

Cybersecurity threatscape Asia 2022-2023



Contents

Introduction.....	3
Main conclusions.....	3
Digital development and new threats in Asia.....	4
Main targets of attackers.....	6
Main cyberthreats.....	10
Cyberespionage and data leaks.....	11
Malware.....	15
Ransomware.....	17
Social engineering.....	18
Development of cybercrime forums.....	19
Legislative issues.....	21
Conclusions and recommendations.....	23
Recommendations for governments.....	23
Recommendations for businesses.....	24
About the research.....	26

Introduction

Cybersecurity becomes a key challenge to governments, organizations, and individuals in a world where digital technology permeates every area of life. Culturally, politically, and economically diverse Asia is no exception when it comes to this global trend. Asian nations have been at the forefront of technological innovation in recent years, but the evolution of digital technology has inevitably increased the need for robust cybersecurity strategies in these countries.

This report deals with the state of cybersecurity in Asian countries. We focus in detail on six major nations in the region: China, India, Thailand, Malaysia, Vietnam, and Indonesia. These countries hold significant regional influence, are at different phases of digital transformation, and face various cybersecurity challenges.

The precise goals of this report are as follows:

- Make an assessment of the current cybersecurity landscape in the region.
- Define common cyberthreats and vulnerabilities.
- Analyze the cybersecurity law and regulation issues.
- Suggest recommendations for improving cyberresilience.

Main conclusions

- Asia has a rapidly evolving digital economy and technology. However, with this innovation has come an increase in cybercriminal activity, and consequently, a need for stronger cybersecurity.
- Asia-Pacific (APAC) was the most attacked region in 2022: it accounted for 31% of attacks globally.
- The rise in cyberattacks is threatening Asia's vital economic sectors, which grow more vulnerable as digital transformation continues. The most frequent victims of cyberattacks were government agencies (22% of total attacks on organizations), industrial companies (9%), IT companies (8%), and financial institutions (7%).
- Cyberespionage is a major threat to organizations and states in Asia. As many as 49% of successful attacks on organizations resulted in compromise of sensitive information. Bad actors hunting for both user data and trade secrets. Governments and organizations invest heavily in research and technology, which explains the increased activity by cyberespionage gangs: stealing this kind of information can give competitors a technological advantage.
- In 27% of successful attacks, organizations' core operations were disrupted, with business processes suspended and access to infrastructure and data interrupted.
- Ransomware poses a major threat to businesses in the region. Its main victims were industrial companies, which accounted for 34% of successful attacks. Extortionists also target healthcare institutions, financial organizations, and IT companies.

- Dark web forums are seeing sales of network access credentials, compromised databases, and breach services. The most common ads in the region are for the sale of access to organizations in China, Thailand, and India. These are mainly government organizations, IT companies and service sector companies. The price of information that can be used to access a network ranges from a mere one hundred dollars to several thousand, and varies with the organization and the level of permissions.
- Despite the rapidly evolving digital infrastructure and the readiness to invest in cybersecurity, cybersecurity laws still offer room for improvement. Moreover, there is a noticeable want of international cooperation and uniform regional standards.
- Recommendations for governments on improving the standards of cybersecurity include updating cybersecurity laws, improving liaison between organizations and national cyberincident response centers, supporting cybersecurity training programs, and promoting international ties and data exchange.
- Recommendations on improving the cyberresilience of organizations include defining non-tolerable events and protecting critical assets, monitoring and responding to cyberthreats with advanced security tools, evaluating the efficacy of implemented measures, and training employees.

Digital development and new threats in Asia

A unique confluence of cultures and traditions, Asia is also a hub for innovation and technology. The Asian economies are some of the world's most dynamic and fastest growing. The region's digital economy is evolving in a rapid manner. Technology giants maintain a presence in Asia, and e-commerce platforms are sprouting. Southeast Asia's digital economy [is growing](#) by 17% annually, and China's by 13%; these rates of growth exceed those of both the United States (7%) and Europe (10%). The Internet economy of Southeast Asia is predicted to reach [\\$1 trillion](#) by 2030, driven by e-commerce, digital payments, e-learning, and remote work. In the digital payments sector alone, transactions are expected to [total](#) between \$600 billion and \$1 trillion.

The number of Internet users is rising at an accelerated pace. The overall percentage of the Asian population with access to the Internet is 67%, reaching even higher in Southeast Asia (80%). Smartphone usage in the region's most developed nations is similarly high, for example, 90% in Malaysia. The technologically advanced nations are increasingly adopting new technologies, such as the Internet of Things, virtual reality, artificial intelligence, and autonomous vehicles, which are critically dependent on secure Internet service.

Governments have adopted digital transformation programs to promote infrastructural growth. The many government initiatives, such as Digital India, Smart Nation Singapore, or Malaysia's MyDIGITAL, are proof of the region's ambition to become a digital leader. Large-scale investments in digital infrastructure make the region a magnet for technology startups and large, established market players.

47%

of those surveyed spoke about an increase in the attacks on their organizations ([the 2023 Thales Data Threat Report states](#))

Threats go where innovation is: the rapid digital development has not always been accompanied by bolstering cybersecurity, while the region's attractiveness to cybercriminals has only increased. The growing dependence on technology makes cybersecurity a top priority for governments, businesses, and individuals.

According to an [IBM report](#), APAC was the most attacked region in 2022, with 31% of attacks globally. A [Check Point report](#) indicates that the weekly average number of attacks in APAC in Q2 2023 increased by 22% year-on-year. More than half (59%) of all APAC organizations [said](#) that they experienced cyberattacks in 2022.

A [July 2023 survey](#) by Cloudflare that involved more than 4,000 cybersecurity managers in Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam showed that 78% of those interviewed had experienced at least one cybersecurity incident in the previous 12 months. Of these, 80% reported 4 or more incidents, and 50%, 10 or more. Around 63% put the financial impact of cyberincidents on their organizations in the previous 12 months at a minimum of \$1 million, with 14% saying their losses had exceeded \$3 million.

The region's governments are cognizant of the threat, so they increasingly attach value to developing national cybersecurity programs and investing in the implementation of these. That said, the region suffers from a lack of cooperation between nations and uniform cybersecurity standards, save for isolated ASEAN initiatives. In several of the countries, the legal framework lags behind the threat landscape. Organizations face vague or unrealistic regulatory requirements the violation of which carries harsh penalties.

Despite the rising frequency of attacks, only 38% of those surveyed by Cloudflare [described](#) their organizations as being well prepared to deal with cyberthreats, whereas those in the healthcare, education, the public sector, and tourism said they were likely unprepared for repelling cyberattacks.

Despite the large number of cyberincidents, more than one-third (36%) of organizations [lack an incident response plan](#) and are therefore vulnerable to attacks.

Although Asian nations are investing substantial resources in cybersecurity, there is a shortage of skilled professionals who are capable of countering advanced threats. Malaysia alone needs 8,000 more cybersecurity professionals. The Malaysia Cyber Security Strategy (MCSS) aims to solve the problem by training and certifying [20,000 cybersecurity professionals](#) by 2025. According to a [VNISA survey](#) on the state of cybersecurity of 135 organizations in Vietnam, up to 76% have a cybersecurity workforce that is inadequate to today's requirements. APAC in general has recorded the highest rate of increase in cybersecurity professionals in 2022 (15.6%). Still, according to [ISC2 data](#), the shortage of trained cybersecurity employees is estimated at 2.16 million. Most experts in the region believe this gap is putting their organizations at a risk of cyberattacks.

The evolution of technology in Asia and the rise in the number of Internet users will continue to attract cybercriminals to the region. Unless measures are taken to raise cybersecurity standards, Asian nations will continue to face economic losses from cyberattacks every year.

