# How APT groups operate in Southeast Asia

Positive Technologies ⁝⁝ 7/24/2024

This report presents the results of research on the tactics and techniques of 20 APT groups that attacked government and commercial organizations in Southeast Asian countries from January 2020 to April 2024. You can find the list of APT groups at the end of the report. It's not exhaustive as it is based only on data from open reliable sources and the expertise of Positive Technologies.

The tactics and techniques of these groups are described in terms of the MITRE ATT&CK Matrix for Enterprise (version 14.1). The report provides links to detailed descriptions of the mentioned techniques. Additionally, examples of the use of some sub-techniques can be found in the report, with links to them in brackets represented by identifiers (for example, T1566.001).

The appendix to the report contains a heat map of tactics and techniques. The geography of the heat map is limited to APT attacks on the member countries of the Association of Southeast Asian Nations (ASEAN): Brunei, Vietnam, Indonesia, Cambodia, Laos, Malaysia, Myanmar, Thailand, Singapore, the Philippines.

The study's purpose is to draw the attention of companies interested in the current state of information security to the most relevant tactics and techniques of APT attacks on organizations in Southeast Asian countries. The terms used in the report are explained in the glossary on the Positive Technologies website.

## Summary

- Top 5 countries in Southeast Asia by the number of APT groups attacking them: the Philippines (85%), Vietnam (85%), Thailand (70%), Malaysia (70%), and Indonesia (60%). The activity of cybercriminals is largely driven by territorial disputes in the South China Sea between ASEAN countries and China, as well as the US-China rivalry for dominance in the region.
- All APT groups operating in Southeast Asia target government organizations. Telecommunications companies and military-industrial entities are also under attack. They are targeted by 60% and 50% of APT groups, respectively.
- Three-quarters of the APT groups studied begin cyberattacks with phishing emails, and 50% of the APT groups exploit vulnerabilities in internet-facing systems, such as Microsoft Exchange servers.
- To avoid detection, all APT groups strive to use legitimate tools already present in the compromised system (living off the land tools). This allows them to disguise their actions as those of IT personnel.
- 70% of APT groups use Cobalt Strike in their attacks—commercial software that was created as a pentesting tool but is now widely exploited by attackers due to its extensive functionality.
- Every second APT group uses the well-known PlugX Trojan in their attacks. Among other popular malware are the ShadowPad Trojan and the China Chopper web shell, used by 35% of APT groups. These malware programs are characteristic of cybercriminal groups that various researchers consider Chinese-speaking.

## Digital transformation in Southeast Asia

Southeast Asia is an important territory both in terms of the global economy and geopolitics. The Association of Southeast Asian Nations (ASEAN) plays the role of an institution that supports political stability and security in the region. It includes ten countries: Brunei, Vietnam, Indonesia, Cambodia, Laos, Malaysia, Myanmar, Thailand, Singapore, and the Philippines. It is one of the largest region-specific organizations in the world: the total area of member countries is 4.5 million km², and the population, according to 2024 data, exceeds 683 million people. Today, the combined nominal GDP of ASEAN is estimated at $4.16 trillion USD, with Indonesia, Thailand, and Singapore generating the main share.

The COVID-19 pandemic had a serious impact on the pace of economic development in Southeast Asia. In 2020, for the first time since the Asian financial crisis of 1997–1998, the average GDP growth rate in ASEAN countries was negative. During the lockdown period, the majority of the population lacked access to digital technologies; this created serious problems. According to ASEAN data for 2020, only 53% of the region's rural children and adolescents had Internet access at home, and in Cambodia, Laos, and Myanmar, less than 5% of homes were connected to broadband.

The crisis became a catalyst for technological and digital transformation in the region. At the 37th ASEAN Summit in 2020, leaders adopted the ASEAN Comprehensive Recovery Framework. In addition to plans to restore key sectors of the economy and support vulnerable groups affected by the pandemic, the program addresses the need to accelerate digital transformation. The main challenges faced by Southeast Asian countries on the path to digitalization are the gap between urban and rural areas, the high cost of the internet, and the lack of a sufficient regulatory framework. ASEAN has developed a number of programs, strategies, and initiatives aimed at expanding broadband and mobile internet coverage, training the population in necessary digital skills, and creating safe digital services, including e-government services.

Today, digital transformation in Southeast Asia is in full swing. Singapore, Malaysia, Thailand, Vietnam, the Philippines, and Indonesia have become the main drivers behind the implementation of new technologies in the region. In 2023, according to the e-Conomy SEA 2023 report, the GMVGross merchandise value (GMV) is the total value of all goods sold through an e-commerce platform over a certain period of time. in Southeast Asia was estimated at $218 billion USD. For comparison, in 2021, the GMV was $161 billion USD. It is expected that by 2030 its value will approach the $1 trillion USD mark. Revenues from the digital economy in Southeast Asia in 2023 are estimated at $100 billion USD, 1.7 times more than in 2021. The main contributors to this growth are e-commerce, tourism, and media. As of early 2024, the rate of Internet penetration in the region exceeded 70% in all countries except Laos, Myanmar, and East Timor.

## Cybersecurity in Southeast Asian countries

For the residents of Southeast Asia, especially young people, digital technologies have transformed everyday life—the way they shop, use financial services, and interact with the government. The rapid growth of the digital economy in Southeast Asia opens up a range of opportunities for businesses and governments. At the same time, as the region's digital potential grows, so does the number of cyberattacks. We previously reported on current cyberthreats to Asian countries, including Southeast Asia, in one of our reports.

The level of cybermaturity in Southeast Asia varies greatly between countries, depending directly on the political and economic development of each state. For example, Myanmar, which has long been subject to political isolation and military conflicts, today occupies one of the lowest places both in terms of digital economy development and the cybersecurity index. Meanwhile, the strongest economic players in the region—Malaysia and Singapore—have achieved the highest cybersecurity indices.

Malaysia has the National Cyber Security Agency (NACSA) and the CyberSecurity Malaysia (CSM) agency. Since 2008, the CSM has been conducting X-Maya cybersecurity exercises. A regulatory framework for cybersecurity is being developed. In June 2023, the CSM released a development roadmap for the next five years—The Cyber Security Technology Roadmap: Cybersecurity Malaysia Framework 2024–2029. In April 2024, a new cybersecurity bill was passed, aimed at strengthening the cyber resilience of the country's critical information infrastructure.

Singapore has its own Cyber Security Agency (CSA). It closely cooperates with ASEAN member states on the creation of a regional cybersecurity incident response center (CERT). In September 2023, the fifth cyberexercises, Exercise Cyber Star (XCS23), took place in Singapore, during which various attack scenarios were practiced, including attacks on critical infrastructure. To strengthen regional cooperation, in July 2023, the headquarters of the Center of Excellence in Cybersecurity and Information (ACICE) opened at the Changi Naval Base in Singapore, one of its key tasks being providing early warnings about cyberthreats.

The level of cybercrime in the region is directly influenced by current geopolitical issues. Rivalry between states inevitably manifests itself in cyberspace, leading to complex, carefully planned targeted cyberattacks. Such attacks are called APT attacks. They are carried out by groups of professional cybercriminals known as APT groups. Having infiltrated a target organization's network, an APT group can maintain its presence there for months or even years, gathering intelligence. Successful APT attacks can impact the country's economy, critical information infrastructure, and national security.

## Leading countries in terms of the number of APT-groups targeting them

The top five most attacked countries by APT groups are the Philippines (85%), Vietnam (85%), Thailand (70%), Malaysia (70%), and Indonesia (60%). To a large extent, cybercriminal activity here is driven by territorial disputes in the South China Sea between ASEAN members and China.

**Historical background.** Four ASEAN states (the Philippines, Malaysia, Vietnam, Brunei), China, and Taiwan all claim territories in the South China Sea—the Spratly Islands, the Paracel Islands, and an exclusive economic zone 200 nautical miles wide. The disputed territories are rich in resources, including oil, gas, and minerals.

Until the end of World War II, the islands were under Japanese control. In 1951, under the terms of the San Francisco Peace Treaty, Japan renounced these territories, but the document did not specify the new owner. Since then, there have been repeated clashes between the countries that claim the islands.

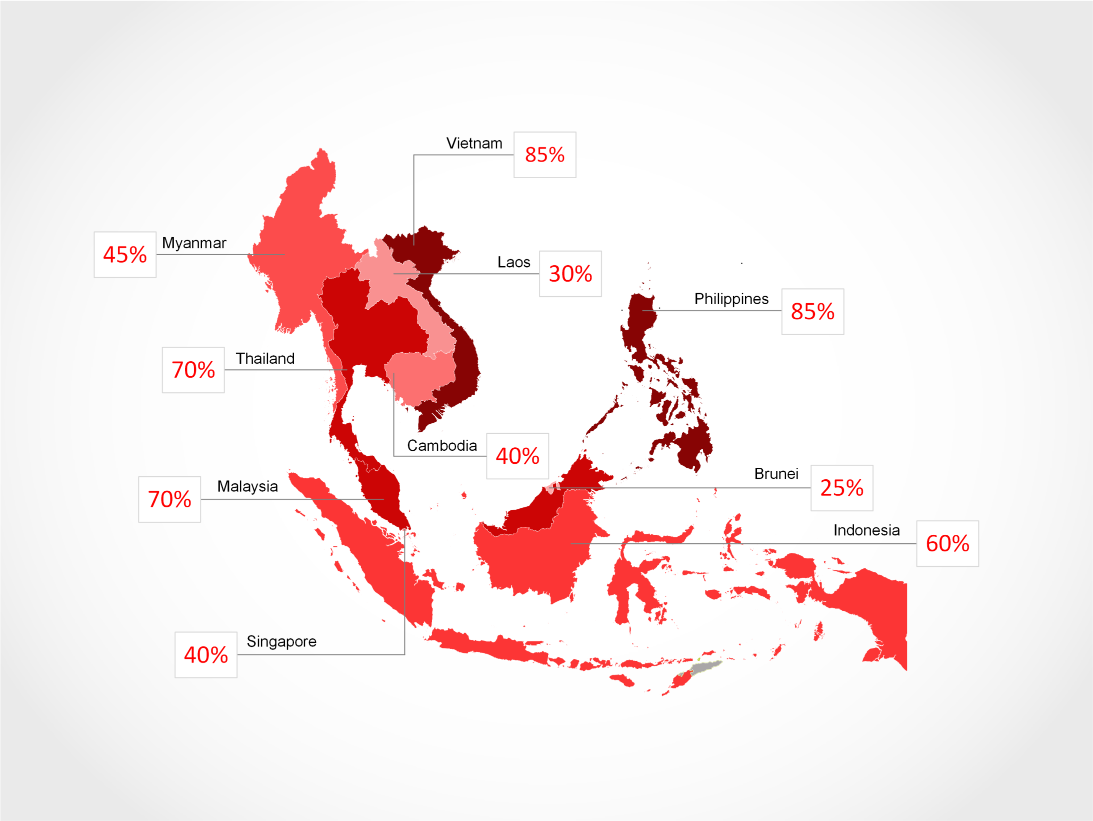


Figure 1. Geography of cybercriminal activities (share of APT groups attacking the region)

