact model approach to categorize the impact of cyberattacks
- Growth in the number of unsecured IoT devices
- Key cities in the region are not just getting attacked but are also serving as malware transit points
- Massive growth in the number of malicious URLs
- BYOD leading to core networks getting infected
- Phishing attacks emerging from fake news sites and information shared on social media
- The cybersecurity posture of companies in the regions needs a revisit
- Regional convergence of attacks from multiple botnets
- Lack of visibility into networks leading to the malicious activity going undetected
- Sub geopolitical events are being used to target critical infrastructure

Percentage of sophisticated attacks logged



Most Attacked Countries in Europe

Country	Percentage of overall attacks
UK	13
Germany	8
Spain	7
Ukraine	6
Italy	3
The Netherlands	3

Most attacked cities in Europe

Cities	Percentage of attacks recorded
London	15
Kiev	9
Madrid	8
Berlin	7
Tallin	7

Inbound cyberattacks into Europe (origin)

Country	Percent
North Korea	21
Pakistan	17
Iran	13
Russia	12
Others including unknown	37

Oil and gas projects at risk across Europe

This is the most vulnerable sector in Europe which is now facing some unique challenges including:

- Stagnant cybersecurity budgets leading to a stagnation in the launch of new and improved risk management plans
- Increased attention from APT actors who are targeting exploration, drilling, and refining facilities in the region. Facilities in Bosnia, Croatia, Denmark, and Austria are at risk
- Increased detection of a new malware that is being used by APT groups to target Eastern European nations is also making its way into Western Europe leading to intentional or unintentional attacks on regional businesses
- Chatter picked up from the Dark Web and other forums point to growing interest in this sector among hackers
- Pipeline controls need to be secured as well

Just like North America and some parts of Asia-Pacific, government communications were targeted extensively throughout the region. Industrial and business-related cyberattacks that were targeted at entities connected with governments or those that had bagged projects from the government registered a significant rise.

Business users of infrastructure that relied on operational technologies that were running industrial communication systems and SCADA systems were targeted extensively. In some instances, in factories and plants where the assembly line was not functional during the lockdown and was restarted later, safety issues and problems related to malfunctioning of equipment were recorded due to residual malware that was not eliminated previously.

OUTLOOK FOR 2022 AND ADVISORY

Businesses need to stay alert and on guard on these dates in 2022. These events could serve to intensify cyber risks or could see a peak in cyberattacks due to geopolitical stresses unleashed. The defining event of 2022 for cybersecurity in Europe and for the world as a whole is the crisis in Ukraine. If this crisis is sorted out, it could have a positive bearing on the overall threat landscape around the world.

Table: key geopolitical events that could have an impact on the volume of cyberattacks in the region

Dates and Month	Events
February	Beijing Winter Olympics and European Central Bank meeting; tensions around Ukrainian crisis as well as challenges in Belarus
March 26	Hong Kong Chief Executive elections
April	Elections in Hungary and France and ECB meeting
June	G7 Summit
October	20th National Party Congress of the Chinese Communist Party
November	US mid-term elections

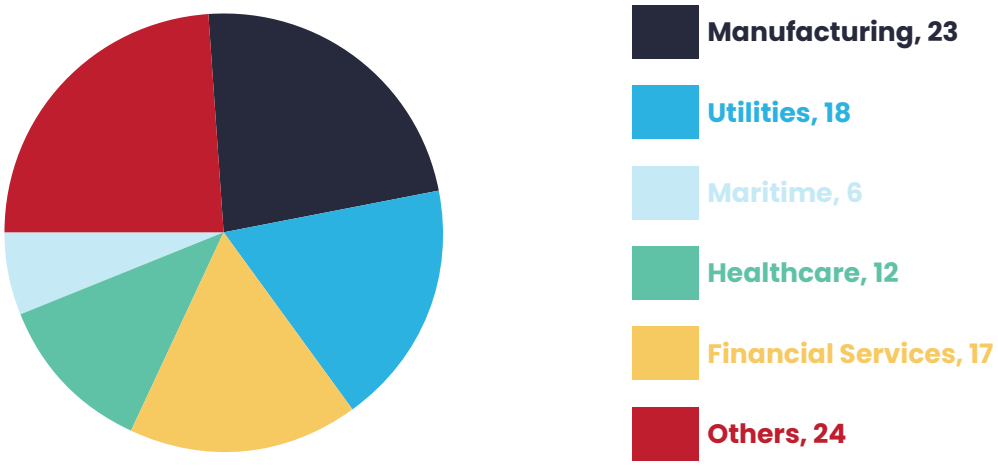
Asia-Pacific

Vietnam became the most attacked country in the region and the 4th most attacked country in the world. Vietnam rose by positions in a matter of just 7 months. All sectors in the country witnessed a significant rise in attacks from a new cluster that has sprung up in APAC in February this year. Attacks on the manufacturing sector in Vietnam alone grew by as much as 700 percent in 2021.