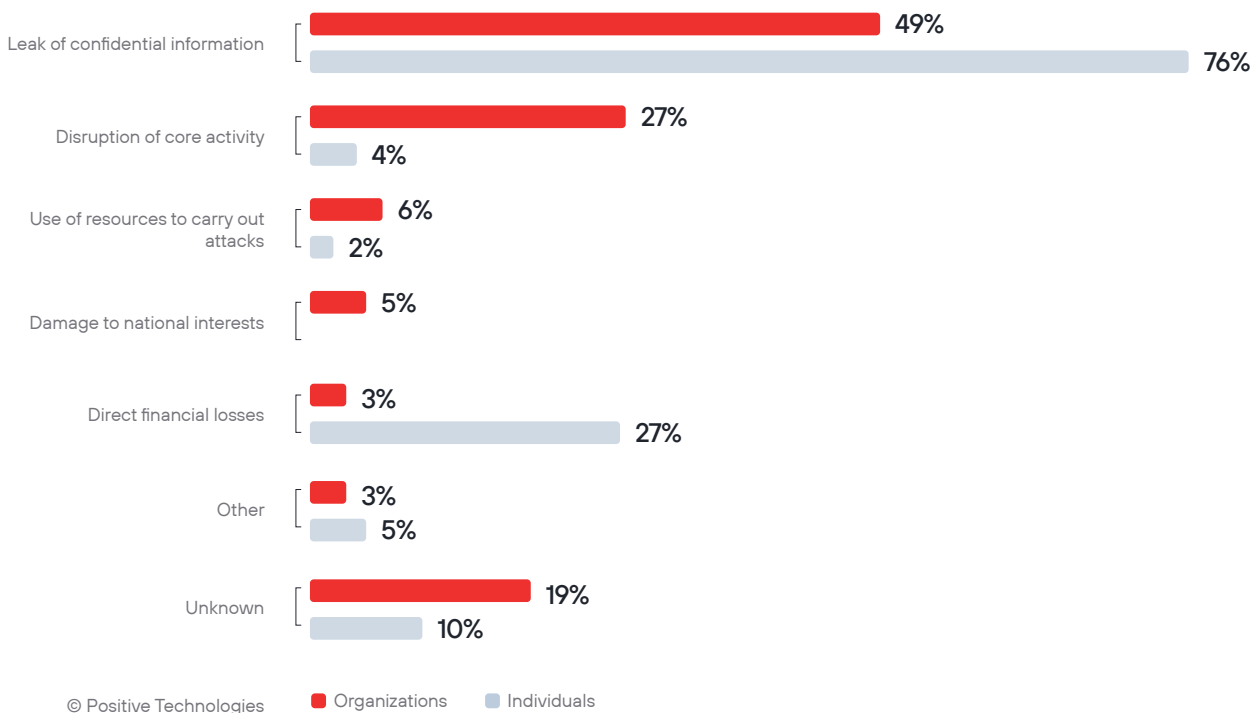
Main targets of attackers

Cyberattacks may have various negative consequences, all the way to non-tolerable events that have a catastrophic effect on the organization's operations. Virtually every other (49%) successful attack on an organization resulted in compromise of sensitive information, and in 27% of cases, victims suffered disruption of core operations¹ including suspension of business processes and interruption of access to infrastructure or data.

A relatively small percentage of attacks (3%) resulted in direct financial loss due to the need to pay a ransom or theft of funds from the company's accounts. Yet the cumulative damage from a cyberattack includes overhead, such as the costs of response, investigation, recovery of infrastructure, downtime, and customer churn. For instance, [IBM estimates](#) the average cost of a data leak to a company in an ASEAN country in 2023 at \$3.05 million, and in India, at \$2.18 million.

¹ A non-tolerable event is an event, caused by a cyberattack, that prevents the organization from achieving its operational or strategic goals or leads to long-term disruption of its core business.

Figure 1. Attack consequences



74%

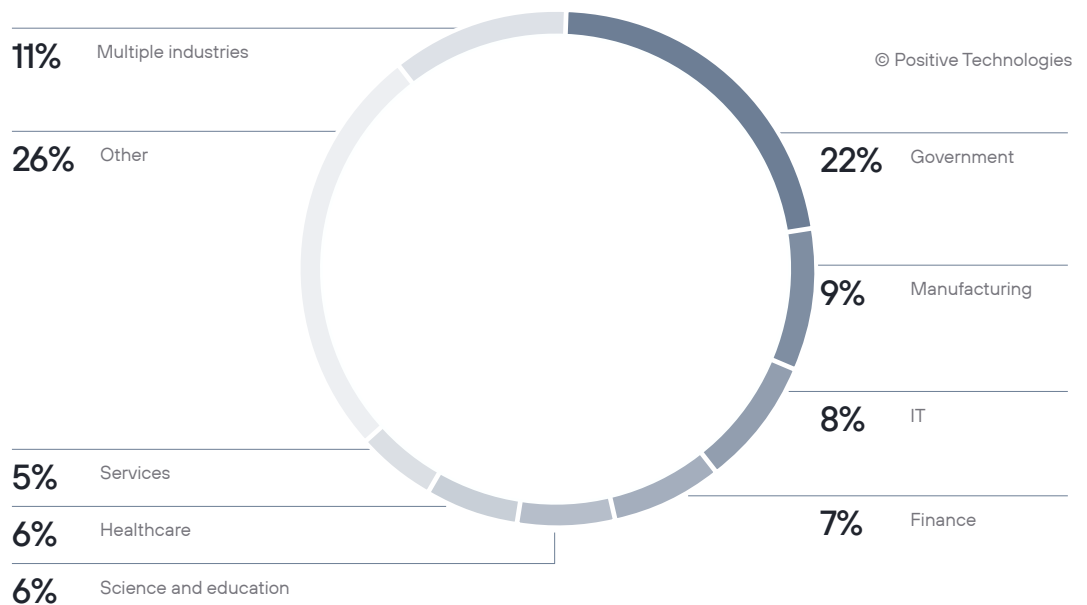
of attacks were targeted, that is, they were aimed at specific organizations, industries, or individuals.

Common users have experienced data leaks as well, with 76% of successful attacks producing such consequences. In 27% of cases, users lost money to malicious activities.

During the period in review, from early 2022 through H1 2023, the most frequently attacked organizations were government agencies (22%), industrial companies (9%), IT companies (8%), and financial institutions (7%).

24%
of successful attacks
were aimed at
individuals

Figure 2. Categories of victim organizations



Government agencies

The government agencies in Asia have become cybercrooks' main target for several reasons. First of all, their systems hold a lot of valuable information, such as citizens' personal data, statistics, and information of national importance. Attackers managed to steal data in 44% of successful attacks on government organizations. In 2022, several major data breaches from government agencies in Asian countries were recorded. For example, in the autumn of 2022 in Indonesia, a cybercriminal [stole](#) a database containing information on 105 million citizens, including personal data such as identification numbers. It is believed that the data was stolen from the Indonesian General Election Commission. The database was put up for sale on the dark web for \$5,000.

Many countries in the region are pursuing digital transformation and actively integrating new technologies into their government systems. However, this gives rise to new vulnerabilities. Some government agencies cannot meet high cybersecurity standards due to limited resources or insufficient awareness about cyberthreats. In July 2023, it was [reported](#) that data from over 300 million Indonesian residents had been leaked, presumably from the Dukcapil system. Among the leaked data were citizens' identification numbers, contact phone numbers, email addresses, and home addresses. Dukcapil, a department of the Ministry of Home Affairs, is responsible for handling citizens' data and maintaining population registries in Indonesia. Dukcapil provides government services to the population, including issuing identity cards, birth certificates, and death certificates. It allows organizations, including financial institutions, to prevent fraud by verifying users. This agency plays a crucial role in Indonesia's population accounting system and is actively involved in digital transformation and the adoption of new technologies.

Furthermore, Southeast Asia, India, and China have significant political influence. Cyberattacks on government institutions can be carried out both by hackers wanting to express their political ideas and by highly skilled APT groups aiming for espionage or destabilization in the region. For instance, in 2022, the hacker group DragonForce [attacked](#) the web resources of over 70 government and commercial organizations in India.