According to some researchers, cyberattacks on the Philippine military-industrial complex and government organizations have intensified since a new president came to power in 2022 and entered into a strong alliance with the United States. The attacks are allegedly from China. Some of the cyberattacks were timed to coincide with major US-Philippine military exercises near the disputed Scarborough Shoal. In August 2023, amid rising tensions between the Philippines and China, the APT group Mustang Panda carried out cyberattacks on organizations in the South Pacific, resulting in the compromise of a government institution in the Philippines. In February of this year, cybercriminals tried and failed to hack the websites and email of the president of the Philippines and various government institutions, one of which deals with maritime security. In June 2023, the National Defense College of the Philippines announced that the state-sponsored operations pose a serious threat to commercial and government institutions. The country recently published an updated national security policy to respond to cyberthreats, and the military announced the creation of a cybercommand to ensure the security and protection of military systems from cyberattacks.

Vietnam shares the first place with the Philippines in the number of APT groups attacking the country: it is attacked by 85% of the groups we considered. Among the most active APT groups here are APT41, Mustang Panda, Sharp Panda, Dark Pink, and ToddyCat.

More than half (60%) of the APT groups studied attack Indonesia. Here, as in other Southeast Asian countries, the transition to a digital economy is underway, with e-commerce and fintech actively developing. However, the population's digital literacy remains at a low level, and Indonesia's spending on cybersecurity as a percentage of GDP (0.02%) is the lowest in Southeast Asia. The state is located at the intersection of many trade routes between two continents and has large reserves of natural resources, making it attractive to criminals. Cybercriminal interest in Indonesia is primarily directed at industrial enterprises: construction, mining, aviation. Criminals seek to exploit vulnerabilities in such infrastructure for various purposes, including causing economic damage and stealing intellectual property.

## The most attacked industries

All the APT groups operating in Southeast Asia that we studied attack government institutions, and half of the APT groups target military-industrial entities.

As shown by the results of a survey conducted by the Singaporean research center ISEAS—Yusof Ishak Institute, some ASEAN member states, particularly Vietnam and the Philippines, tend to support the US, while others, such as Myanmar and Indonesia, prefer to trade with China and rely on its investments. Today, China is the main trade partner for half of the ASEAN countries (Indonesia, Malaysia, Myanmar, Singapore, and Thailand) and is seeking to further expand its influence in the region, including in cyberspace. In the fall of 2023, Palo Alto Networks' Unit 42 incident response team discovered the infrastructure of Chinese APT groups disguised as cloud backup services. The researchers found that at least 24 Cambodian government organizations regularly connected to this infrastructure. Experts believe that these organizations were victims of a long-term cyberespionage campaign by China, with which Cambodia has strong diplomatic and economic ties.

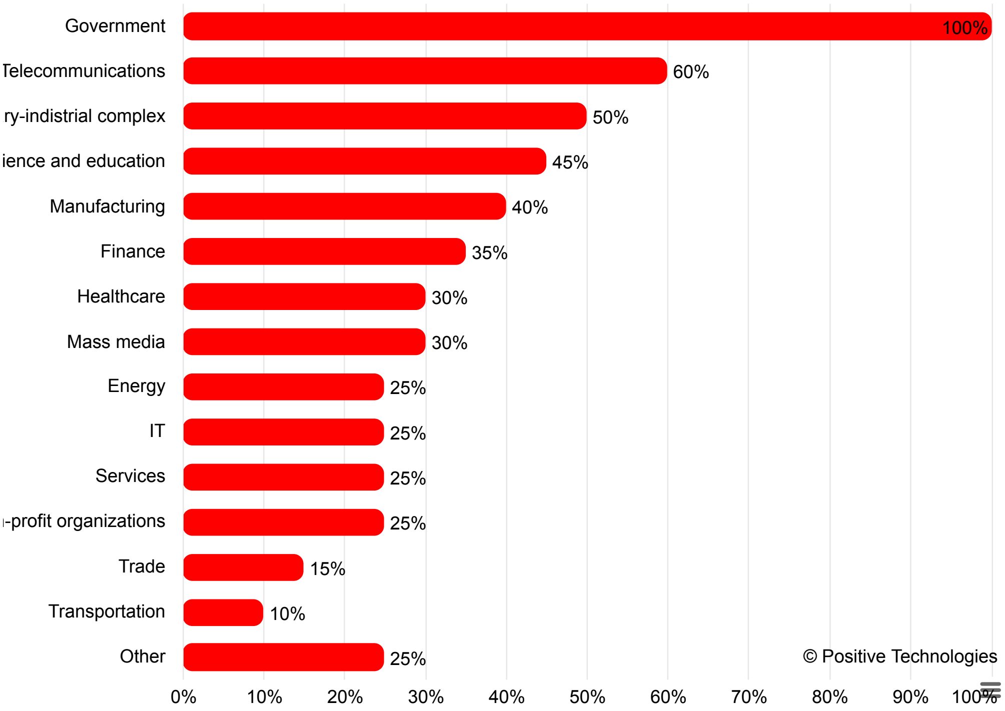


Figure 2. Industries attacked (share of APT groups)

APT groups have been targeting telecommunications service providers around the world for years, and Southeast Asia is no exception. Telecommunications companies attract attackers because they manage the internet, phone networks, and satellite systems. With access to a telecom operator, cybercriminals can destabilize the situation during geopolitical conflicts. Additionally, cyberspies hack providers to access their clients' confidential information for use in further attacks. In Southeast Asia, 60% of active APT groups attack this sector.

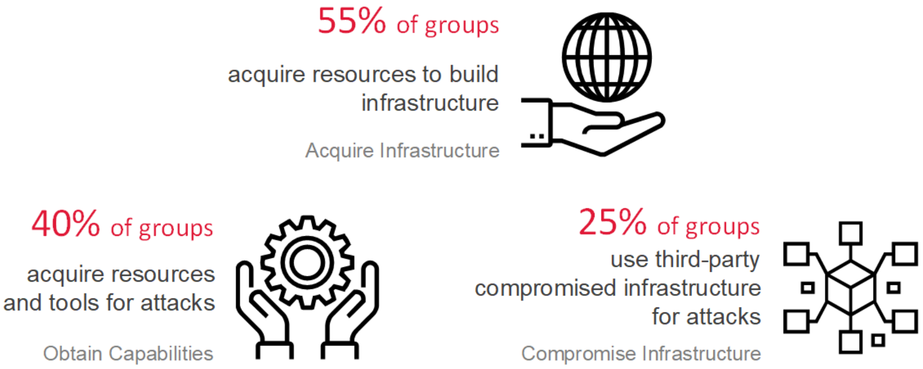
Telecommunications also attract attention due to the spread of 5G technology in the region. According to Ericsson's forecast, the number of 5G subscribers in Southeast Asia and Oceania will grow from 57 million in 2023 to 548 million by 2029. The adoption of new technology in Southeast Asia is outpacing the development of cybersecurity, which means the rapid deployment of 5G telecommunications could lead to an increase in cyberattacks on this sector. Due to concerns about cyberespionage from other countries, some states, like Vietnam, are refusing to use foreign network equipment and developing their own 5G infrastructure using domestic electronics.

## How APT groups operate at different stages of an attack

APT attacks pose a serious security threat not only to individual organizations but also to entire states, especially when initiated by professional cybercriminal groups. In this section, we'll take a closer look at the working processes of APT groups that have repeatedly targeted Southeast Asian organizations. We will describe APT group actions using the MITRE ATT&CK terminology. The most common tactics, techniques, and sub-techniques are illustrated with examples from recent publicly disclosed cybercampaigns.

### Preparing resources for attacks

Before the phase of active intrusion, cybercriminals prepare the turf. This primarily involves creating the infrastructure needed to manage and control the attack (Acquire Infrastructure, Compromise Infrastructure). For example, the Earth Lusca group used compromised web servers (T1584.004) and rented virtual dedicated servers (T1583.003) from the provider Vultr to build infrastructure for a cybercampaign targeting numerous Asian organizations. The group registered domains (T1583.001) to create fake pages and host malicious payloads for watering hole attacks.