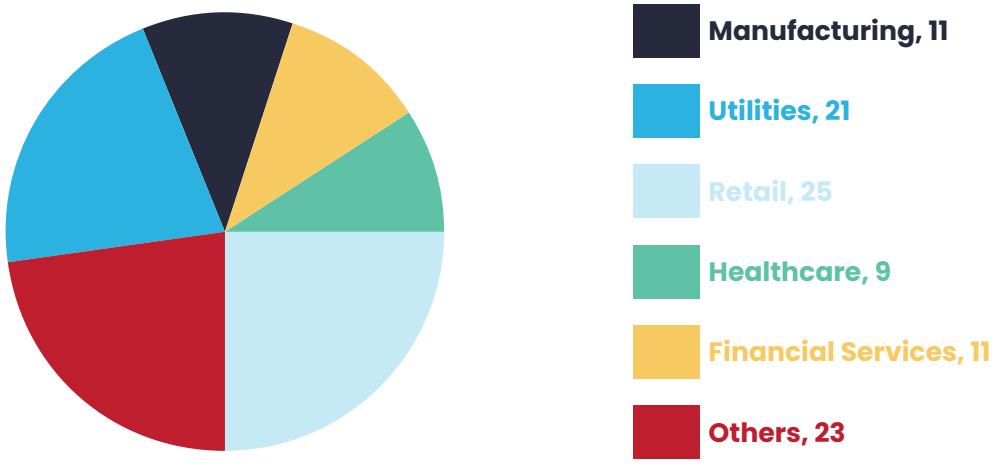
With many manufacturing hubs restarting (some without patching their digital infrastructure, the attacks on distributed manufacturing facilities continued throughout 2021. Manufacturing facilties in APAC are extensive and well established. Some of these facilities were not functioning at optimal employee strength and due to the disruption caused by the ongoing pandemic cybersecurity procedures were not followed and many drills and patch schedules were missed.

Hackers took this opportunity to ramp up their attacks using new malware and intrusion tactics. The rise in sophistication of attacks clearly led to more breaches and loss of data in the region.

Sectorwise percentage attacks logged



Percentage of sophisticated attacks logged



Most attacks on APAC businesses emerge from within the region itself, In addition to Vietnam, Singapore, Malaysia, Indonesia, and Taiwan were in the top five list of most attacked countries in the region. Our analysis points to the immediate countries surrounding the 3 APT clusters being the testing grounds for new malware and breach tactics. Some targets are also on the radar of these three clusters we have been tracking.

Together, these three clusters account for almost 13 percent of all cyberattacks logged in the region. The attacks have become qualitatively superior and more sophisticated. This is why the number of attacks has grown significantly and so have the number of cyberattack disclosures. The cybersecurity measures implemented by businesses in the region are yet to catch up with the level of sophistication we have seen among hackers.

Attacks from the region were also spilling over into other regions across the globe in the form of unintentional targeting as well as the leak of sophisticated malware and stolen information.

Regional malware launchpads

The presence of significant APT clusters aided by semi-independent hackers adds to the diverse cyber risk landscape of APAC. These clusters and their extended enablers were launching malware from diffused launchpads across the region. Such diffusion of malware launchpads also served to hide the origin of the malware while reducing the digital footprint of hackers. A study of over 700 suspicious IP addresses reveals that a majority of them were set up to confuse forensic and offensive cybersecurity teams that were out to uproot such hackers.

Where are the hackers getting their malware from? Even before we answer that question, we need to understand that hackers are trying their best to cover their tracks as mentioned earlier. Of the 700 malware variants we examined from the region, almost 70 percent had added codes to mask their origin and also to make it difficult to break them. Most of the malware we encountered were either procured or developed locally.

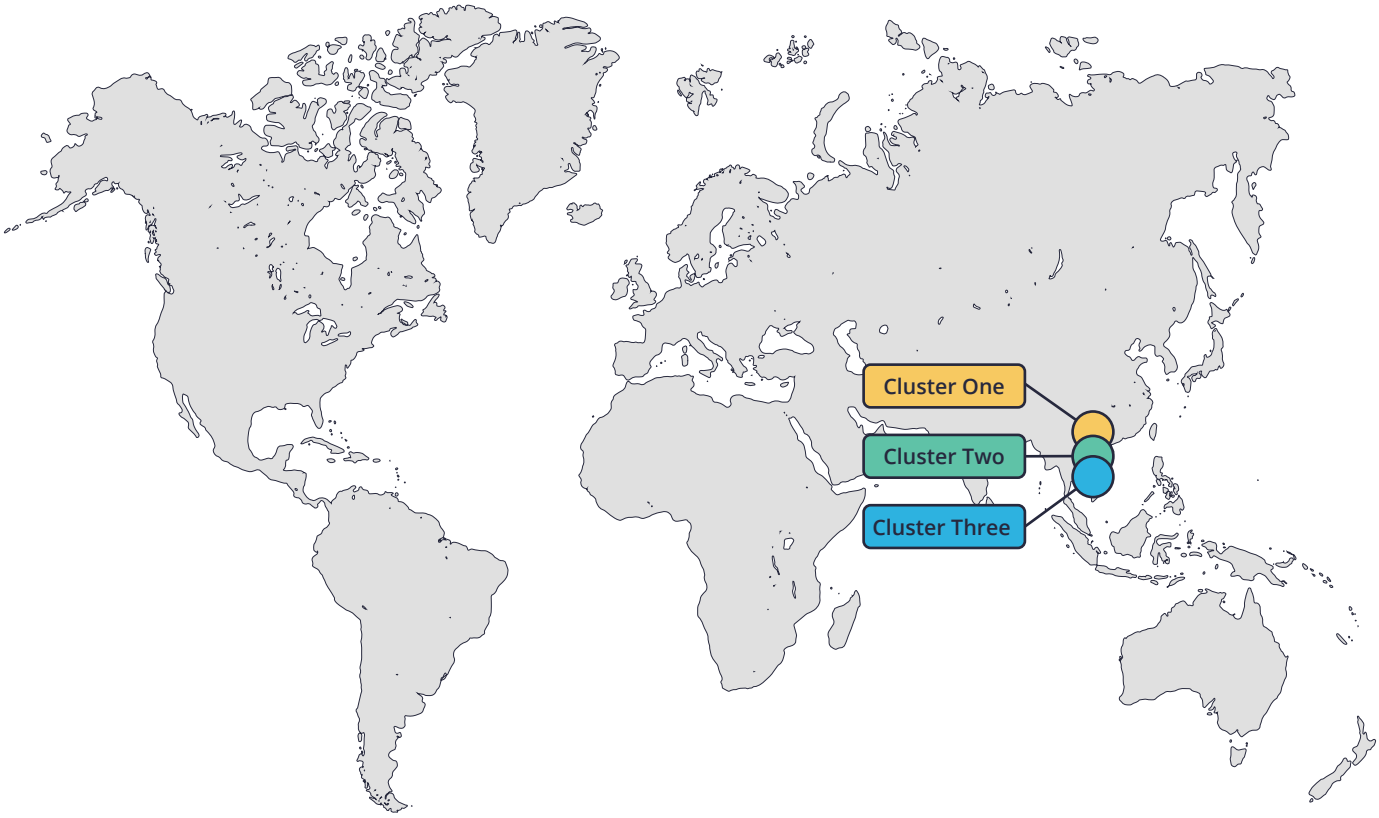
Reconnaissance attacks persisted for the longest time in APAC. This means that hackers are keeping a watch over networks for a long time waiting for an opportune time to strike. APAC is also among the most the three most profitable regions in the world for hackers. This could be because of the volume of cyberattacks, the number of successful breaches, and the ransom extracted from victims.