Manufacturing

Manufacturing enterprises in the region are important elements of the global supply chain and play a key role in the world economy. These countries are global leaders in the production of goods. For example, China accounts for about 30% of the world's total production. As a result, they are subject to attacks involving cyberespionage or economic sabotage. Furthermore, from the perspective of extortionists, large manufacturing and industrial companies are tempting targets, as they are more willing to pay substantial ransoms to restore operations and avoid downtime.

Manufacturing plants and industrial companies often possess valuable intellectual property, such as technology patents and trade secrets, which can be the target of cyberespionage. Asian manufacturers invest billions of dollars in research and development annually. For instance, China [spent](#) over 3 trillion yuan (about \$456 billion) on scientific research in 2022. Stealing such information can provide competitors or foreign states with a technological advantage.

In 2023, the Indian company Solar Industries Limited, a manufacturer of industrial and defense explosives, fell victim to a ransomware [attack](#). The BlackCat group (ALPHV) stole 2 TB of data from the company's servers. Among the stolen data were technical details of the manufactured weapons and explosives, blueprints, information on arms shipments, and the company's contracts.

Disruption of key enterprises' operations can seriously impact a country's economy as a whole. Attacks on such factories or production facilities can disrupt global supply chains, causing economic losses and market instability. Suzuki Motorcycle India faced a [cyberattack](#) in May 2023 that shut down its factories for a week. The company estimates that the loss in production during this period was more than 20,000 vehicles. Suzuki Motorcycle India is the fifth-largest manufacturer of two-wheeled vehicles in India, with a production volume approaching one million units.

IT

IT companies are among the top three most targeted industries for a number of reasons. First of all, the countries of Southeast Asia, including India and China, have experienced rapid growth in the IT sector and become centers of technological innovation, home to some of the world's leading IT companies. These companies possess a large amount of valuable data, including intellectual property and user information, which is of particular interest to cybercriminals. Hacking into these companies can bring attackers substantial profits, whether through selling information on the black market or using it for a competitive advantage. Furthermore, the resources of well-known IT companies can be used to carry out attacks on other organizations worldwide.

In June 2023, Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest microchip manufacturer, reported a [data breach](#). The culprit, LockBit ransomware group, demanded a \$70 million ransom from the company, threatening to release the stolen data. The data breach, described by a company representative as «related to the initial setup and configuration of a server,» occurred due to a security incident at one of TSMC's IT providers, Kinmax Technology. The extortionists threatened to disclose TSMC's network entry points and access credentials.

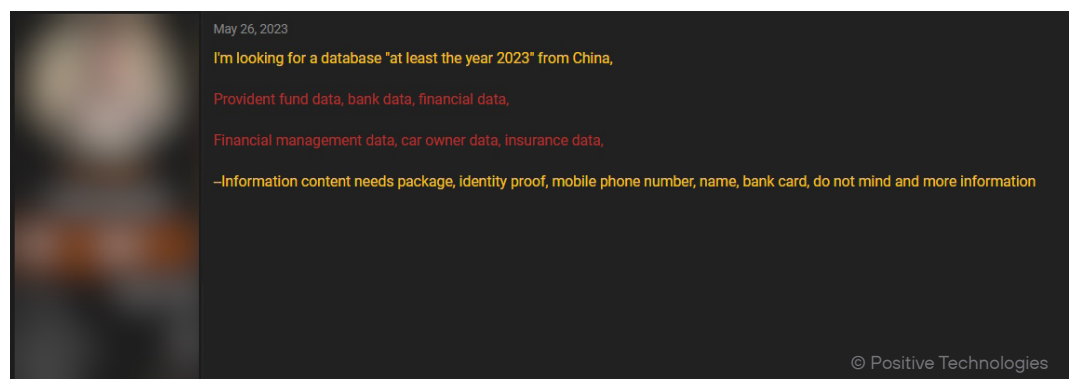
While security regulations are becoming stricter, many companies in these regions do not yet fully comply with international security standards. This can make them more vulnerable to cyberattacks.

Finance

Financial and insurance organizations are often at more advanced stages of digital transformation compared to other industries. As a result, cybercriminals must work harder to successfully carry out attacks against these organizations, and they typically resort to social engineering methods. However, in this region, we see two main attack vectors: malicious email attachments and vulnerability exploitation. This indicates a relatively low level of security for financial organizations. The main victims of these attacks were Indian banks. In half of the cases, a successful attack resulted in the theft of bank customer data.

It is noteworthy that the advertisements for the purchase of databases on shadow forums are mainly related to financial institutions. Such information can be used to carry out phishing attacks. For example, in March 2023, news broke about the [data leak](#) of 600,000 customers of the Indian HDFC Bank. The compromised data included names, birthdates, phone numbers, email addresses, physical addresses, employment information, credit ratings, and loan details. Following this, users began reporting breaches of their bank accounts and attempted phishing attacks.

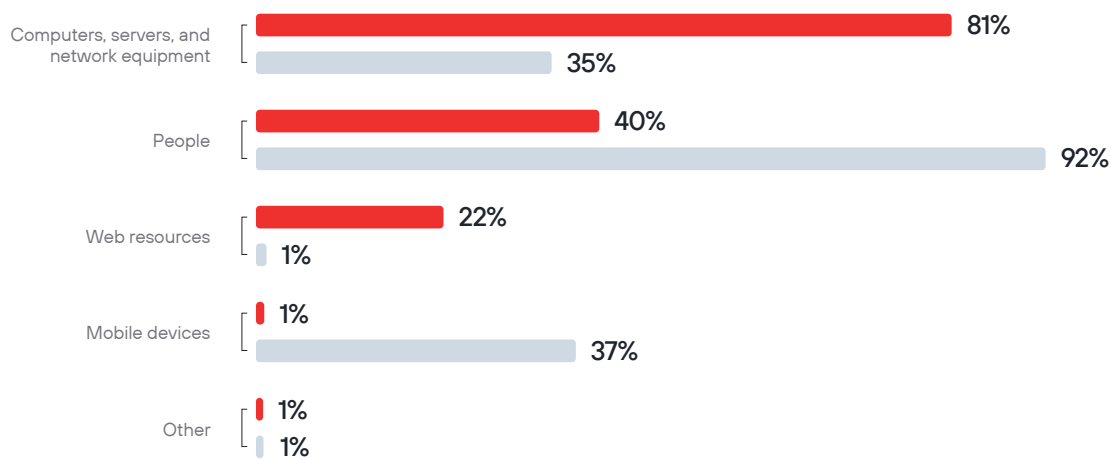
Figure 3. Announcement for the purchase of data on a shadow forum



Main cyberthreats

The majority of attacks on organizations (81%) are aimed at computers, servers, and network equipment. In 22% of cases, attackers successfully hacked web resources, most often using known vulnerabilities or compromised credentials.