55% of groups

acquire resources to build infrastructure

Acquire Infrastructure

40% of groups

acquire resources and tools for attacks

Obtain Capabilities

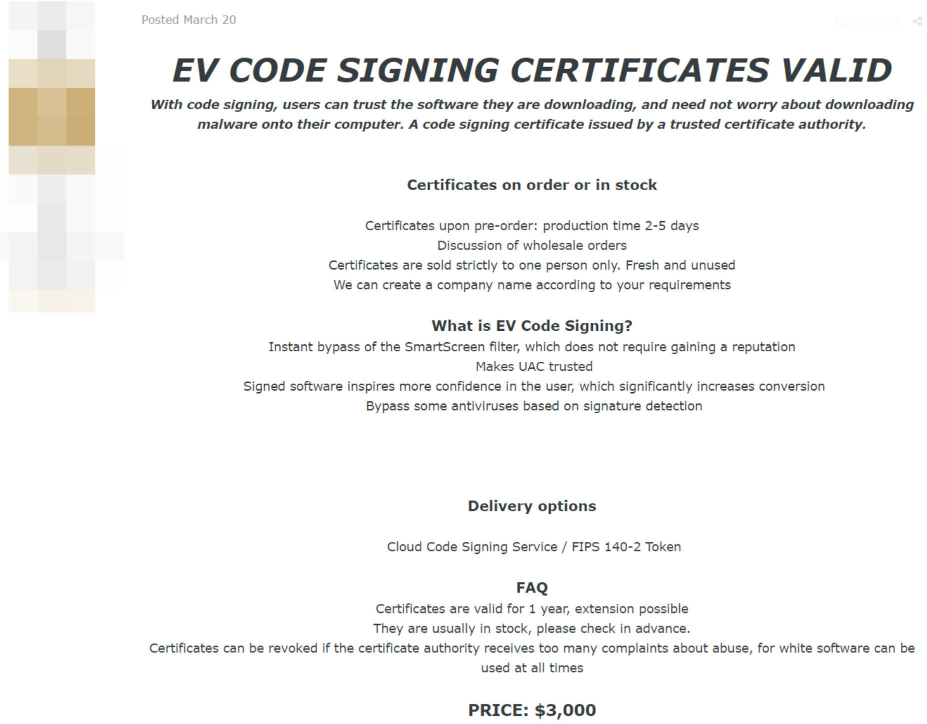
25% of groups

use third-party compromised infrastructure for attacks

Compromise Infrastructure

Figure 3. Most common techniques for preparing APT attacks

APT groups acquire various resources and tools needed for the attack (Obtain Capabilities). In addition to malware, these can include legitimate programs, both free and commercial. Some attackers modify publicly available tools to suit their needs. For instance, the APT10, Gallium, and GhostEmperor groups have modified a number of utilities to avoid detection by security tools. To disguise malware as legitimate software, cybercriminals acquire code signing certificates (T1588.003). For example, the Earth Krahang group used certificates issued by GlobalSign to sign XDealer loaders. Researchers at Trend Micro suggest these certificates might have been stolen from their legitimate owners. Criminals either steal certificates themselves or buy them on dark web forums.



Posted March 20

Report post

**_EV CODE SIGNING CERTIFICATES VALID_**

***With code signing, users can trust the software they are downloading, and need not worry about downloading malware onto their computer. A code signing certificate issued by a trusted certificate authority.***

**Certificates on order or in stock**

Certificates upon pre-order: production time 2-5 days
Discussion of wholesale orders
Certificates are sold strictly to one person only. Fresh and unused
We can create a company name according to your requirements

**What is EV Code Signing?**
Instant bypass of the SmartScreen filter, which does not require gaining a reputation
Makes UAC trusted
Signed software inspires more confidence in the user, which significantly increases conversion
Bypass some antiviruses based on signature detection

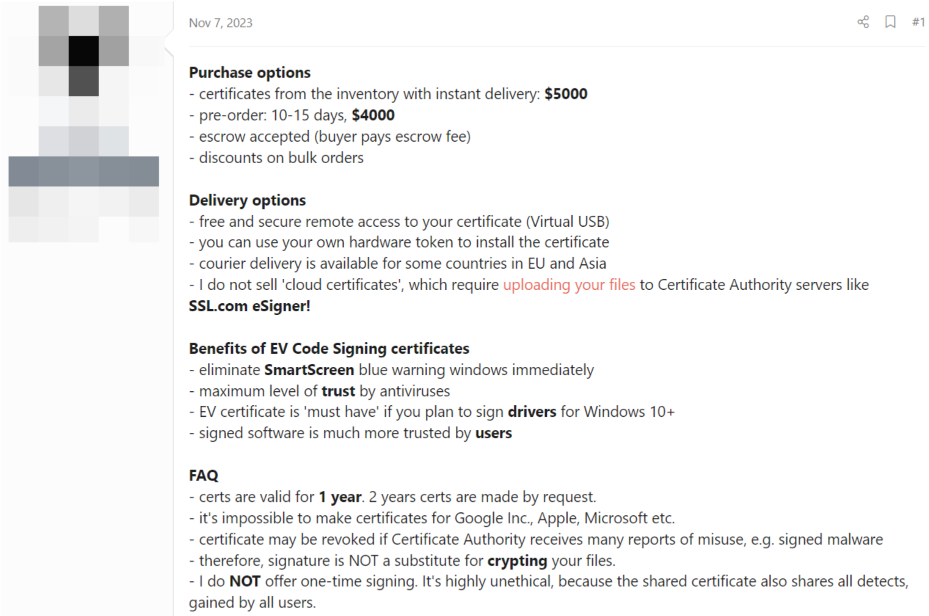
**Delivery options**

Cloud Code Signing Service / FIPS 140-2 Token

**FAQ**
Certificates are valid for 1 year, extension possible
They are usually in stock, please check in advance.
Certificates can be revoked if the certificate authority receives too many complaints about abuse, for white software can be used at all times

**PRICE: $3,000**

Figure 4. Advertisement for the sale of code signing certificates (example 1)



Nov 7, 2023

#1

**Purchase options**
- certificates from the inventory with instant delivery: **$5000**
- pre-order: 10-15 days, **$4000**
- escrow accepted (buyer pays escrow fee)
- discounts on bulk orders

**Delivery options**
- free and secure remote access to your certificate (Virtual USB)
- you can use your own hardware token to install the certificate
- courier delivery is available for some countries in EU and Asia
- I do not sell 'cloud certificates', which require uploading your files to Certificate Authority servers like **SSL.com eSigner!**

**Benefits of EV Code Signing certificates**
- eliminate **SmartScreen** blue warning windows immediately
- maximum level of **trust** by antiviruses
- EV certificate is 'must have' if you plan to sign **drivers** for Windows 10+
- signed software is much more trusted by **users**

**FAQ**
- certs are valid for **1 year**. 2 years certs are made by request.
- it's impossible to make certificates for Google Inc., Apple, Microsoft etc.
- certificate may be revoked if Certificate Authority receives many reports of misuse, e.g. signed malware
- therefore, signature is NOT a substitute for **crypting** your files.
- I do **NOT** offer one-time signing. It's highly unethical, because the shared certificate also shares all detects, gained by all users.

Figure 5. Advertisement for the sale of code signing certificates (example 2)

## Reconnaissance and initial attack vectors

During the reconnaissance stage, attackers try to gather as much information as possible about the target organization (Gather Victim Org Information) and its employees (Gather Victim Identity Information). To collect preliminary information about the victim, some groups, like Mustang Panda, APT32, and SideWinder, conduct phishing campaigns (Phishing for Information). For example, the SideWinder group sent emails with links leading to phishing sites to steal passwords. The stolen employee credentials could then be used for initial penetration into victim organizations (Valid Accounts).

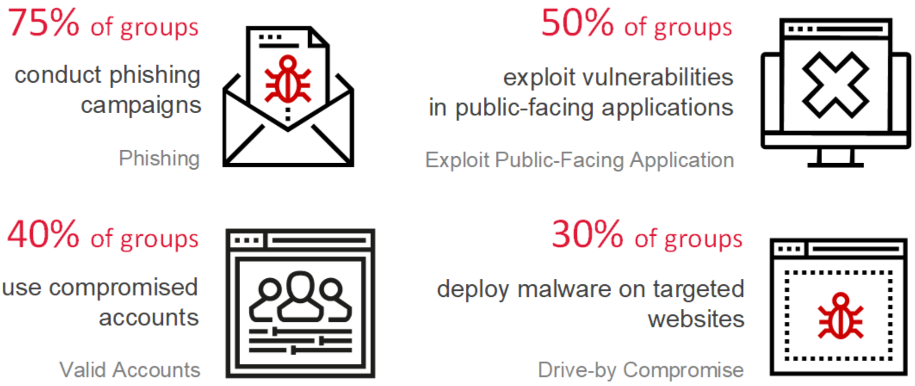


Figure 6. Most common techniques for gaining initial access

The information gathered during reconnaissance can be useful for attackers when composing emails with malicious attachments or links. Phishing campaigns (Phishing) are the most common technique for initial access, used by 75% of the APT groups we studied.

Email headers and attachment names may reflect geopolitical themes, and phishing campaigns are often timed to coincide with significant events in the region. For example, the Mustang Panda group sends out emails related to ASEAN summits. In February 2022, in a campaign targeting Southeast Asian countries, the group used malicious attachments named "ASEAN Leaders' Meeting.exe". In March 2024, the group conducted phishing campaigns referencing the ASEAN-Australia Special Summit.

**Table 1. Examples of phishing email attachments from APT groups attacking ASEAN countries**

| File name | APT group | Source |
|---|---|---|
| Talking_Points_for_China.zip | Mustang Panda | Unit 42 by Palo Alto Networks |
| Plan of Action (POA) - TH-VN - TH_Counterdraft_as of Feb 2022.doc.exe | Earth Krahang | Trend Micro |
| [Update] Counterdraft on the MoU on Rice Trade.zip.iso | Dark Pink | Group-IB |

Some attackers conduct phishing campaigns using previously compromised email addresses or documents stolen from previous victims, significantly increasing the chances that malicious emails will be delivered and read. For example, the Earth Krahang group used the hacked email account of a government agency to send phishing emails to other countries' governments. The Mustang Panda group sent phishing emails to organizations in Myanmar using documents in Burmese as bait. Trend Micro experts suggest these documents might have been previously stolen from other Myanmar organizations.

The second most popular technique for gaining initial access is exploiting vulnerabilities in public-facing servers (Exploit Public-Facing Application). This technique is used by half of the APT groups attacking Southeast Asian countries. First, attackers conduct active network scanning (Active Scanning) to find potential entry points. The Earth Krahang group, targeting government organizations in Southeast Asia, uses a whole arsenal of tools for scanning: sqlmap, kernel, xray, vscan, pocsuite, and wordpressscan. Attackers perform recursive searches in .git and .idea directories, browse directories for files with paths or credentials (T1595.003), and check subdomains to find interesting and potentially unmaintained servers with vulnerabilities (T1595.002). The APT41 group also uses various programs for active scanning. These include tools for brute forcing directories on web servers, the Nmap network scanner, the Acunetix vulnerability scanner, and the JexBoss tool for finding and exploiting vulnerabilities in Jboss and other Java applications.