Porous networks and their impact

From IP cameras, human-machine interface systems, applications, controllers to smart assets and IT assets many businesses in the region are running their disparate systems on a single network. Because of such converged use of networks, laterally moving malware moves across different systems over the same network with ease. We came across instances where WiFi networks built for different end-uses were converging for no specific reason. In such networks, data from different end-use merges and moves together creating an environment where a single breach can expose the entire infrastructure to adversarial entities. In such instances, the entire network turns into an attack surface offering plenty of opportunities for hackers and adversarial entities to exploit.

This makes cyberattacks more impactful and destructive. Hackers in the region have identified this as an Achilles heel for businesses here and are working to exploit it. If businesses in the APAC region alone were to segment their networks and keep track of what's happening on their networks, the volumes of cyberattacks will dip significantly.

Distributed workforce, lack of cyber hygiene on the shop floor, partially secure control systems, lack of visibility into network components, and use of easy to hack credentials are among the other reasons for the rising cyberattacks and the increasing success of hackers. In countries such as Vietnam and Thailand, factories and manufacturing units expanded their production capacity by adding new devices without scanning for vulnerabilities or checking with published CVE databases.



APAC cyberattack clusters and their geographic origin

Another hotbed of cyberattacks was the East Asian region where we saw the highest volume of geo-politics-driven cyberattacks. Manufacturing, utilities, and smart city projects registered the highest volume of cyberattacks while the volume of attacks on defense, telecom and data centers again registered their all-time highs. Most attacks do have a geopolitical motivation in some form or manner as most malicious actors in APAC were either supported by or trained by states or state agencies. Some actors were also looking at state-owned or backed facilities for obtaining malware.

Rising attacks on key sectors in the region

Sector	Trend
Manufacturing	81 ↑
Smart Homes	55 ↑
Utilities	54 ↑
Banking	47 ↑
Defense	21 ↑
Others including agriculture, public safety, unspecified projects, and telematics projects not falling under the above categories	23 ↑

India

Is fast emerging as a malware playground for global malware developers

India registered a 290 percent rise in cyberattacks in 2021.Cyberattacks in India have certainly evolved in terms of complexity in 2021. While in 2020 we saw a rise in cyberattacks, in 2021 we logged significant targeted activity in the country. The emergence of transitionary botnets (I.E those that went silent after a short period of intense activity) targeting India is a new phenomenon that we are observing and this has significant ramifications for businesses in the region.

The biggest trend that was recorded in India in 2021 is that of the country emerging as a testing ground for new malware from across the globe. India's manufacturing and financial services sectors are today being targeted by malware developers from a range of countries who are using these attacks to:

- Study institutional responses and response mechanisms
- Improve the odds of successful cyberattacks on other regions in the future
- Hold data to ransom
- Test new variants of malware for their potency and stealth
- Study malware propagation streams (patterns of disbursement across regional networks)

In the crosshairs

Towards the mid/second half of 2021, we also saw the establishment of large-scale botnets to target key sectors in the country. These include manufacturing, defense, utilities, supply chains, and oil and gas infrastructure. These botnets that were switched on and off at random and operating across a wide range of IP addresses were sending a huge volume of phishing emails into the country

Why is India attracting a high volume of cyberattacks?