Figure 4. Attack targets



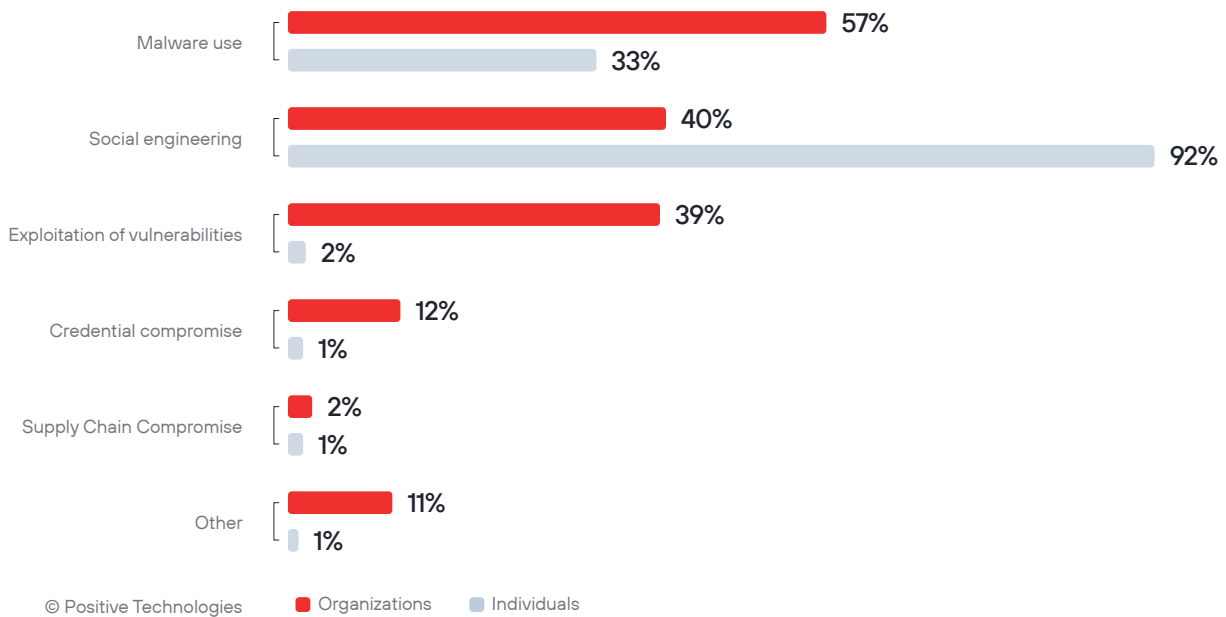
© Positive Technologies

■ Organizations ■ Individuals

In attacks on organizations, malware is used in 57% of cases. Social engineering methods (40% successful attacks) and vulnerabilities in company resources (39%) are almost equally common vectors. This indicates that the publicly available resources of companies are not sufficiently protected. Resources in less secure countries can also be [used](#) as training grounds for exploiting vulnerabilities.

In 12% of cases, attacks were carried out using compromised credentials.

Figure 5. Attack methods



Individuals were victims of social engineering in 92% of attacks, and malware was used in every third successful attack against them.

Cyberespionage and data leaks

In attacks on organizations, the perpetrators most often managed to steal personal data (38% of the total stolen information), credentials (14%), and trade secrets (28%). Personal data leaked mainly from the systems of government agencies, service companies, retailers, and financial organizations. Meanwhile, trade secrets were the criminals' main goal in attacks on industrial organizations and IT companies.

In attacks on individuals, malicious actors were mostly interested in credentials and personal data (35% and 28%, respectively), as well as payment card data (12%).

Figure 6. Types of data stolen in successful attacks on organizations

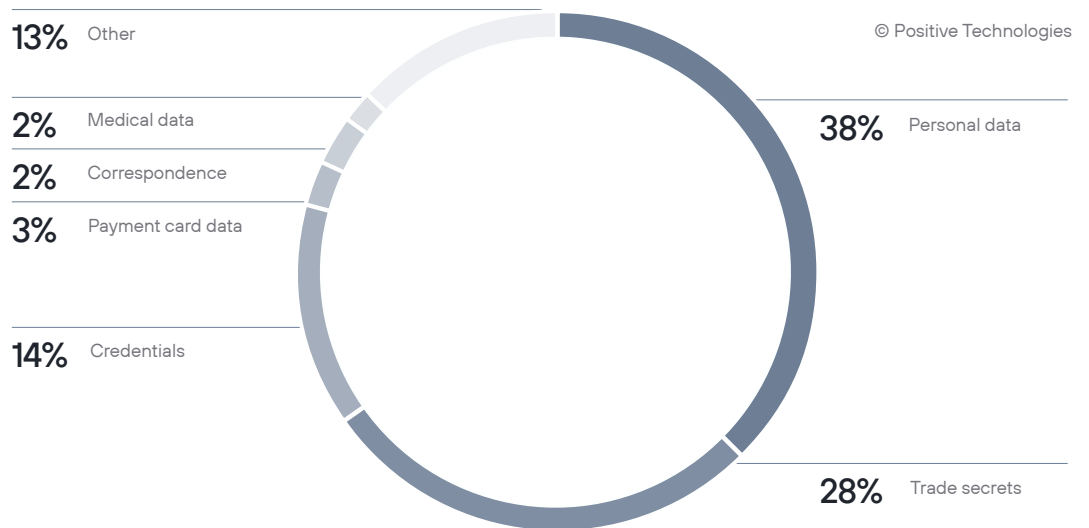
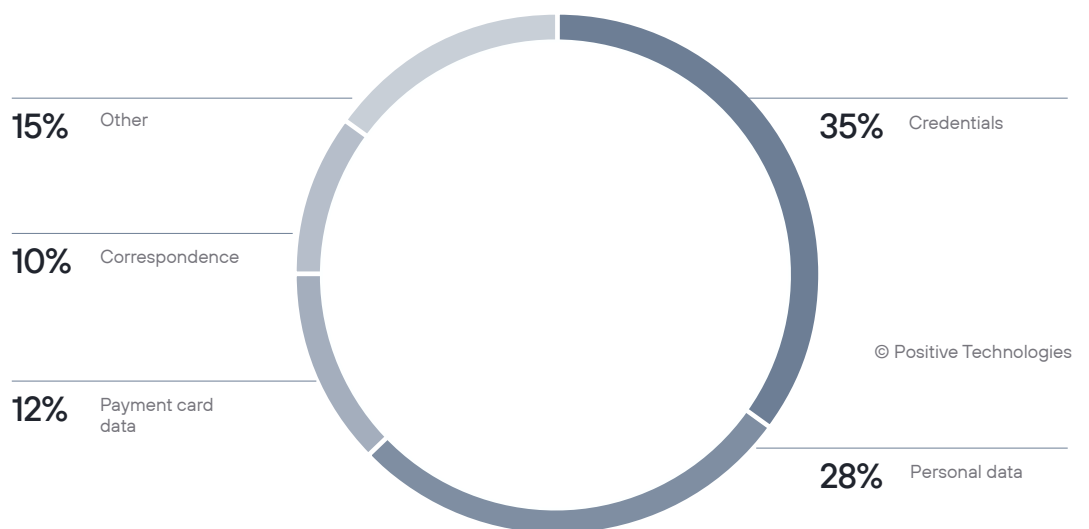


Figure 7. Types of data stolen in successful attacks on individuals



Attackers can openly publish or sell stolen databases and other information on the dark web. For example, in May, a database containing 2.1 billion unique records on customers of a Chinese express delivery service, including personal data and mobile numbers, was put up for sale for \$40,000.

Figure 8. Advertisement on the dark web for the sale of the user database of a Chinese express delivery service

05.04.2023 #1

For Sale: Chinese Express Delivery order data. © Positive Technologies
 Source: <https://www.yicaiglobal.com/news/china-courier-shares-dip-after-alleged-massive-data-breach>

Total records: 2.1billion (unique)
 Format: JSON

Price: \$ 40k
 (This was previously posted on Breach forums. Please note contact information is the same).

Sample records :

```
[ CODE ] { "_source": { "BIG_SOURCE": "WA", "COUNT": "1", "DATA_SOURCE": "115", "DETAIL": "{ \ "nameinfo \
<":1557911268 "," IDENTITY_TYPE ":" mobile "," IDENTITY_VALUE ":" 13148898467 "," LAST_TIME ":" 1557911268
"," MRG_ID ":" 38d42546fdfd","TABLE_SOURCE ":" icpoof_delivery " } }
{ "_source": { "BIG_SOURCE": "WA", "COUNT": "4", "DATA_SOURCE": "115", "DETAIL": "{ \ "nameinfo \": <TAG4
"7","IDENTITY_TYPE ":" mobile "," IDENTITY_VALUE ":" 13607607390 "," LAST_TIME ":" 1605251579 "," MURRG_ID
```

The majority of data offered for sale or distributed for free on the dark web is stolen from Chinese (39% among Asian countries) and Indian (22%) organizations and individuals. Primarily, the data sold is taken from government and financial organizations. In July 2023, an announcement appeared on the dark web about the sale of a database of 30 million users of the Indonesian government service Dukcapil for \$15,000.