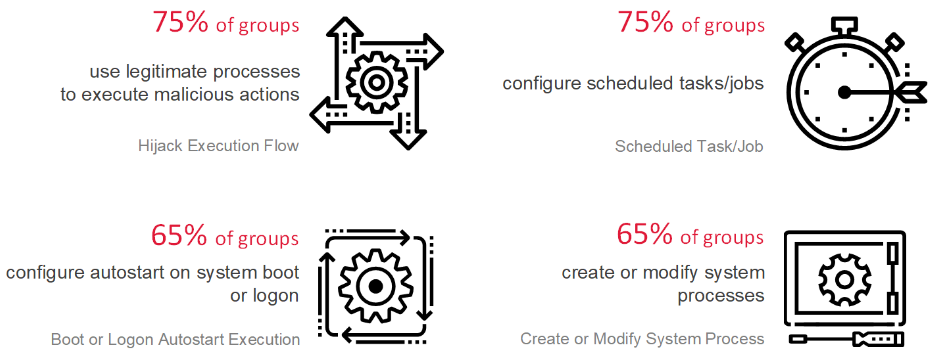
One of the attack vectors for APT groups targeting Southeast Asia involves finding and exploiting unpatched Microsoft Exchange servers. The Microsoft Exchange mail server is used by hundreds of thousands of companies worldwide. Its popularity and accessibility from the internet make it an attractive target for attackers. At least 30% of APT groups targeting Southeast Asia exploit vulnerabilities in Exchange. In 2022, the APT group ToddyCat compromised several organizations in Asian countries by exploiting a chain of critical vulnerabilities in Microsoft Exchange, known collectively as ProxyLogon. In 2023, the Earth Lusca group attacked government agencies and telecommunications companies in Southeast Asian countries, exploiting the ProxyShell vulnerabilities in Microsoft Exchange.

A number of APT groups (30%) choose watering hole attacks as their initial vector. They place scripts on websites that silently download malicious programs onto the computers of visitors (Drive-by Compromise). As bait, attackers might use compromised relevant resources or create their own sites that mimic real pages frequently visited by potential victims. For example, in the summer of 2021, ESET specialists discovered that the Mustang Panda group had hacked the website of the Myanmar presidential office and embedded a Cobalt Strike loader in a font package available for download on the site's main page.

## Gaining persistence in the victim's infrastructure

To maintain their presence in the victim's infrastructure, attackers must ensure that they retain access to the system even after a reboot or password change. Only then can they control the compromised environment and advance through the infrastructure in search of valuable information.

Three-quarters of APT groups maintain their presence in a compromised system by executing malicious code within the context of a legitimate process (Hijack Execution Flow). The two most popular methods are based on loading malicious dynamic link libraries (DLLs) in the context of legitimate applications. One-fifth of the groups use the sub-technique involving DLL search order hijacking in Windows (T1574.001). Attackers place a malicious library in a directory that the operating system checks before the one containing the legitimate DLL. Thus, when the application is launched, the malicious library is loaded instead of the legitimate one, allowing the attackers to execute their code on the victim's computer. Another popular approach involves attackers delivering a legitimate application and a malicious DLL to the victim's computer, placing them in the same directory, and then launching the application; thus, the malicious DLL is executed in the context of the legitimate process (T1574.002). This sub-technique doesn't rely on software installed within the infrastructure, making it very popular: 70% of the APT groups we studied use it. The Lancefly group is one of them. This group's Merdoor backdoor uses older versions of various legitimate programs, delivered in an SFX archive along with the loader and payload, to establish persistence.


75% of groups

use legitimate processes to execute malicious actions

Hijack Execution Flow

75% of groups

configure scheduled tasks/jobs

Scheduled Task/Job

65% of groups

configure autostart on system boot or logon

Boot or Logon Autostart Execution

65% of groups

create or modify system processes

Create or Modify System Process

Figure 7. Most common persistence techniques

Another common persistence technique involves using a task scheduler (Scheduled Task/Job). This allows malicious code to run each time the system starts or at scheduled intervals. Scheduled tasks can be created using the schtasks system utility. This technique is used by 75% of APT groups targeting Southeast Asian countries.

To maintain presence in the target environment, 65% of groups set up autostart programs (Boot or Logon Autostart Execution). They add malware to the Run registry key or the Startup folder (T1547.001), ensuring the malicious code executes every time the operating system starts. The Dark Pink and APT23 groups modify registry keys used by the

Winlogon.exe component (T1547.004). It handles various events: system login, loading the user profile during authentication, shutdown, and lockout. Modifying the corresponding registry keys turns these events into triggers for malicious payload execution, ensuring persistence in the system. Cybercriminals can add new registry keys or modify existing ones to install malware as print processors (T1547.012). Print processors are DLLs loaded by the print spooler (spoolsv.exe) during startup. This persistence method is used by the Earth Lusca and Gelsemium groups.

To maintain persistence in the victim's infrastructure, attackers can install malware as a service (Create or Modify System Process). In Windows, services run through the svchost.exe process, which provides them access to host resources. Services can be configured to run malicious code at specific times to ensure continuous presence. APT groups targeting Southeast Asian countries frequently hide malicious services behind the svchost.exe process. As a result, the attackers obtain a running process persisting through a service, enabling further development of the attack. This technique is used by 65% of the APT groups studied.

Attackers may use various combinations of persistence techniques. In attacks on Southeast Asian governments from Q2 2021 to Q3 2023, the Mustang Panda group used the multi-component Trojan ToneShell. The component designed for persistence tasks consists of DLL files. They were embedded in the context of PwmTower.exe—a component of Trend Micro's Password Manager program. Then, depending on privileges, a malicious service named DISMsrv and scheduled tasks or registry keys for autostart and scheduled tasks were created to establish persistence. After achieving persistence, the group loaded the next component of the Trojan, which is responsible for establishing network connections.

### Credential harvesting

As soon as attackers gain system privileges on a compromised host, they try to collect as many credentials as possible. Compromised accounts allow attackers to masquerade as legitimate users, making them difficult to detect. Additionally, the same passwords may be used to access different resources, facilitating lateral movement within the perimeter.

The most commonly used technique for obtaining credentials is extracting them from the memory of system components (OS Credential Dumping), used by 65% of APT groups. Here are the main sources the APT groups we studied use to search for credentials in Windows:

- **lsass.exe process memory** (T1003.001). Responsible for authenticating users during system login and enforcing security policies. Passwords are extracted from lsass memory by 45% of APT groups. For this purpose, public tools such as Mimikatz, ProcDump, and LaZagne are frequently used.
- **Security Account Manager database (SAM)** (T1003.002). It stores local user credentials in the form of hash values. Credential extraction from the SAM database is practiced by 35% of APT groups. For example, in cybercampaigns targeting Southeast Asian governments in 2022 and 2023, the Gallium group created scheduled tasks that ran scripts with commands to extract credentials from the SAM registry hive using the reg.exe utility.
- **NTDS database** (T1003.003).Some groups (15%) extracted accounts from the NTDS.dit database file, which stores Active Directory information, including password hash values of all domain users. To do this, attackers used the system utilities ntdsutil and vssadmin. For example, the Mustang Panda group makes a shadow copy of the volume on the domain controller and extracts from it the NTDS.dit file and the key to decrypt it.

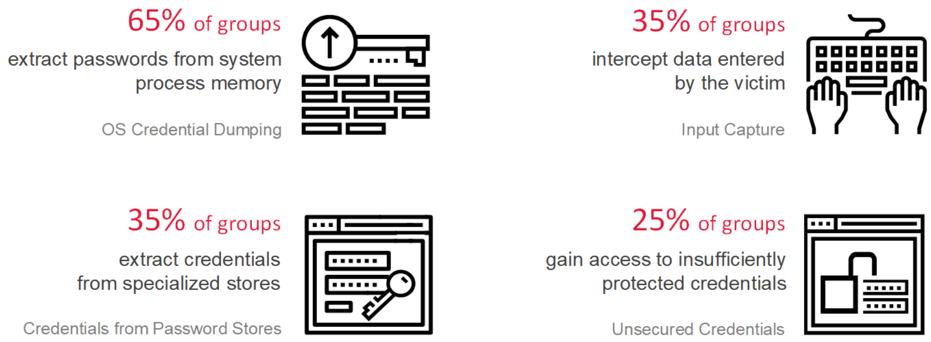


Figure 8. Most common techniques for credential access

A third of APT groups (35%) intercept data that the victim enters on a compromised device (Input Capture). For this purpose, they use keyloggers—malware that intercepts keystrokes. Keyloggers are in the arsenal of many groups, such as APT10, APT41, Lancefly, and Mustang Panda.

Some groups extracted credentials from specialized storage locations (Credentials From Password Stores). Since web browsers have built-in password stores, a number of APT groups use tools to extract credentials from these stores (T1555.003). For example, for this purpose the Earth Estries group uses the TrillClient stealer, while APT41 uses the BrowserGhost utility. The Goblin Panda group has the ChromePass tool in its arsenal, which steals saved passwords from Chromium-based browsers. The program collects credentials in an HTML document containing a table with addresses, usernames, and passwords.