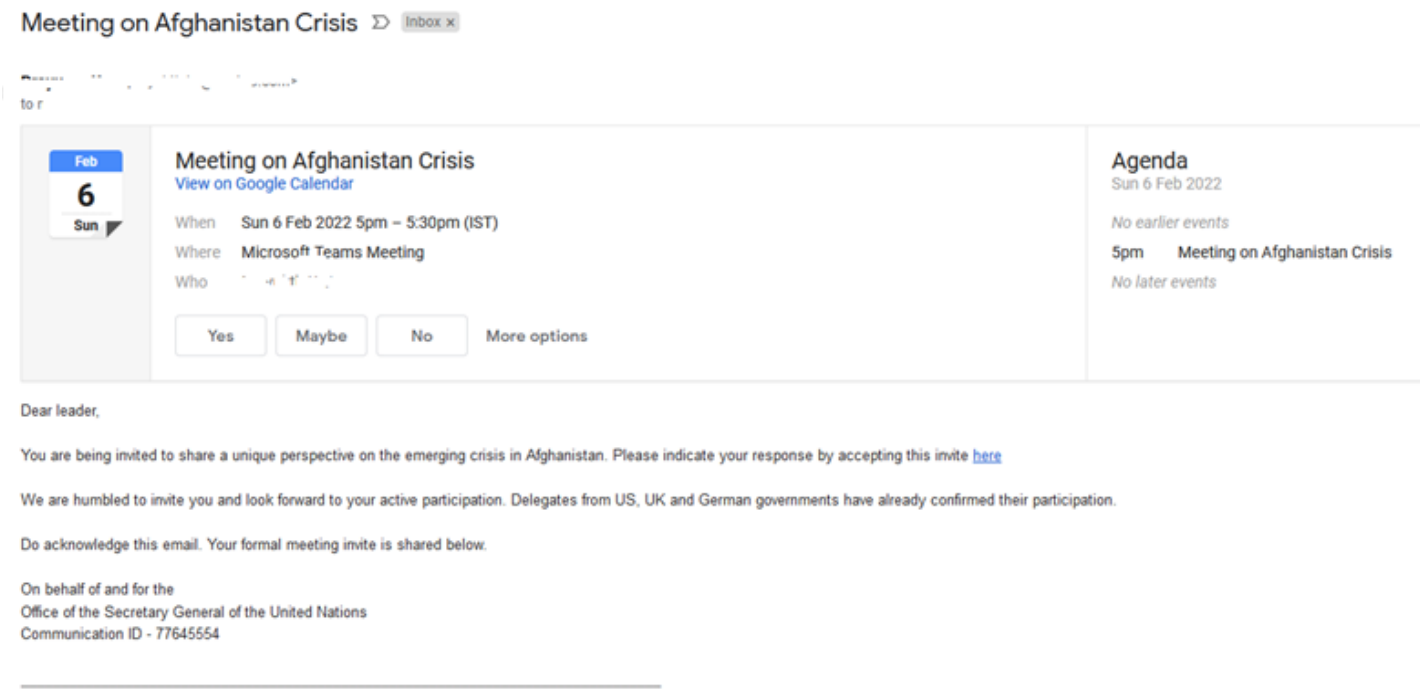
- A high number of malware variants were recorded by our regional honeypot network in 2020 and 2021.
- Extensive use of stolen AI-based tools that are helping create malware that are highly stealthy and adaptive
- The large presence of legacy unpatched systems
- The growing availability of connectivity and bandwidth
- The rapid expansion of digital threat surfaces
- Increasing volume of digital transactions in the country
- Regional geopolitical tensions in the region
- Growing penetration of financial services
- Expanding footprint of APT groups such as TA406 and APT29

The rising activity levels of North Korean APT groups is a matter of concern as they are known to target diplomatic and government communication.

All these factors have contributed to a major rise in cyberattacks in the country. In the financial services sector, small and medium banks have been extensively targeted by two specific APT groups from North Korea. These two groups one of which was also connected to an attempt to exfiltrate foreign exchange from an offshore account of a regional government in APAC are actively trying to infiltrate banking networks to target financial transactions at a very large scale.

RISING CYBER-ATTACKS FROM PAKISTAN

At least one APT group based in Pakistan was targeting India's government, maritime, oil and gas, and utility sectors. Mails similar to the one given below were sent out to various government officials across the country. The embedded link led to a malicious website that downloaded a RAT in the infected device. Targeting of defense assets is also done similarly with the devices belonging to armed forces personnel being targeted through a phishing campaign conducted through a popular instant messaging platform.


Meeting on Afghanistan Crisis Inbox ×

to r

Feb
6
Sun

Meeting on Afghanistan Crisis
View on Google Calendar

When Sun 6 Feb 2022 5pm – 5:30pm (IST)
Where Microsoft Teams Meeting
Who

Yes Maybe No More options

Agenda
Sun 6 Feb 2022

No earlier events
5pm Meeting on Afghanistan Crisis
No later events

Dear leader,

You are being invited to share a unique perspective on the emerging crisis in Afghanistan. Please indicate your response by accepting this invite here

We are humbled to invite you and look forward to your active participation. Delegates from US, UK and German governments have already confirmed their participation.

Do acknowledge this email. Your formal meeting invite is shared below.

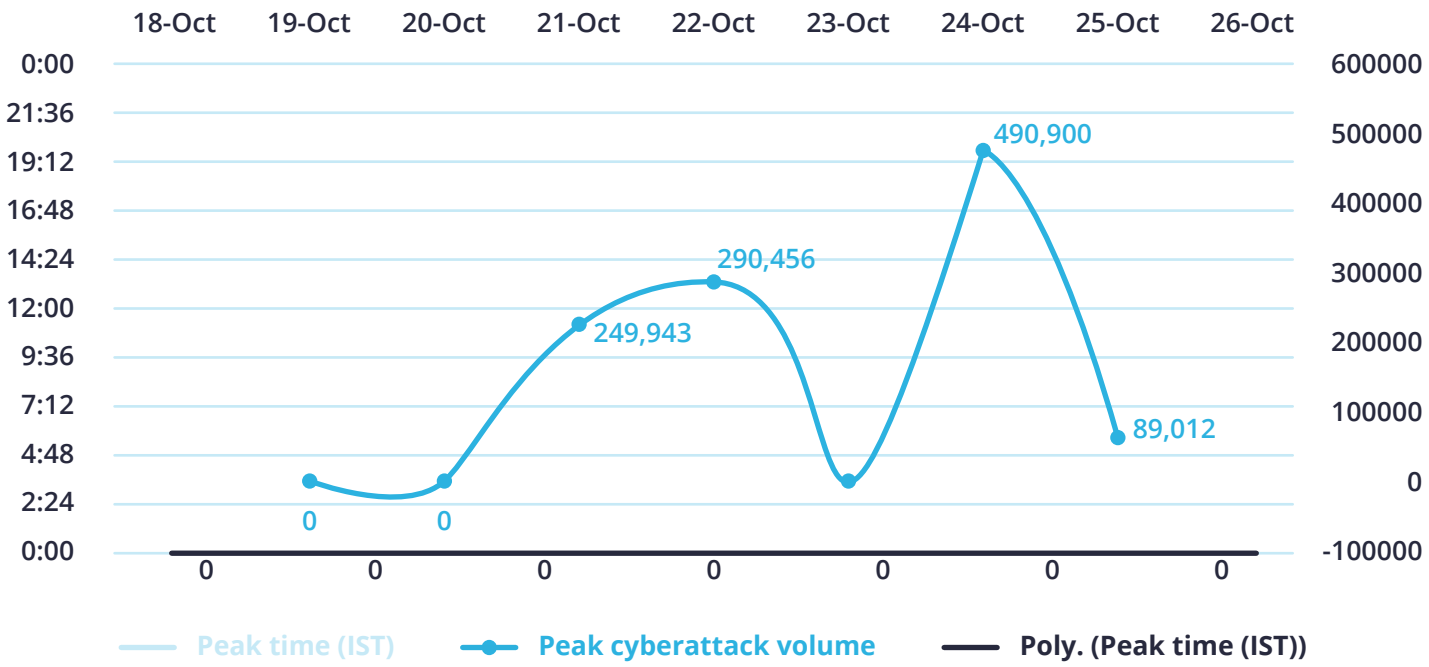
On behalf of and for the
Office of the Secretary General of the United Nations
Communication ID - 77645554