Figure 9. Advertisement on the dark web for the sale of the Dukcapil user database

Posted July 21

Selling:
 Dukcapil Indonesia Data leak - 30m Users. © Positive Technologies

Source:
 Elasticsearch
 Source IP: 103.198.120.226

News Article: <https://voi.id/en/technology/294145>

Note: Someone on another forum is advertising the sale of 300m records from this database. However, I have downloaded the data directly and there Elasticsearch server only contains 30m enteries. In his original post he also tasks about merging data from other databases so i do not believe that to be authentic.

Full Sample (100k)
https://anonfiles.com/N9A2h43ez2/dukcapil_indonesia_sample_tar_gz

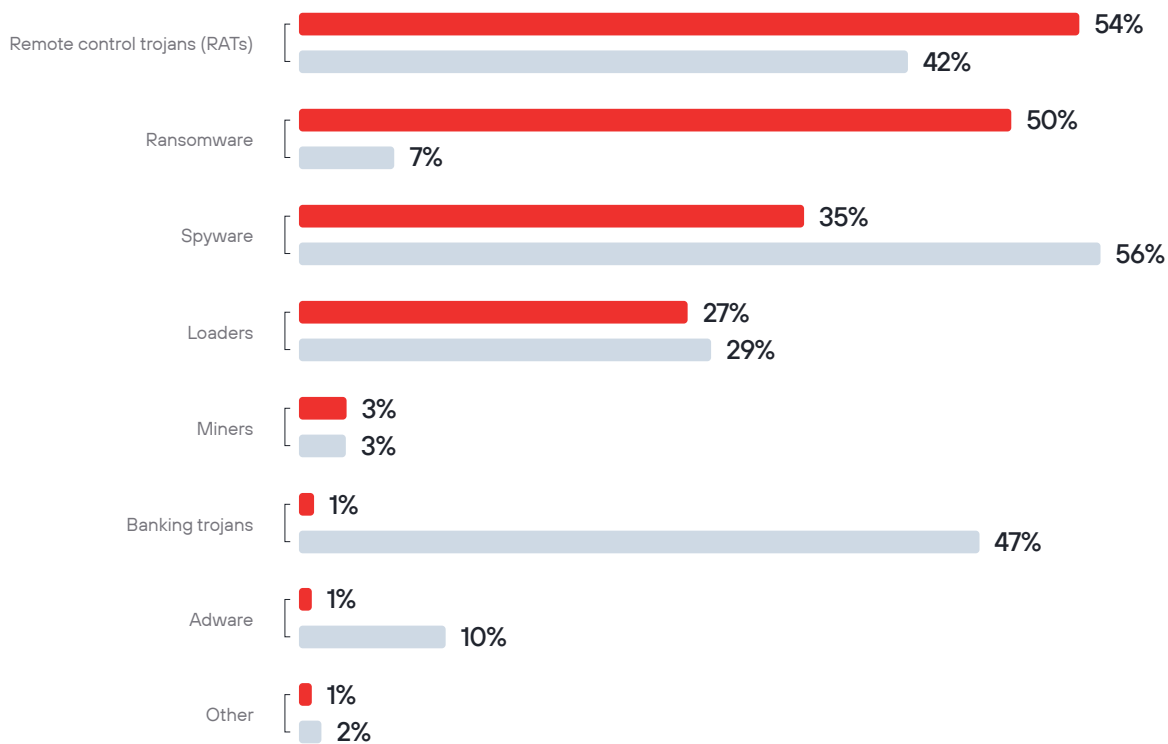
In Asian countries, attacks are carried out by a variety of highly qualified APT (advanced persistent threat) groups. These groups are well organized, experienced and technically skilled. They can carry out attacks for the purposes of cyberespionage, obtaining financial gain, or disrupting enterprise activities. Listed below are some notable APT groups and financially motivated groups that were active in 2022 and 2023 and engaged in cyberespionage in the region:

- **Mustang Panda** (also known as TA416, RedDelta, and Bronze President), is a cyberespionage group discovered in 2017. The criminals have attacked government, religious and non-profit organizations in Vietnam, China, Myanmar, Pakistan, and Mongolia. Mustang Panda operates not only in Asia but also in Africa, Europe, and the U.S.
- **Sharp Panda** has been conducting campaigns in Southeast Asia since 2021. The cyberspies are targeting government organizations in Vietnam, Thailand, and Indonesia.
- **APT32** (also known as OceanLotus, Canvas Cyclone, APT-C-00, and Cobalt Kitty) has been active since at least 2012. The group specializes in cyberespionage and targets government and corporate networks in East and Southeast Asian countries.
- **Dark Pink** (Saaiwc Group) has been active since 2021. The cybercriminals steal documents from military, government, non-profit, and religious organizations in Southeast and Pacific Asia. They operate covertly and select their targets carefully.
- **BlueHornet** (also known as AgainstTheWest and APT49) attacks government organizations in China, North Korea, Iran, and Russia as well as APT groups based in these countries. Blue Hornet compromised and leaked data from Kryptonite Panda and Lazarus Group.
- **Transparent Tribe** (also known as APT36, Copper Fieldstone, Mythic Leopard, and ProjectM) is a Pakistani group which has been attacking Indian governmental, military, and research organizations, as well as their employees, since 2013. Since 2022, the cybercriminals have additionally targeted educational institutions and students on the Indian subcontinent.
- **Billbug** (also known as Lotus Blossom and Thrip) has existed since 2009. These cyberspies target government and industrial organizations in Asia. In their attacks, the criminals use both legal dual-use software and specialized backdoors.
- **Charming Kitten** (also known as APT35, Phosphorus, TA453, and Ajax Security Team) specializes in cyberespionage and stealing data of organizations and individuals connected to Iran's geopolitical interests. The cybercriminals target victims in the Middle East, Asia, Europe, and the USA.
- **Desorden** (also known as chaoscc) is a financially motivated group which has been attacking Indian and Malaysian companies in various sectors of the economy since 2021. The group steals data from high-revenue enterprises to get larger ransoms. In the summer of 2022, Desorden launched a regional campaign focusing on Thai organizations.

Malware

Remote administration tools (RATs) have become the most common type of malware in attacks on organizations (54% of attacks using malware). Ransomware ranked second, being used in half of the malware attacks. Nearly every third attack involved the use of spyware.

Figure 10. Types of malware (percentage of successful malware attacks)



© Positive Technologies ■ Organizations ■ Individuals

Individuals' devices were most frequently infected with malware designed to steal data: spyware (56%), banking trojans (47%), and RATs (42%).

The distribution of malware in attacks on organizations primarily occurs through the compromise of computers, servers, and network equipment (44%), and through email (41%). Malware most often infiltrates regular users' devices through infected websites (34%), email (16%), social networks (16%), and instant messengers (11%).