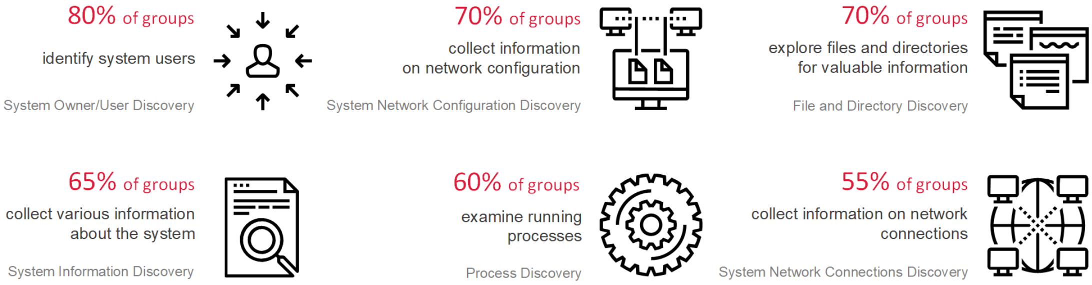
A quarter of APT groups search for unsecured or poorly protected credentials (Unsecured Credentials). They can browse user files on the hard drive in search of saved logins and passwords (T1552.001). For example, the APT41 group searched for strings in files using the keywords "user" and "password".

## Investigating the corporate infrastructure

Attackers try to understand how the environment they've entered operates. To gather information, attackers often use tools included in the operating system. This minimizes any traces of activity, masks their actions, and cuts the cost of developing custom software.

Cybercriminals try to gather as much information as possible about the compromised system (System Information Discovery). The systeminfo utility can be used to collect system information. This is a built-in Windows utility that provides detailed information about the operating system and BIOS configuration, as well as hardware specifications. It is used by the groups Naikon, Mustang Panda, and GhostEmperor.

Most (80%) APT groups seek to identify users of compromised hosts (System Owner/User Discovery). This information can be used to escalate privileges or advance through the infrastructure. The whoami utility is often used to gather information about the current user, including their group and privileges. For example, it is used by groups such as APT32, APT41, Dark Pink, Earth Lusca, and Gelsemium.



80% of groups
identify system users
System Owner/User Discovery

70% of groups
collect information on network configuration
System Network Configuration Discovery

70% of groups
explore files and directories for valuable information
File and Directory Discovery

65% of groups
collect various information about the system
System Information Discovery

60% of groups
examine running processes
Process Discovery

55% of groups
collect information on network connections
System Network Connections Discovery

Figure 9. Most common techniques for environment discovery

Attackers gather information about the network configuration (System Network Configuration Discovery) and active network connections of the compromised host (System Network Connections Discovery). This information is needed for further advancement in the infrastructure and to maintain communication with the command server. At this stage, network diagnostic utilities such as ping, ipconfig, arp, netstat may be used. They are used by groups like Mustang Panda, APT32, APT41, Gallium, Naikon, Earth Lusca, and others.

Attackers explore files and directories on compromised hosts (File and Directory Discovery) to understand the infrastructure and find valuable information, such as credentials or confidential documents. The SideWinder group conducted a cybercampaign from June to November 2021, targeting government, financial, and telecommunications organizations in Myanmar. Using the infostealer SideWinder.StealerPy, the group searched for files with extensions corresponding to office documents and images, and obtained a list of directories and files from the desktop.

More than half (60%) of APT groups study the processes running on the host (Process Discovery). This information is needed to understand the environment, including installed security tools. For example, the Gelsemium group's trojan checks the list of running processes for the presence of security tools from a predefined list. In Windows, there are several ways to get a list of running processes. For example, the groups Mustang Panda, ToddyCat, Earth Lusca, and Naikon use the tasklist command. APT23 and GhostEmperor obtained the list of running processes using the PsList utility from Sysinternals' PsTools suite.

APT groups may use custom-developed software to collect information. For example, the Mustang Panda group's trojan Hodur (a variant of PlugX) collects detailed system information: uptime, Windows version, CPU clock speed, RAM size, and screen resolution. Additionally, the trojan can obtain the current user's name, the host's name, and its IP address.

## Collecting valuable information

An important stage for attackers is collecting information valuable for cyberespionage. Sources of valuable information include local files on employees' workstations, browsers, email, shared network storage, cloud storage, and code repositories.

More than half (65%) of groups search for the information of interest in local files on compromised devices (Data from Local System). Cybercriminals can search for data in various sources. For example, the Dark Pink group collected files from web browsers, while APT41 collected from the Windows Volume Shadow Copy Service and the logging system.

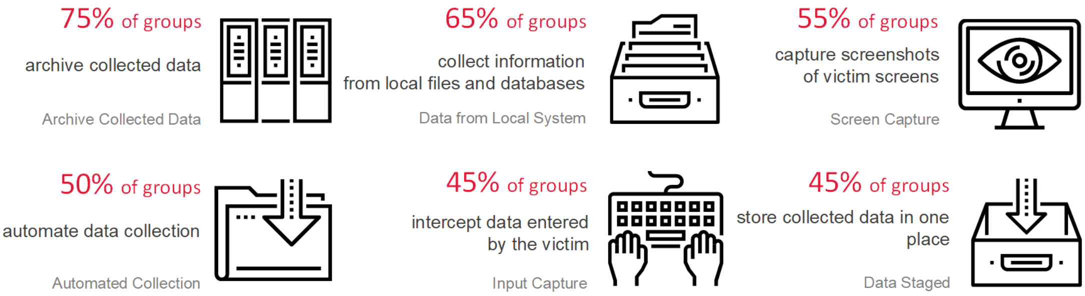


Figure 10. Most common data collection techniques

Attackers take screenshots (Screen Capture) and intercept data entered by the victim (Input Capture). Often, both techniques are implemented using the same software tools. For example, the Gallium group used the trojan Quasar in a cyberattack on government organizations in one Southeast Asian country, which has keylogging and screen recording functions. Similarly, the Earth Estries group used the HemiGate backdoor, which implements both functions.

Attackers can automate data collection using scripts that search for and copy the necessary information (Automated Collection). In 2023, the ToddyCat group conducted a cybercampaign targeting a government organization in Malaysia. Using a PowerShell script that ran in a scheduled task, the attackers found user documents and saved them in a temporary directory. Automated data collection can be performed using malware functionality.

Some APT groups (45%) place collected data in one directory before exfiltrating it (Data Staged). Such storage can be the Recycle Bin, a directory unpopular among regular users, or other local or remote locations. This allows attackers to keep stolen files out of the victim's sight.

Most groups (75%) archive or encrypt collected data (Archive Collected Data). Compressing data allows attackers to transmit the collected information much faster. Usually, the victims' devices already have the necessary software for this, such as WinRAR, 7z, or tar. Many groups use these utilities, including APT41, Earth Estries, GhostEmperor, Lancefly, Mustang Panda, and ToddyCat (T1560.001). Coding and encryption of information is carried out in order to hide stolen data. For example, the Sharp Panda group encrypted collected information using the RC4 algorithm and converted it to Base64 format.

### Interacting with the C&C server

The ability to exchange data with compromised devices within the network and transmit stolen information externally is one of the factors determining a successful outcome of an APT attack (for attackers that is). Usually, attackers configure multiple channels to interact with the command server. It's crucial for attackers that these network connections remain undetected by security tools, such as network traffic analyzers.

A common strategy is to mix malicious traffic with legitimate traffic. Attackers prefer to use application layer protocols (Application Layer Protocol). Primarily, the HTTP(S) protocol (T1071.001), used by 85% of APT groups. In addition to HTTP(S), 25% of groups use the DNS protocol (T1071.004) for communication with the command server.

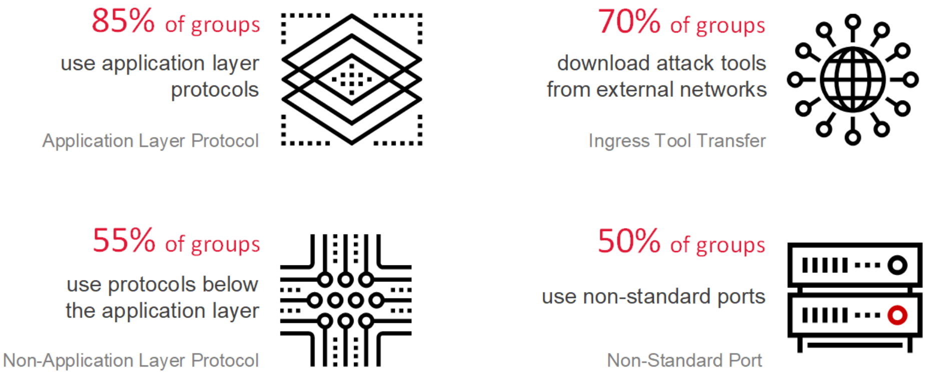


Figure 11. Most common techniques for command and control

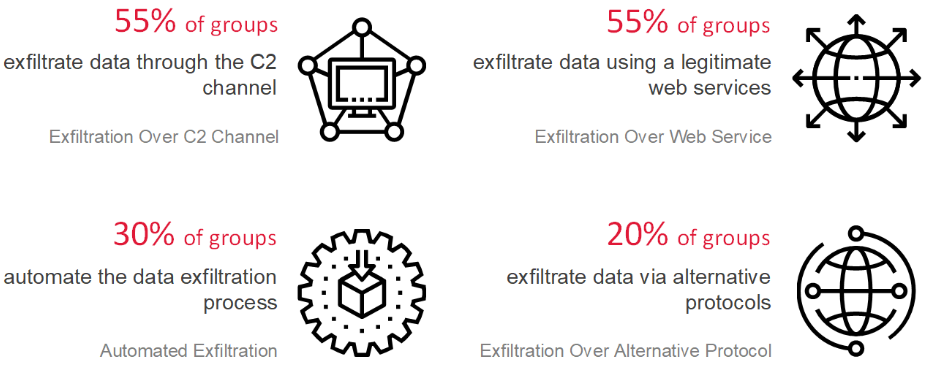
At the same time, 55% of APT groups use lower-level protocols in the OSI model than the application layer (Non-Application Layer Protocol). For example, the SmileSvr backdoor of the APT23 group communicates with the command server using the ICMP protocol. The MgBot backdoor of the Evasive Panda group interacts with the command server using UDP and TCP protocols. Some malware supports protocols at different levels. For instance, the Lancefly group's Merdoor backdoor can receive commands via HTTP, HTTPS, DNS, UDP, and TCP protocols.