India Vs. Pakistan: cricket encounters on the field and digital battles off it Source: Sectrio.com/blog, October 25, 2021

While yesterday was a big day for cricket fans in the Indian sub-continent. Cricket teams from India and Pakistan clashed in a T-20 encounter as part of the ICC Men's T20 World Cup in Dubai. While the match was being held, we were able to record some interesting developments in cyberspace.

For the last 6 days, the number of inbound cyberattacks logged by our physical and virtual honeypots in India held steady in the region of about 3,00,000 attacks a day. On October 24th, however, the number of attacks rose substantially to hit the 490000 mark briefly before dipping significantly towards midnight Indian Standard Time. The cricket match was over by then. We are only considering the sophisticated attacks here (this does not include reconnaissance or low-grade probing).

Trends: Inboundcyber attack logged in India



Most of the cyberattacks were coming directly from IP addresses belonging to a certain country to the West of India (no prizes for guessing). There were also a few IP addresses from South East Asia and Eastern Europe that were participating in these attacks. These IP addresses belonged to known botnets which meant that they were being leveraged for coordinated event-based cyberattacks on the country.

While the spike in cyberattacks connected to a **geopolitical event** is now commonplace, it is the first time that such cyberattacks have been linked to a sporting event involving teams from the sub-continent.

GEOPOLITICAL DEVELOPMENTS AND CYBERATTACKS

Sectrio has in the past shown the links between geopolitical developments and cyberattacks in the Middle East, North America, and Southeast Asia. The mode of operation is more or less the same in all the cases which are that every spike in the volume of cyberattacks logged by our honeypot networks is linked to a geopolitical development in the region.

State-sponsored actors or nation-state groups are often behind such attacks. Third-party actors affiliated with state-backed actors are also activated by nation-state groups (or specifically their controllers) to increase the impact of such attacks. Even states that are not recognized by the United Nations have their own hacker groups that participate in such attacks. These groups earn foreign exchange or specifically hard currency for the treasuries of the states involved.

The cyber armory deployed by such groups has diversified in recent years with the induction of stealthy ransomware and advanced military-grade malware developed and sold by agencies backed by the cyber intelligence wings of nation-states. Malware dumps in the Dark Web and

malware procured from groups that steal them from academic institutions and private labs and sell them through forums are also used in such attacks after modifying them enough to evade detection and to hide their origin.

Every possible outcome including disruption, espionage, and theft of critical and confidential information, deployment of trojans for long-term spying, and infrastructure monitoring are pursued by such groups. The targets include critical infrastructures such as water treatment plants, power grids, oil and gas infrastructure, key manufacturing facilities, stock exchanges, and defense installations.

For possibly the first time, the background level of cyberattacks which usually rises during a geopolitical episode rose during a sporting event (refer report provided alongside). This marks the start of a new era of cyberattacks that are triggered not by major geopolitical tensions but by sub-geopolitical events such as cricket matches

This trend is not going to go away any time soon and needs to be addressed with urgency. The rise in background levels of cyberattacks also pushes the peak attack values to new highs (as seen in October) and during such phases, inbound cyberattacks may succeed by simply overwhelming cyber defenses and tiring out SOC teams. Which could be a possible motive for these attacks.

Key points

Looking at the data from the quality of malware and cyberattack sophistication perspective, the following inferences can be drawn:

- India's manufacturing capacity is being targeted systematically and this seems to be part of a larger gameplan
- Attacks on critical sectors are growing and 2022 may see a large attack succeeding to some extent
- In addition to utilities, adversarial entities seem to be interested in conducting persistent reconnaissance on critical infrastructure projects
- Hackers are trying to get into key projects early and stay on in the network through low footprint malware and communication tactics. The volume of data stolen from businesses here that are leaked on forums like the Dark Web is low because the hackers do not want to disclose their success or presence on the victim's networks
- Traffic rerouting and the use of malicious domains are now common tactic. Because of the widespread use of social media and instant messaging platforms, fake news and other means are deployed to trick victims to visit such sites and download malware on their personal or work devices.
- India is receiving a very high level of attention from hackers. There could be some long-term implications of this

Increasing attacks on manufacturing

Sector	Trend
Critical infrastructure (including government) attacks	70 ↑
Banking and finance	26 ↑
Smart cities	20 ↑
Defense	2 ↑
Manufacturing	101 ↑
Smart home devices	47 ↑
Others including agriculture, public safety, transportation unspecified projects, and telematics projects not falling under the above categories	35 ↑

We expect these attacks to increase in volume and sophistication in the second half of 2021.