Figure 11. Malware distribution methods in successful attacks on organizations

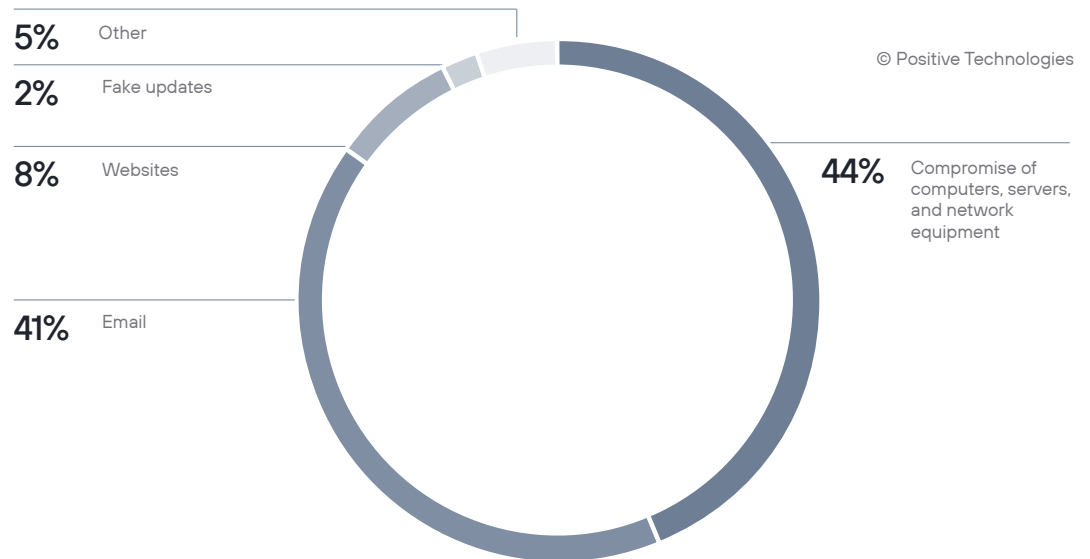
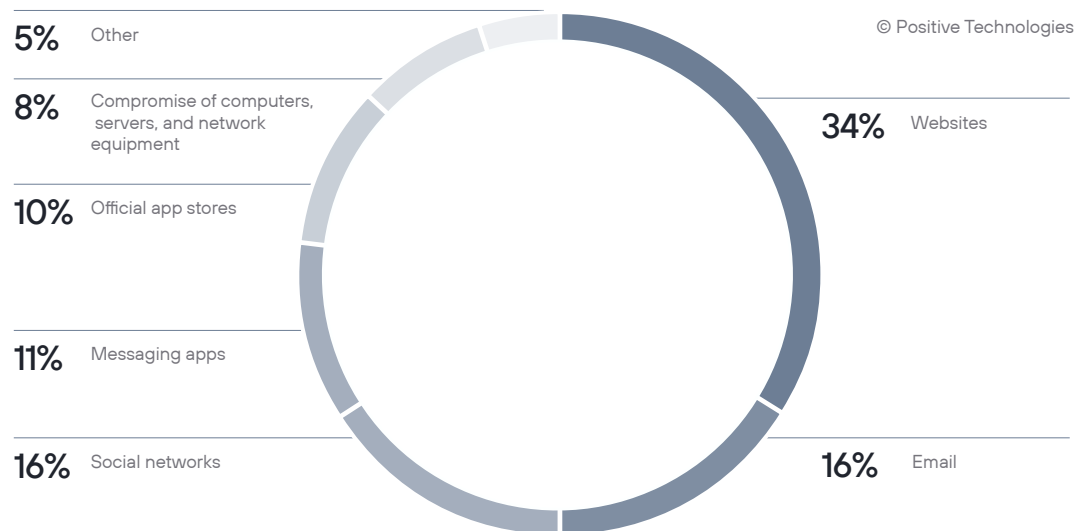


Figure 12. Malware distribution methods in successful attacks on individuals

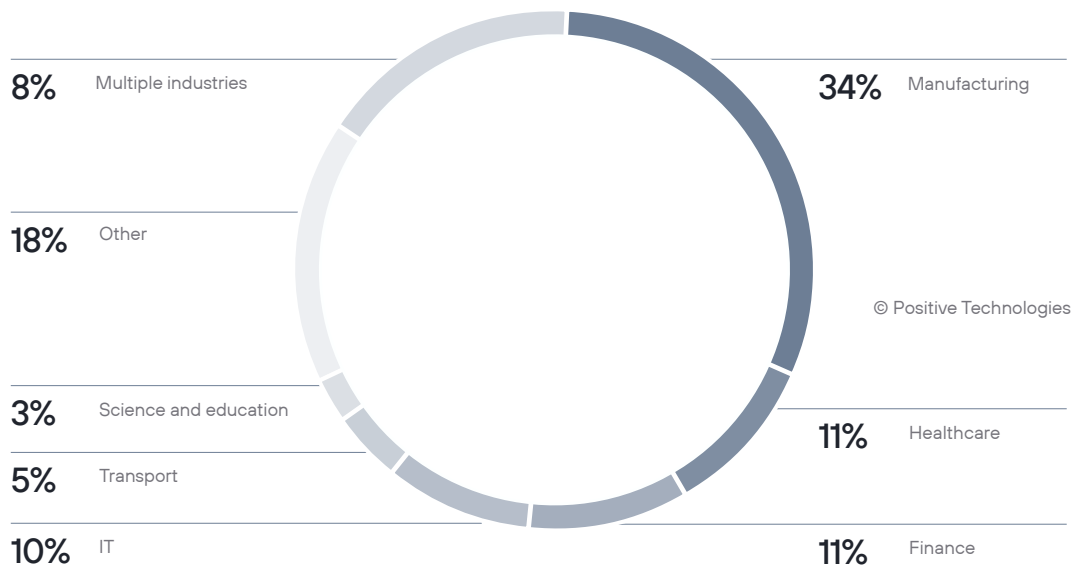


Ransomware

As in the rest of the world, the region is experiencing a surge in ransomware activity. For example, according to the Indian Computer Emergency Response Team (CERT-In), the number of ransomware attacks in India increased by 53% in 2022. A recent trend in these attacks is that attackers prefer not to encrypt infrastructure but rather demand a ransom in exchange for not spreading compromised information. This is a global trend that we mentioned in our 2023 forecasts. Meanwhile, the average ransom amount demanded remains high, in millions of dollars. For example, in India in 2022, the average ransom for decrypting data and restoring access to infrastructure was \$1.2 million. Not all companies are prepared for ransomware attacks: according to a survey conducted by Corinium Intelligence in Southeast Asian countries, 45% of respondents believe that the damage to their company in the event of a ransomware attack would range from moderate to significant, with only 55% of respondents confident in the reliability of their backup and recovery measures.

The main victims of ransomware attacks are industrial enterprises, accounting for 34% of successful attacks. Extortionists also target healthcare institutions, financial organizations, and IT companies.

Figure 13. Distribution of ransomware incidents by industry



In November 2022, the All India Institute of Medical Sciences (AIIMS) in New Delhi experienced [a ransomware attack](#) that resulted in the suspension of medical services. The attack affected various digital services of the hospital, including billing, reporting, lab testing, emergency services, and the appointment system. The IT systems responsible for the functioning of the healthcare services had to be shut down, and all operations were switched to manual mode. It took about two weeks to restore the IT systems. Furthermore, the attackers [stole](#) patient data, including medical records, donor information, hospitalization records, and vaccination records, etc. The hospital administration refused to pay the ransom, and the extortionists published this data on the dark web. The hospital managed to prevent another attack in June 2023, which did not affect patient services.

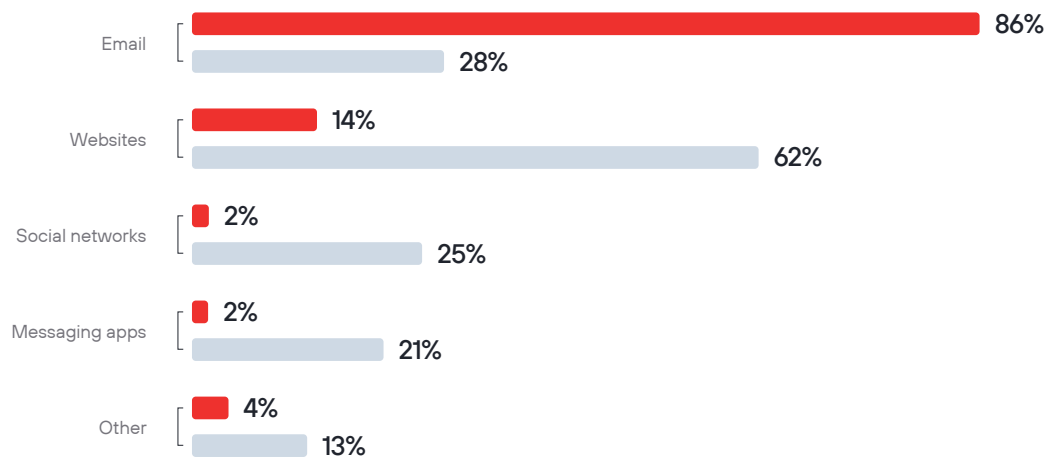
In early April 2023, Fullerton India, a major credit institution in India, fell victim to a LockBit 3.0 [ransomware attack](#). As a result of the attack, more than 600 GB of data was compromised, including customers' personal data, financial information, bank account numbers, and loan agreement details. The extortionists demanded a ransom of 240 million rupees (about \$3 million), but the company refused to negotiate, and the criminals published the stolen data on the dark web.