Every second APT group uses non-standard ports (Non-Standard Port). For example, the backdoors of the SideWinder group established connections on ports 41236, 47896, 45632, 45689, 8087, 8090.

After establishing themselves in the compromised environment, attackers can download additional tools from outside (Ingress Tool Transfer). This occurs both through the communication channel with the command server and through alternative methods. For example, the APT41 group used Cobalt Strike to download additional files onto compromised devices. In the "Arsenal of APT groups" section, we'll discuss some other tools used by cybercriminals to load their files into the victim's infrastructure.

### Exfiltration of stolen data

Most APT groups upload stolen data through the communication channel with the command server (Exfiltration Over C2 Channel) or via legitimate web services (Exfiltration Over Web Service). For example, the Dark Pink group used Telegram and Dropbox to transfer stolen data in their attacks on Southeast Asian countries at the end of 2022 (T1567.002). Later, in attacks on organizations in the Asia-Pacific region, including Vietnam, Thailand, and Indonesia, this same group transferred stolen data using webhook.site—a free platform for testing and debugging incoming HTTP requests and emails. The attackers used this service to generate temporary addresses and receive webhooks, through which they transmitted stolen confidential data (T1567.004). Transferring stolen information through the webhook mechanism allows attackers to disguise data exfiltration as legitimate traffic. The Earth Estries group uploaded stolen data to anonymous file-sharing services AnonFiles In 2023, the service was shut down due to cybercriminals abusing it as a platform for exfiltrating stolen data. and File.io using the Curl utility (T1567.003).



55% of groups
exfiltrate data through the C2 channel
Exfiltration Over C2 Channel

55% of groups
exfiltrate data using a legitimate web services
Exfiltration Over Web Service

30% of groups
automate the data exfiltration process
Automated Exfiltration

20% of groups
exfiltrate data via alternative protocols
Exfiltration Over Alternative Protocol

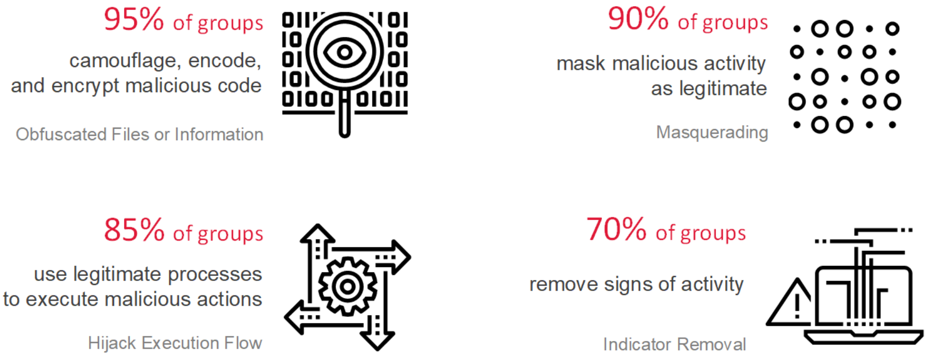
Figure 12. Most common data exfiltration techniques

Every fifth group exfiltrates stolen information using alternative protocols (Exfiltration Over Alternative Protocol). Alternative protocols include any network protocols not used for communication with the command server. Attackers can encrypt data transmitted through alternative channels.

Cybercriminals can automate data exfiltration from a compromised infrastructure (Automated Exfiltration). For example, the SideWinder group's info-stealer can automatically send collected data to a special email address or another network resource controlled by the attackers.

### Evasion techniques

APT groups have numerous techniques to bypass security mechanisms and hide malicious activities. Attackers try to make executable files difficult to detect and analyze by compressing, encoding, encrypting, and obfuscating the malicious code (Obfuscated Files or Information). This is the most common technique, used by 95% of APT groups. A significant portion of groups (45%) use specialized tools to obfuscate code and prevent analysis (T1027.002). Such tools include packers and protectors, as well as commercial software designed to protect against reverse engineering. Some groups, like Mustang Panda, Gelsemium, APT32, APT40, and APT41, add "garbage" code to their malware to complicate analysis by antivirus tools (T1027.001).



95% of groups
camouflage, encode, and encrypt malicious code
Obfuscated Files or Information

90% of groups
mask malicious activity as legitimate
Masquerading

85% of groups
use legitimate processes to execute malicious actions
Hijack Execution Flow

70% of groups
remove signs of activity
Indicator Removal

Figure 13. Most common techniques for defense evasion

Almost all APT groups (90%) targeting Southeast Asia disguise their activities as legitimate operations, processes, files, and commands (Masquerading). Most groups (70%) use names for malware that are partially or fully identical to legitimate file names and place them in non-suspicious directories, like the System32 directory (T1036.005). More than half (55%) of the groups disguise malware as Windows system services (T1036.004). In one of its operations against military organizations in Southeast Asian countries, the Naikon group disguised malware as executable files from Google Chrome, Adobe, and VMware. For malicious services and scheduled tasks, the group used names resembling or completely copying legitimate service names; for example, they named a malicious service "taskmgr" to pass it off as Task Manager. In one of its large-scale cybercampaigns targeting Asian organizations, the SideWinder group disguised Trojans as the Windows Defender antivirus and hid tasks in the task scheduler under names like WindowSecurityPatch, CloudAPIManager, WindowsUpdate, WindowHost. At the initial penetration stage, the group used a decoy file named Wang_Yi_Statement_to_Defeat_COVID19.pdf.lnk in phishing emails. This is an LNK loader mimicking a PDF document. Thirty percent of APT groups targeting Southeast Asia use double extensions to disguise malicious files (T1036.007).

We previously mentioned that many APT groups use the Hijack Execution Flow technique to persist in the system. In addition, 85% of groups use this technique to bypass security tools and remain in the victim's infrastructure as long as possible. For example, the Earth Estries group used old versions of legitimate programs to implement the DLL Side-Loading sub-technique.

Most APT groups complicate the work of cybersecurity specialists by hiding or erasing traces of activity (Indicator Removal): they delete their files and programs (T1070.004), modify timestamps on malicious files (T1070.006), clear event logs (T1070.001), and erase command execution history (T1070.003). For example, the APT23 group has a custom tool for clearing event logs on a compromised computer. Cybercriminals may destroy any artifacts that provide evidence of their presence in the system; they delete malicious services and previously created accounts, and reverse registry changes (T1070.009).

## Arsenal of APT groups

Let's look at the tools used by APT groups targeting Southeast Asia. Many groups have unique software in their arsenal that they've developed themselves. For example, Dark Pink uses the info stealers Cucky and Ctealer to steal data from browsers; this malware has never been seen from any other group. In addition to self-developed malware, APT groups also frequently use common malware and legitimate tools.

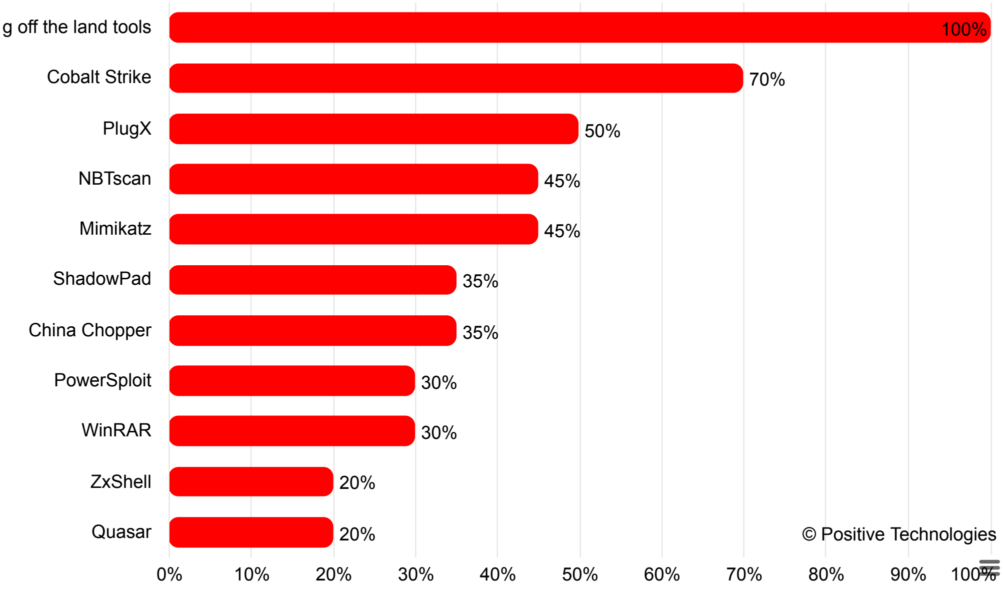
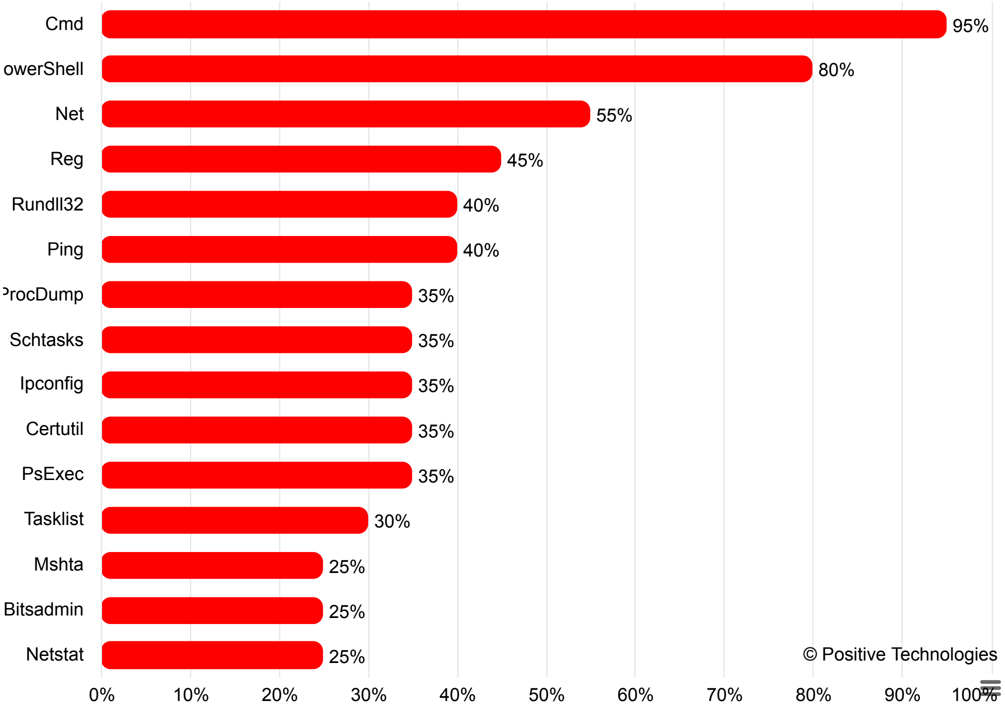


Figure 14. Most common tools used in APT attacks on ASEAN countries (share of APT groups)

**Living off the land tools**

Let's start with legitimate tools that attackers don't need to load from outside because they are already present in the compromised system. This is known as living off the land, and such tools are known as LOLBins, or LOL binaries. Using them has undeniable advantages: it allows cybercriminals to disguise their activities as actions of IT personnel, thus avoiding detection by security tools, and minimizes the costs of developing their own programs.