The Middle East and Africa

Cyber-attacks on Middle Eastern entities continued to rise in 2021 with rising cyberattacks logged from 5 known clusters outside the region targeting critical infrastructure, manufacturing, utilities, and oil and gas sectors. Most of these attacks were characterized by:

- The exponential increase in the degree of sophistication
- A strong geopolitical connect
- The timing of the attacks was designed to coincide with major offline events including the onset of holidays, reopening of offices, and even government to government discussions
- Malware deployed in the region showed higher levels of new codes and segments indicating that the hackers may be working towards exclusively targeting entities in the region or using the region as testing grounds
- Attacks on manufacturing registered a 200 percent rise
- Cyberattacks are carried out in waves on targets with increasing intensity and loss of data registered in each wave
- New APT clusters have sprung up within the region and are now targeting strategic sectors of the economy in countries like Saudi Arabia, UAE, and Oman

> Attacks on OT environments and niche IoT projects are rising in the region

Attacks on oil and gas entities and manufacturing sectors continue to rise disproportionately. Through infrastructure optimization measures, many new devices and systems were introduced into the networks of companies in these two sectors across 2020 and 2021. These devices are introducing new vulnerabilities into the system and creating opportunities for large-scale breaches to occur in the future.

A large number of digital transformation projects have taken off in countries like UAE, Saudi Arabia, Oman, and Qatar in 2021. Most of the projects involve phased transition to technologies such as IoT, AI, blockchain, and others. Due to this transition as well as the increased infusion of automation, an increasing number of enterprises and business units are now functional with a diverse mix of infrastructure subsystems that permit cyberattacks by malware that move laterally. This includes movement through high levels of stealth and passive means of transit across networks and even air-gapped systems.

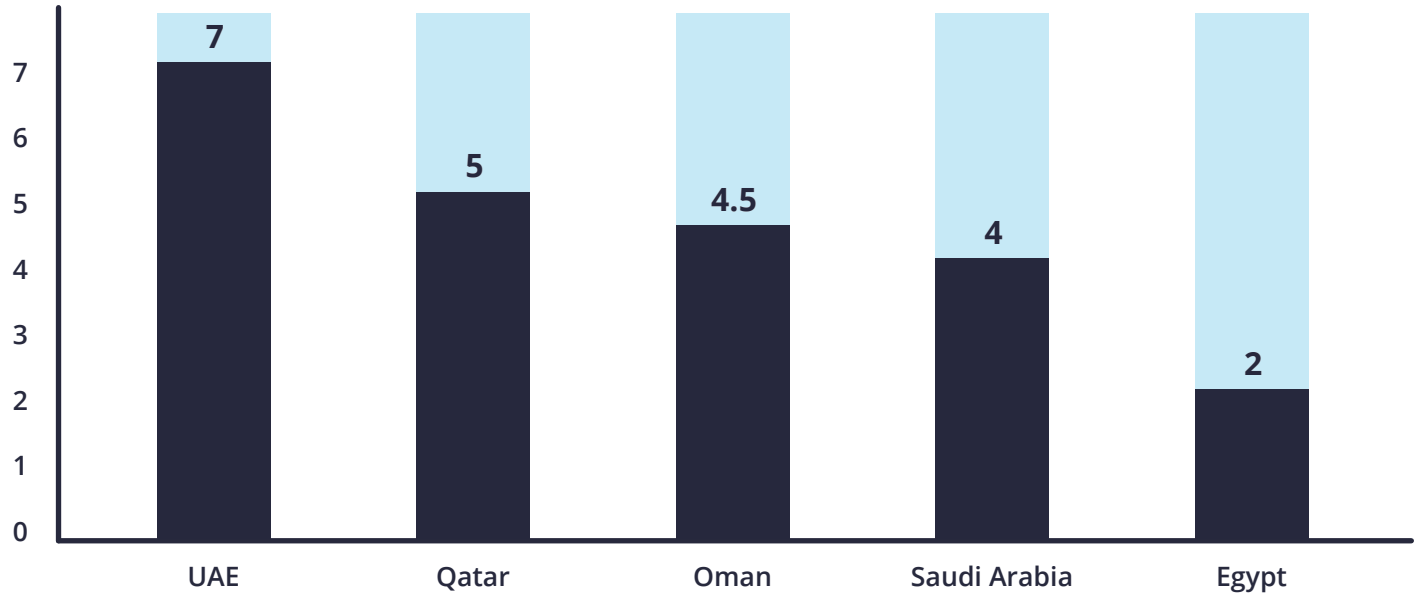
Extensive use of social engineering

Hackers are using a variety of social engineering means to attack targets. These include forged official emails and messages from instant messaging and other platforms to trick the recipient into thinking the emails are genuine and must be acted upon. We also came across some instances of reply phishing as well.

Bleeding data

UAE firms lost the maximum amount of data per cyber-attack as compared to other countries in the region. Other countries also lost data in proportion to the volume of cyberattacks experienced by them. Such data is turning up in all sorts of places. We are not sure about the amount of ransom that could have been paid by companies in the region but by looking at the volume of data leaked so far, significant amounts of ransom could possibly have exchanged hands in 2021.

Average volume of data stolen per cyberattack in 2021 (TB)



Energy plants, oil and gas transportation infrastructure, ports, large manufacturing plants, data centers, and projects that house eco-systems comprising diverse technologies that are connected and permit movement of data and therefore malware are prevalent in the region and have been extensively targeted.

The readiness of businesses to address threats related to OT or those that involve the lateral movement of malware is enabling malware developers to gain access to sensitive data by compromising key systems. This leads to large-scale exfiltration of data from systems. There have been instances of attackers creating and using digital profiles of actual equipment or monitoring systems to lure employees or trick systems. This is another gap that we have seen across the globe. Lack of multi-level access authentication and Zero Trust methods have made core systems sitting ducks for post-reconnaissance long terms attacks and data theft.