The primary method of spreading ransomware (63% of successful attacks) is through email. In 32% of cases, vulnerabilities in organizations' publicly accessible resources are exploited.

Social engineering

Social engineering is the primary vector for infiltrating organizations' infrastructures and is used in 40% of successful attacks. The threat of social engineering attacks is high throughout the region. For example, Vietnam's Ministry of Information and Communications [reported](#) that the number of attacks in the country increased by 44% in the first 11 months of 2022 compared to the same period in 2021. Phishing attacks accounted for 35% of the total number of incidents. The number of phishing attacks in Singapore in 2022 [more than doubled](#) compared to the previous year. According to [IBM's report](#), email attachments are the main vector for distributing malware in the Asia-Pacific region. IBM experts also [note](#) that the average damage from a phishing attack is \$4.76 million, second only to attacks from internal intruders by cost.

Figure 14. Social engineering channels



© Positive Technologies

■ Organizations ■ Individuals

Social engineering is used by inexperienced cybercriminals who buy ready-made tools for phishing campaigns, as well as by extortionists and APT groups. The most common vector for phishing attacks against organizations is email campaigns, but attackers can also create fake websites to steal credentials or distribute malware. Most often, the websites of banks and payment services are faked, to steal money or authentication data.

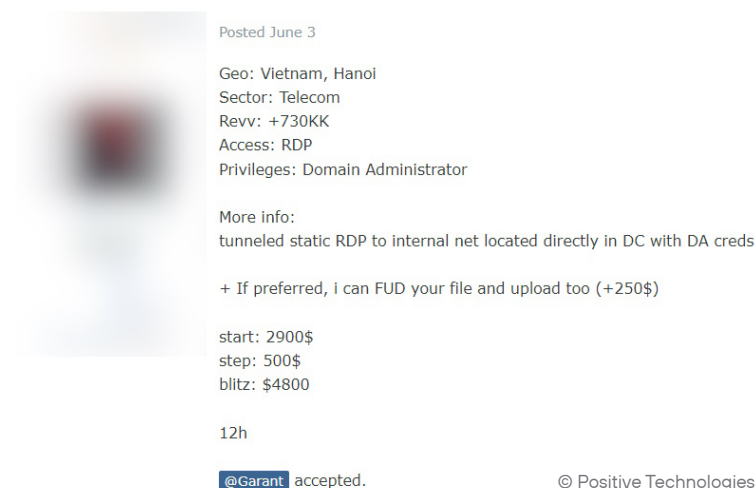
According to a KnowBe4 [report](#), about 30% of employees in Asia find it difficult to recognize a phishing email, which means that in the event of an attack, one in three employees could open a malicious attachment, click on a malicious link, or give the attacker their credentials. With the development of AI tools, this problem is becoming even more serious, as generative models allow criminals to create highly convincing emails in various languages and make it easier for international groups to carry out attacks.

Development of cybercrime forums

On shadow forums, cybercriminals trade and exchange malware and stolen data, and offer various illicit services. Here, malicious actors can acquire access to the networks of organizations that interest them. In the countries of the region, the most common ads are for the sale of access to companies in China, Thailand, and India. These are mainly government organizations, IT companies and service sector companies.

The cost of access depends on the size of the organization and the privileges of the account. Access to a network with the rights of an ordinary user or to a small company can cost \$100–200, while domain administrator privileges cost upwards of \$500. For example, one of the most expensive offers we found was access with domain administrator privileges to the network of a Chinese manufacturer of photovoltaic modules, priced at \$20,000. For access to the infrastructure of a Vietnamese telecommunications company, the attackers expected to receive up to \$4,800.

Figure 15. Advertisement for the sale of access to a Vietnamese telecoms company



Posted June 3

Geo: Vietnam, Hanoi
Sector: Telecom
Revv: +730KK
Access: RDP
Privileges: Domain Administrator

More info:
tunneled static RDP to internal net located directly in DC with DA creds

+ If preferred, I can FUD your file and upload too (+250\$)

start: 2900\$
step: 500\$
blitz: \$4800

12h

@Garant accepted.

© Positive Technologies

Legislative issues

Unlike other regions, such as Europe or Africa, in Asia (with the exception of individual initiatives of the ASEAN countries) there is no push to create uniform cybersecurity standards across the region. Despite having the same goals, each country pursues its own approach in accordance with its national interests and specific circumstances.

Without delving into the details of information security legislation in each country, we will attempt to highlight the main problems requiring attention at the national level.

■ Outdated legislation

Technology evolves rapidly, and legislation may struggle to keep up with the constant changes, inadequately addressing today's threats. The issue of outdated legislation is pressing in many countries across the region. Some of the countries lack unified or dedicated cybersecurity legislation.

For instance, in India, the main problem with cybersecurity regulation is [outdated](#) and non-transparent laws. India does not have unified cybersecurity legislation; instead, it relies on an information technology law and a number of industry-specific regulations to maintain cybersecurity standards. The legal foundation for protecting critical information infrastructure is equally loose. To address these challenges, India needs up-to-date comprehensive laws, a clear legal framework for cybersecurity, and an open dialogue with cybersecurity experts. The government is currently [developing](#) a new national cybersecurity strategy and considering updating its IT laws.

Malaysia also lacks unified or specialized legislation in the field of cybersecurity, though the Malaysian government has announced its intention to introduce a dedicated cybersecurity law to regulate issues in this area and fill gaps in the existing legal framework. The absence of specialized legislation means that cybersecurity in Malaysia is regulated by a variety of laws including the Communications and Multimedia Act of 1998 and the Personal Data Protection Act of 2010. These laws only affect various aspects of cybersecurity and are by no means exhaustive: they are outdated and lag behind the rapid development of modern technologies. The Malaysian Cybersecurity Bill aims to establish a comprehensive legal framework for regulating cybersecurity and safeguarding Malaysian citizens from cybersecurity threats.

■ Unclear or fragmented requirements

Many organizations face challenges in understanding and implementing the necessary security measures due to unclear requirements and fragmented data privacy and cybersecurity legislation.

In India, a complex multi-agency system has emerged in the field of cybersecurity, with several ministries, departments, and agencies performing separate critical functions. For instance, the Ministry of Electronics and Information Technology (MeitY) is in charge of policies related to IT, electronics, and the Internet, and has established the national cyberincident response center CERT-In. The Information Technology Act imposes security obligations on organizations handling personal data. These rules comply with the international ISO/IEC 27001 standard for information security management, with corporations subject to audits by independent government-approved auditors at least once a year or when there are significant updates to processes and computer resources. Industry regulators and central agencies also prescribe security measures. The Reserve Bank of India sets standards for banks, requiring them to establish mechanisms for handling and reporting incidents and organize continuous monitoring of systems and customer data protection. It also requires banks to comply with ISO/IEC 27001 and ISO/IEC 27002 standards. The confusing range of requirements and many regulatory bodies make it difficult to understand which security measures should be taken and can diminish their effectiveness.

Thailand's cybersecurity legislation has also been criticized for its lack of clear, precise guidance. Given the severity of sanctions for non-compliance, this is a serious issue for organizations.