Bitsadmin

Percentage: **25%**

Figure 15. Top-15 LOLBin tools in APT attacks on ASEAN countries (share of APT groups)

First and foremost, we're talking about the command line (cmd.exe) and the PowerShell scripting language. Attackers use the Windows command line interface to execute system commands and run malicious scripts. With PowerShell, you can automate tasks, manage configurations, and access virtually any component of the operating system.

More than half (55%) of APT groups use the system utility net.exe. This is a tool for managing various network components. It can be used to perform many tasks, including viewing and managing network resources, user accounts, group memberships, services, and print queues, all while masquerading as a network administrator. For example, with the net start command, the Evasive Panda group's MgBot Trojan installer starts the AppMgmt system service, allowing centralized application installation on remote computers via a group policy.

Using LOLBin files signed with trusted digital certificates, attackers can proxy the execution of malicious code to avoid detection by security tools (System Binary Proxy Execution). One such file is rundll32.exe. This is a Windows component responsible for loading and running functions from DLL libraries (T1218.011). The primary scenario for attackers is to run malicious libraries on compromised hosts. Rundll32 is used by 40% of APT groups targeting Southeast Asia. Another Windows component frequently used by attackers is the mshta.exe command-line utility. It is designed to execute HTA (Microsoft HTML Applications) format files. One in four groups uses mshta.exe to execute HTA files with malicious scripts in JavaScript, JScript, or VBScript (T1218.005).

Some groups (35%) use the system utility certutil. The utility is intended to display certification authority configuration information, configure certification services, and backup and restore certification authority components. It allows files to be downloaded, which attackers exploit to download their tools (Ingress Tool Transfer). For example, the Earth Krahang group used certutil to download the SoftEther program onto compromised servers to set up VPNs.

Another system utility frequently abused by attackers to download additional tools is Bitsadmin. It is used by one in four APT groups. The utility is designed to manage BITS (Background Intelligent Transfer Service) tasks, primarily for downloading Windows updates, but attackers use it to download arbitrary files. For example, after gaining initial access, the APT23 group uses Bitsadmin to deliver next-stage loaders to compromised servers.

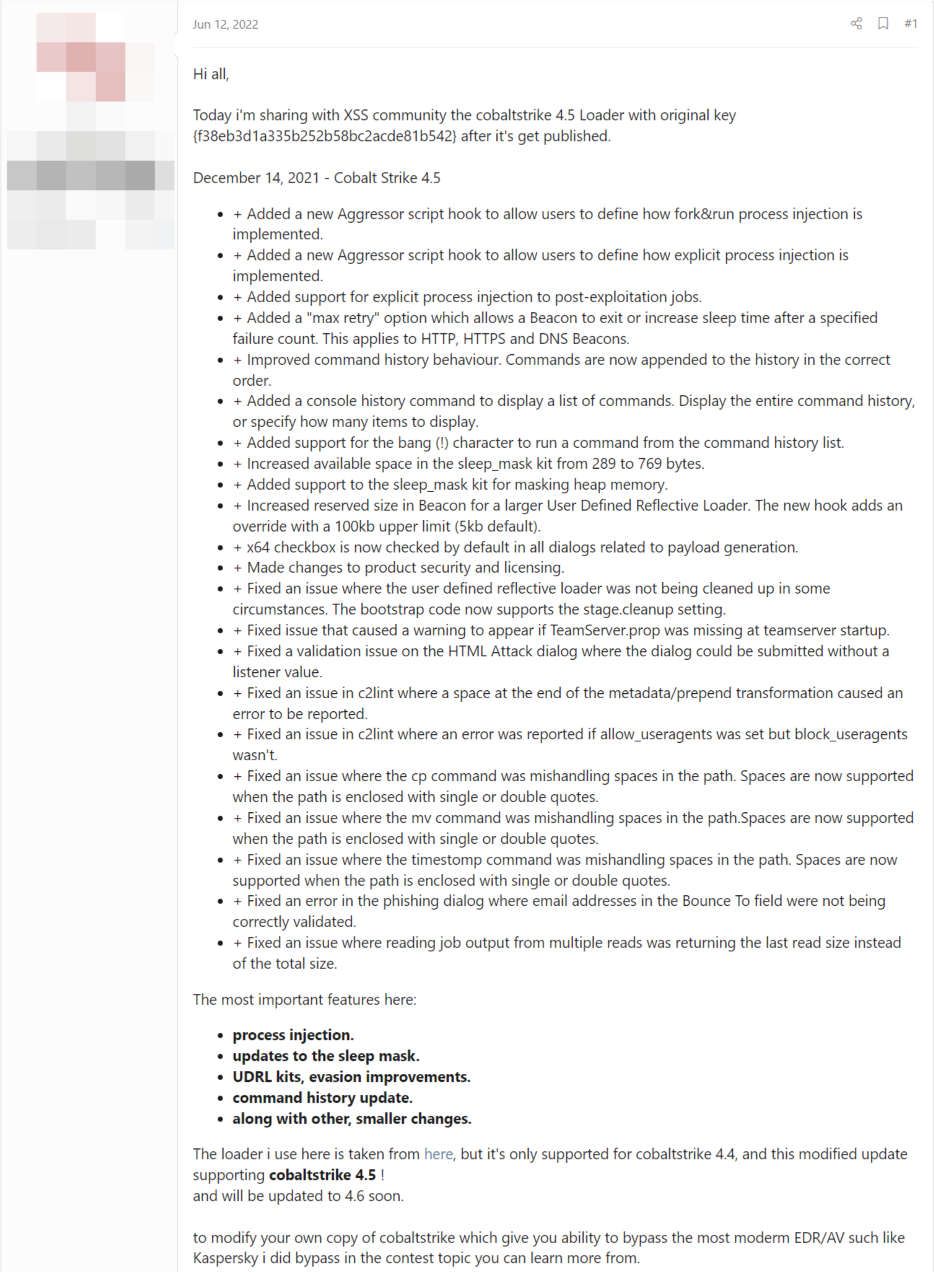
The most comprehensive lists of LOLBin tools can be found in the GitHub repository and the guide by the U.S. agency CISA. Every APT group targeting Southeast Asian countries uses one or another of these tools. For example, the Lancefly group used LOLBin techniques for credential theft: they ran rundll32.exe to call the MiniDump function from the comsvcs.dll library in order to dump the memory of the LSASS process, and they used the reg.exe utility to dump the SAM and SYSTEM registry hives to extract credentials from the SAM database.

**Cobalt Strike**

The Cobalt Strike platform is commercial software developed as a penetration testing tool. Due to its extensive functionality, the platform has attracted the attention of cybercriminals. Although the developers of Cobalt Strike take measures to protect the product from hacking, many cybercriminals use old cracked or pirated versions of Cobalt

Strike at various stages of an attack. The flexibility of this tool allows APT groups to create custom builds, adding or removing features depending on their goals. Some attackers do this themselves, while others buy modified versions of Cobalt Strike on the dark web.

Cobalt Strike is in the arsenal of 70% of APT groups targeting Southeast Asia. For example, the Earth Longzhi subgroup of APT41 used special versions of Cobalt Strike loaders with sophisticated anti-detection mechanisms in attacks on organizations in the Philippines, Thailand, Malaysia, and Indonesia. Combined with other techniques, this allowed the attackers to remain undetected in victims' infrastructures from September 2021 to June 2022.



Jun 12, 2022 #1

Hi all,

Today i'm sharing with XSS community the cobaltstrike 4.5 Loader with original key {f38eb3d1a335b252b58bc2acde81b542} after it's get published.

December 14, 2021 - Cobalt Strike 4.5

- + Added a new Aggressor script hook to allow users to define how fork&run process injection is implemented.
- + Added a new Aggressor script hook to allow users to define how explicit process injection is implemented.
- + Added support for explicit process injection to post-exploitation jobs.
- + Added a "max retry" option which allows a Beacon to exit or increase sleep time after a specified failure count. This applies to HTTP, HTTPS and DNS Beacons.
- + Improved command history behaviour. Commands are now appended to the history in the correct order.
- + Added a console history command to display a list of commands. Display the entire command history, or specify how many items to display.
- + Added support for the bang (!) character to run a command from the command history list.
- + Increased available space in the sleep_mask kit from 289 to 769 bytes.
- + Added support to the sleep_mask kit for masking heap memory.
- + Increased reserved size in Beacon for a larger User Defined Reflective Loader. The new hook adds an override with a 100kb upper limit (5kb default).
- + x64 checkbox is now checked by default in all dialogs related to payload generation.
- + Made changes to product security and licensing.
- + Fixed an issue where the user defined reflective loader was not being cleaned up in some circumstances. The bootstrap code now supports the stage.cleanup setting.
- + Fixed issue that caused a warning to appear if TeamServer.prop was missing at teamserver startup.
- + Fixed a validation issue on the HTML Attack dialog where the dialog could be submitted without a listener value.
- + Fixed an issue in c2lint where a space at the end of the metadata/prepend transformation caused an error to be reported.
- + Fixed an issue in c2lint where an error was reported if allow_useragents was set but block_useragents wasn't.
- + Fixed an issue where the cp command was mishandling spaces in the path. Spaces are now supported when the path is enclosed with single or double quotes.
- + Fixed an issue where the mv command was mishandling spaces in the path.Spaces are now supported when the path is enclosed with single or double quotes.
- + Fixed an issue where the timestomp command was mishandling spaces in the path. Spaces are now supported when the path is enclosed with single or double quotes.
- + Fixed an error in the phishing dialog where email addresses in the Bounce To field were not being correctly validated.
- + Fixed an issue where reading job output from multiple reads was returning the last read size instead of the total size.