Perimeter-focused security measures and lax employee training have already created conditions that will lead to what will be a huge cyberattack in 2021. The clock is ticking. Hackers who often have multiple motivations including disruption, ransom, data and IP theft, revenge, and even espionage are striking at will to destabilize businesses that are gradually emerging from the pandemic.

Another matter of concern is the increasing digital footprint of North Korean actors in the region. Some of the clusters mentioned earlier were also active across the region. However, most of the activities we studied and isolated related to large-scale reconnaissance than actual attacks.

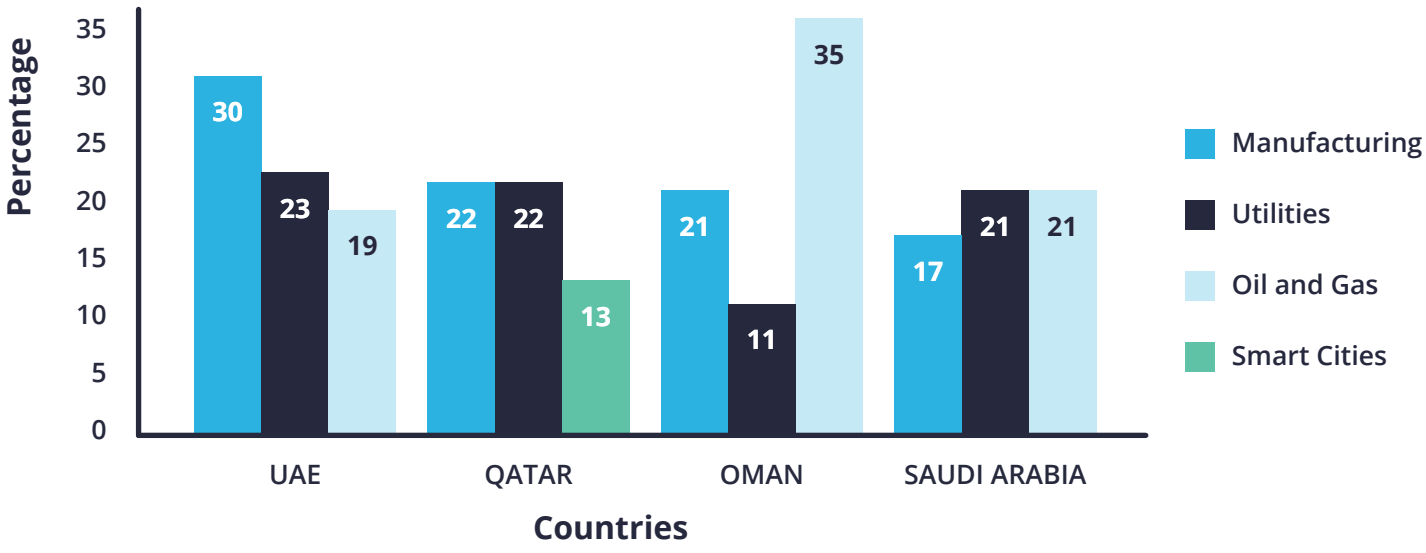
Rising cybersecurity concerns in the region

- Rise of new clusters of hackers
- Significant rise in the volume and sophistication of cyberattacks logged
- High volume of hacktivist driven attacks
- New and undetected vulnerabilities and cybersecurity gaps in key sectors that are open to exploitation by hackers
- Regional malware
- Lack of adherence to proven frameworks such as IEC 66423 and Zero trust

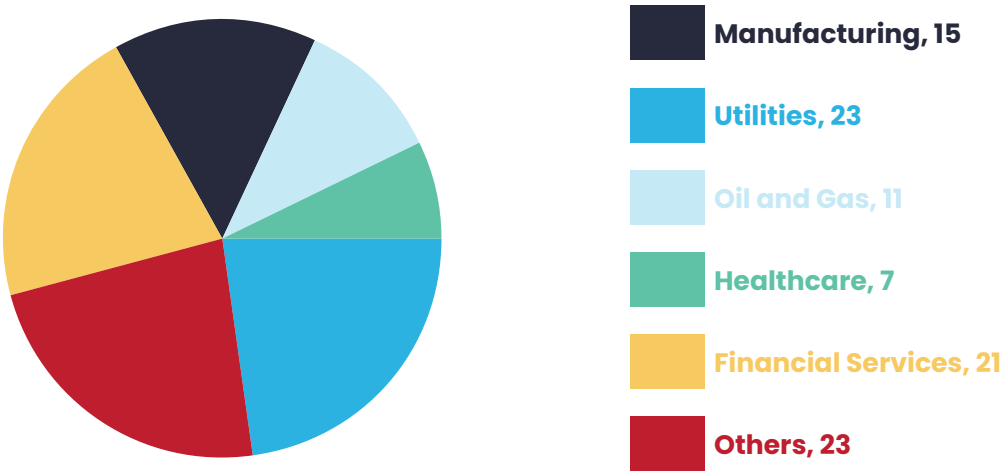
Percentage Geographical distribution (inbound cyberattacks)

Country	Percentage
UAE	19
Saudi Arabia	16
Oman	13
Qatar	9
Nigeria	9
Egypt	7
Bahrain	7
Others	20

Percentage of overall attacks



Percentage of sophisticated attacks logged



Why are cyberattacks on Middle Eastern businesses growing?