■ Lack of unified cybersecurity standards in the region

Each country in Asia has its own set of cybersecurity laws aimed at protecting national security and developing information technology and communications. This approach can hinder international cooperation between countries, making it more difficult to share cyberthreat intelligence, adopt best practices, abandon outdated practices, and encourage effective collaboration between law enforcement agencies.

Meanwhile, it's worth mentioning that the ASEAN countries are showing a shared interest in creating a reliable cybersecurity system. The main goal is to protect Internet users, ensure the stability of digital systems, and support economic growth. The countries have developed a joint [cybersecurity strategy](#), a common data protection framework, and are also working on creating a unified ASEAN CERT. However, despite such promising cooperation, there are currently no guarantees that it will lead to a unified legislative framework in Southeast Asia.

In 2021, the ASEAN countries adopted the [ASEAN Data Management Framework](#) (DMF, a framework similar to European GDPR) and the [Model Contractual Clauses](#) (MCC). These were developed to coordinate data management practices and cross-border data transfer standards throughout the region. These documents are advisory in nature and do not require the participants to amend their existing data protection laws. However, the participants are expected to encourage businesses to comply with DMF and MCC in their respective jurisdictions. For example, the Personal Data Protection of Singapore issued additional recommendations for organizations in Singapore regarding the use of MCC.

■ Excessively strict requirements and sanctions

In 2022, the Indian government introduced new requirements for the cyberincident reporting mechanism. Organizations across India are now required to report cyberincidents to CERT-In within just six hours from the moment of discovery. Cybersecurity experts [agree](#) that such a timeframe is insufficient for conducting all the necessary preliminary investigations required for reporting. Previously, it was required to report a cyberincident «within a reasonable time» after its discovery. Now, the window for notification is significantly shorter than in the EU or the US. For instance, the EU's General Data Protection Regulation (GDPR) requires that security breaches of personal data be reported within 72 hours, which is sufficient for a detailed analysis of the incident. Organizations that fail to comply with the new CERT-In notification requirements may face criminal charges and large fines for violating the law.

In the interests of national security, some countries, such as Vietnam and China, have adopted laws to localize the storage and processing of data. Regulators believe that this approach enhances security but leads to a decrease in economic competitiveness. For example, Vietnam's cybersecurity law has been [criticized](#) for its potential impact on foreign investment and businesses operating in the country. China's legislation is also known for its harsh penalties for cybersecurity and privacy violations—such severe fines pose a significant risk to businesses. Data is a vital part of the digital economy, and data localization policies do not promote its growth. Instead, advanced technologies should be used to support secure cross-border data exchanges based on agreed standards.

In the long run, excessively strict requirements and sanctions may not have the intended effect of enhancing cybersecurity; instead, they can lead to the suppression of information about vulnerabilities and incidents, and can negatively impact business development in the country, especially at the international level. When drafting legislation, it is crucial to foster dialog between the government, businesses, and cybersecurity experts.

Conclusions and recommendations

The number of cyberattacks on Asian countries is increasing every year, making it imperative for both governments and organizations to bolster their defenses. To achieve this, a comprehensive cybersecurity strategy must be developed, with adequate resources allocated for its implementation. A good starting point for cybersecurity professionals is to compare their own cybersecurity systems with global standards.

Effective regulation and cooperation at the government level are of paramount importance. Transnational initiatives, such as cybersecurity cooperation within the Association of Southeast Asian Nations (ASEAN), and updates to legislation in this region's countries can contribute to this.

Recommendations for governments

Update and regularly review cybersecurity and personal data protection legislation

Some countries in the region do not have any dedicated cybersecurity legislation; existing laws are outdated and need to be updated, cybersecurity requirements are not coordinated, and it is difficult for organizations to understand how to properly implement the necessary measures. These issues must be addressed to create effective cybersecurity regulations that can realistically be met. Legislation must be regularly updated to keep pace with the latest cyberthreats and technological advancements. It should also facilitate effective coordination between different law enforcement and security agencies. However, it's important to remember that excessive tightening of requirements and sanctions may not contribute to strengthened security in the long term.

Countries in the region should consider agreeing on shared cybersecurity standards for more effective collaboration or establish common mechanisms for exchanging information on and fighting against international cyberthreats.

Protect critical information infrastructure

Governments should identify non-tolerable events at the industry and national levels. This approach helps to effectively allocate resources to ensure the protection of the most critical systems. Priority should be given to the infrastructure of sectors such as government, telecommunications, and finance, as well as other industries vital to the economy and national security, such as high-tech manufacturing, pharmaceuticals, and agriculture. The speed of digital transformation in the country and the maturity level of information security should also be taken into account.

Improve mechanisms for interacting with national and industry cyberincident response centers

In Asian countries there are already national cyberincident response centers, which monitor threats and help organizations recover from major cyberattacks. However, the mechanisms for reporting incidents may be unclear for security professionals, or the requirements may cause objections and disputes among them. It is necessary to develop clear and transparent mechanisms for reporting cyberincidents in organizations, taking into account the views of experts and the information security community. Improved information sharing between organizations and cybersecurity centers can help prevent attacks and respond to new threats in a timely manner.

Responding to cyberthreats must be integrated into the overall strategy for protecting and restoring critical national infrastructure.

Raise awareness and promote education in cybersecurity matters

Governments should invest in public awareness campaigns about current threats and how to protect against them. In this region, as in the rest of the world, there is a shortage of qualified cybersecurity professionals. Therefore, promoting this field and related professions and supporting educational programs in institutions should be a government priority.

Cooperate internationally

Cybercrime has long transcended the borders of individual states, making it crucial for countries to cooperate with international partners in combating cyberthreats. By sharing information, resources, and expertise, countries can collectively strengthen their defenses and mitigate the risks posed by cybercriminals across jurisdictions. National cybersecurity strategies should include objectives for developing international relations in the field of cybersecurity.

Recommendations for businesses

Identify non-tolerable events and critical assets

To ensure the cyberresilience of a company, it is necessary first of all to analyze the main risks and draw up a list of non-tolerable events that could cause significant damage to its activities. This step will help identify critical assets and focus on protecting the most valuable resources. A strategy should be developed to prevent non-tolerable events, including the necessary security measures and monitoring of network activity using modern security tools.

Monitor incidents and respond to cyberthreats

Incident monitoring and detection systems are needed to respond to potential threats and attacks in a timely manner. For this purpose, we recommend using SIEM systems that collect and analyze information about security events from various sources in real time. Together with XDR (extended threat detection and response) and NTA (network traffic analysis) solutions, this will help detect attacks in the early stages and ensure swift responses, reducing risks for the organization.

Evaluate cybersecurity effectiveness

The effectiveness of adopted cybersecurity measures should be regularly tested to assess the performance of the strategy and defenses. We recommend paying special attention to verification of events that are non-tolerable for the organization.

It is also worth participating in bug bounty programs so that external security researchers can find new vulnerabilities. This will help detect and eliminate vulnerabilities before attackers can exploit them.

Train employees and develop information security specialists

It is essential to educate employees about cybersecurity and conduct training sessions to increase awareness of current cyberthreats and protect against social engineering techniques.

To effectively combat cyberthreats, organizations should invest in the development of their cybersecurity experts. Regular training and certification of employees in the field of cybersecurity will enhance their skills and knowledge, boosting the company with expert support in preventing and responding to cyberattacks. One of the most effective ways to do this is to participate in cyberexercises on dedicated platforms, where information security specialists can practice recognizing attack techniques and countering them.

About the research

The data and findings presented in this report are based on Positive Technologies own expertise, as well as analysis of publicly available resources, including government and international publications, research papers, and industry reports.

We estimate that most cyberattacks are not made public due to reputational risks. As a consequence, even companies specializing in incident investigation and analysis of hacker activity are unable to quantify the precise number of threats. This research aims to draw the attention of companies and individuals who care about the state of information security to the key motives and methods of cyberattacks, and to highlight the main trends in the changing cyberthreat landscape.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies [glossary](#).