- Cybersecurity is yet to receive the required attention from key stakeholders
- APT actors are using businesses to gain access to governance infrastructure
- Regional geopolitical conflicts are also pushing APT activity targeting large scale disruption around utilities, financial services, and manufacturing sectors
- Use of OT networks that are relatively less secure
- Supply chain attacks have significantly evolved in the region
- Financial services and government agencies are being targeted for stealing data and for generating ransom
- To steal Intellectual Property and to keep a tab on some of the emerging start-ups and financial hubs in the region
- Some of UAE's key sectors are embracing automation and experimenting with new and emerging technologies. Some of these projects are not getting adequate security in the pilot phase which opens the door for hackers to deploy malware that resides in these networks beyond the completion of the pilot phase

Looking ahead: cybersecurity predictions for 2022

With the arrival of a new year, new threats also emerge as do new actors, new malware and breach methods. So how will 2022 impact IoT and OT security and what new trends will we have to be aware of? Here are some answers.

Rise of geopolitical threats: with the worsening geopolitical situation in Europe and the Middle East, we can expect new levels of APT activity in these geographies that will have a spill offer effect on other regions.

Network and device vulnerabilities will get more attention from hackers and businesses: while hackers will try and exploit these, businesses will try to get more disciplined with respect to patching and scanning schedules. An event similar to the Colonial Pipeline episode and others cannot be ruled out and we expect a major episode on these lines to occur around the second quarter of this calendar year. In instances where the codes are widely used across an industry such as in the instance of Log4j, more application security vulnerabilities will surface.

2022 will be the year of cyber threat intelligence: towards the second half of 2021, many businesses were seen shopping for threat intelligence feeds. This exercise will intensify in 2022 as businesses seek to improve their threat detection capabilities to improve their cyber risk management efforts and their overall security profile.

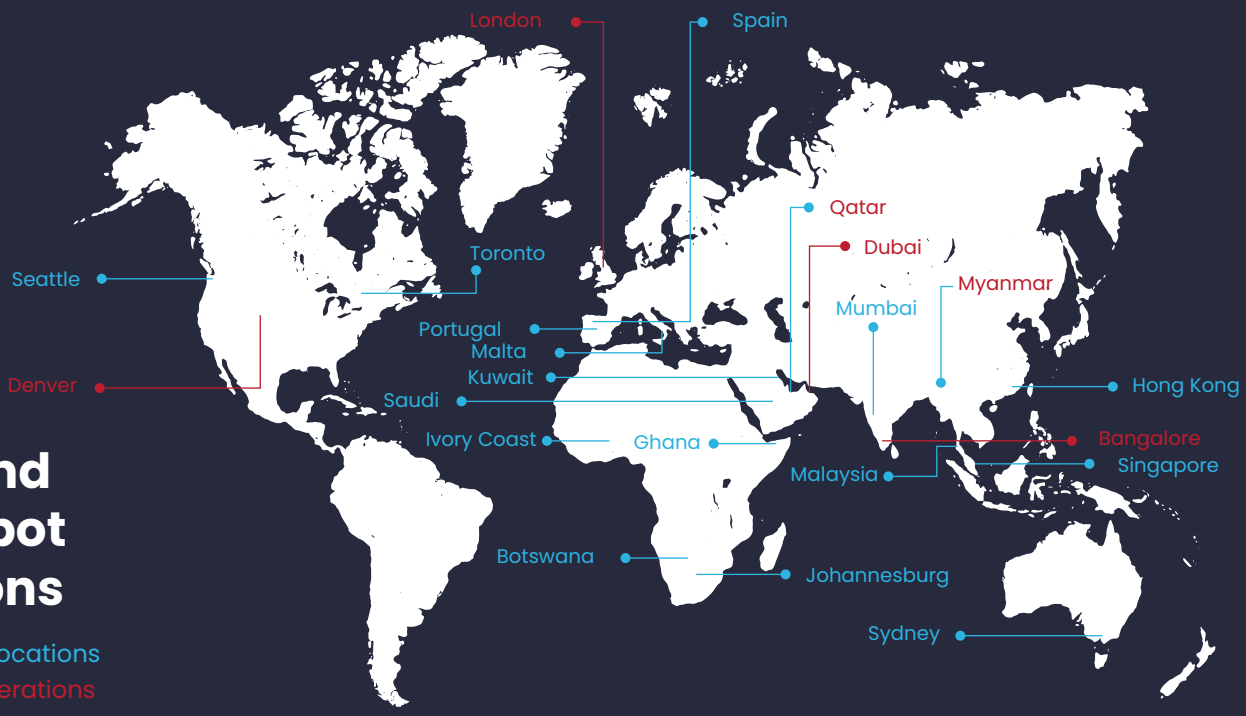
Compliance and standards: with many nations coming out with IoT and OT cybersecurity policies, compliance mandates will move from a voluntary exercise to a compulsory one for sectors that are not hosting any critical infrastructure. This means that governments will ask businesses to ramp their cybersecurity measures to align with existing standards like IEC 62443 or new ones that will be enacted. We can therefore expect more compliance regulations to better manage cyber risks including those related to remote/hybrid workforce.

The year of reporting: as we have seen in the US, reporting after a cybersecurity episode will be made mandatory with clear guidelines on who should know what and when. We expect more incident reporting legislation to be enacted around the world.
Oil and gas companies will be targeted in a new wave: most of these attacks will be carried out by APT actors and hacktivists.

Supply chain vetting and internal security practices will turn mainstream and more streamlined: 2021 was the year of supply chain disruption. In 2022, the supply chain situation will stabilize and will result in the adoption of new cybersecurity practices to deepen resilience and to ensure that these are not disrupted from within by supply chain poisoning. Internal security policies will also be strengthened to reduce threats from insiders.

Attack surfaces will continue to expand Thanks to digital transformation and automation. More IoT and OT cyberattacks will grab headlines: businesses will find it difficult to contain information on such attacks and thus we will a rise in the appearance of such reports in the media.

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

12303 Airport Way, Bldg.
1, Ste. 180, Broomfield,
CO 80021

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