The most important features here:

- **process injection.**
- **updates to the sleep mask.**
- **UDRL kits, evasion improvements.**
- **command history update.**
- **along with other, smaller changes.**

The loader i use here is taken from here, but it's only supported for cobaltstrike 4.4, and this modified update supporting **cobaltstrike 4.5** !
and will be updated to 4.6 soon.

to modify your own copy of cobaltstrike which give you ability to bypass the most moderm EDR/AV such like Kaspersky i did bypass in the contest topic you can learn more from.

Figure 16. Advertisement for the Cobalt Strike version with detection evasion

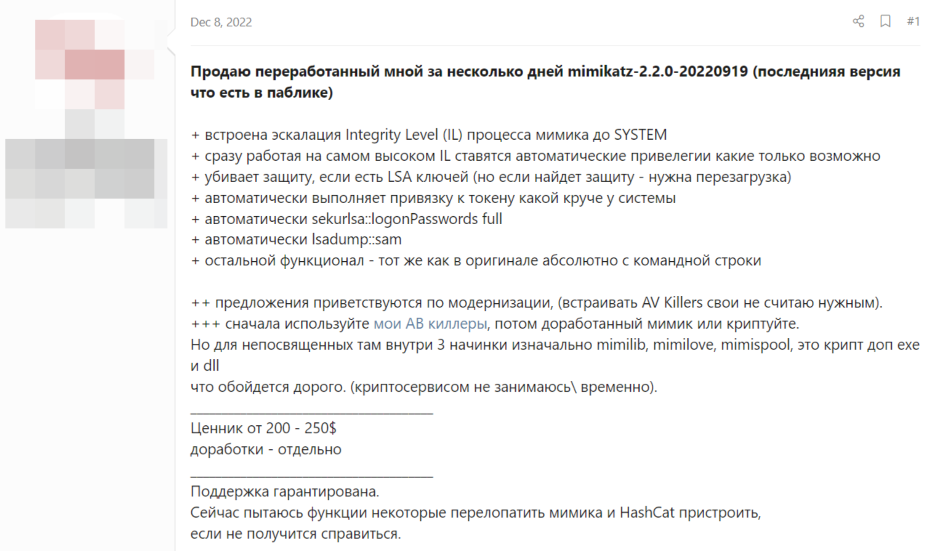
**PlugX**

PlugX is a family of modular remote access malware. It has extensive capabilities, including the ability to take screenshots, capture keystrokes, and load additional modules. To establish PlugX in a compromised system, attackers most commonly use the DLL Side-Loading technique.

PlugX was first observed in attacks by the Mustang Panda group. Trend Micro specialists note that since 2018, this group has had four generations of PlugX in its arsenal. The latest generation, named DOPLUGS, was used by Mustang Panda in 2023 in campaigns against Vietnam, Malaysia, and other Asian countries. Additionally, there is a variant of DOPLUGS with an integrated module called KillSomeOne. This is a USB worm designed for spreading malware and stealing documents. Currently, various modifications of PlugX are used by every second APT group targeting Southeast Asian countries.

**Mimikatz**

Mimikatz is an open-source utility that allows attackers to extract credentials from RAM. There are modified versions of this program. For example, the GhostEmperor group uses a utility called Mimikat_ssp—a modified Mimikatz with detection evasion capabilities. On dark web forums, samples of Mimikatz with enhanced features and detection evasion can be found for sale. Mimikatz is used by 40% of APT groups targeting Southeast Asia.



[redacted]

Dec 8, 2022

#1

**Продаю переработанный мной за несколько дней mimikatz-2.2.0-20220919 (последнияя версия что есть в паблике)**

+ встроена эскалация Integrity Level (IL) процесса мимика до SYSTEM
+ сразу работая на самом высоком IL ставятся автоматические привелегии какие только возможно
+ убивает защиту, если есть LSA ключей (но если найдет защиту - нужна перезагрузка)
+ автоматически выполняет привязку к токену какой круче у системы
+ автоматически sekurlsa::logonPasswords full
+ автоматически lsadump::sam
+ остальной функционал - тот же как в оригинале абсолютно с командной строки

++ предложения приветствуются по модернизации, (встраивать AV Killers свои не считаю нужным).
+++ сначала используйте мои АВ киллеры, потом доработанный мимик или криптуйте.
Но для непосвященных там внутри 3 начинки изначально mimilib, mimilove, mimispool, это крипт доп exe и dll
что обойдется дорого. (криптосервисом не занимаюсь\ временно).

____________________________________

Ценник от 200 - 250$
доработки - отдельно

____________________________________

Поддержка гарантирована.
Сейчас пытаюсь функции некоторые перелопатить мимика и HashCat пристроить,
если не получится справиться.

Figure 17. Advertisement for a modified version of Mimikatz (in Russian)

### NBTscan

NBTscan is an open-source tool designed to scan IP networks for NetBIOS name information. The tool is used by 45% of APT groups targeting Southeast Asia at the stage of corporate infrastructure reconnaissance to gather information about hosts and services on the network.

### ShadowPad

ShadowPad is a remote access trojan that is a less popular direct descendant of PlugX. It was first seen in campaigns by the APT41 group against Japanese organizations and later spread to Southeast Asian countries. Currently, ShadowPad is used by 35% of APT groups targeting Southeast Asian states.

### China Chopper

China Chopper is a well-known web shell that is only 4 kilobytes in size. It has been used in attacks since at least 2012 for remote access to compromised web servers. Due to its small size, there are many ways to deliver the web shell. In attacks on Southeast Asian states, China Chopper is used by 35% of APT groups. For example, the ToddyCat group compromised vulnerable Microsoft Exchange servers in attacks on Vietnamese organizations and then used China Chopper to initiate a multi-stage infection chain.

### PowerSploit

PowerSploit is an open-source framework consisting of modules and scripts written in PowerShell and designed for a wide range of penetration testing tasks. It is used for malicious purposes by 30% of APT groups. For example, the Dark Pink group utilized the Get-MicrophoneAudio module from PowerSploit to record audio from a victim's microphone. The attackers modified the module's code beforehand to bypass antivirus protection.

### WinRAR

To compress stolen data and reduce exfiltration time, attackers use archivers. The most popular is WinRAR, used by 30% of APT groups. Some groups disguise the use of the archiver. For example, the Lancefly group disguised WinRAR as the system process wmiprvse.exe.

### ZxShell

ZxShell is an open-source rootkit known since 2004. It is continuously being developed. It has keylogger functions, can take screen captures, perform network attacks, and load, run, and delete files. It is in the arsenal of every fourth group attacking Southeast Asian countries.

### Quasar

Quasar is an open-source remote access trojan with a wide range of capabilities: keylogging, screenshot capturing, webcam recording, and stealing credentials from browsers and FTP clients. It is used by attackers worldwide, including 25% of APT groups targeting Southeast Asia.

## Conclusions and recommendations

The digital economy has become a significant driver of economic growth in Southeast Asian countries in the post-pandemic era. Today, technologies such as cloud computing, big data, artificial intelligence, the Internet of Things, and 5G are gaining importance in the region's economic development. The number of potential targets for cybercriminals is growing rapidly, and cybersecurity issues are becoming increasingly crucial. To protect their critical infrastructure and ensure national security, ASEAN member states need to prioritize strengthening of their cyberdefense capabilities.

**Raising awareness of cybersecurity importance**

The path to building a robust cybersecurity system in Southeast Asia lies through raising awareness and expanding regional cooperation. The digital divide in ASEAN presents a significant obstacle to cooperation in countering cyberthreats. Not all states have the capacity to resist complex targeted attacks. Developed countries like Malaysia and Singapore have taken a leading role with regional cyberinitiatives. However, the successful development of the region's cyber resilience will depend not only on the actions of economic leaders but also on the willingness of other countries to disclose details of APT attacks.

**Comprehensive response measures**

ASEAN has adopted a cybersecurity cooperation strategy for 2021–2025 and a digital development plan (ASEAN Digital Masterplan 2025). The implementation of these frameworks in each country heavily depends on its resources and priorities. Responses to complex targeted attacks in some Southeast Asian countries are uncoordinated and fragmented. Comprehensive national cybersecurity strategies need to be developed. They should cover every aspect, from policy issues to details of technical implementation. It's important to regularly review strategies and principles to ensure their relevance in the constantly changing cyberthreat landscape.

**Supporting and cooperation with the private sector**

States need to encourage joint initiatives involving the private sector and cybersecurity experts. Partnerships between regulators and key industry players facilitate the prompt sharing of resources, expertise, and information on current APT attack tactics and techniques.

**Results-oriented cybersecurity**

Combating complex targeted attacks requires a special approach based on the concept of results-oriented cybersecurity. Infrastructure and processes should be built in such a way that even if attackers penetrate the organization's network, they cannot inflict non-tolerable damage. The primary goal becomes eliminating the possibility of non-tolerable events—those that prevent an organization from achieving its operational or strategic goals or lead to significant disruption of its core business as a result of a cyberattack. These events are defined by the organization's top management.

We recommend that organizations pay attention to the fundamentals of results-oriented cybersecurity.

- IT asset inventory

The first step is to identify all assets in the organization's infrastructure. It's important to classify them based on their importance, taking into account non-tolerable events for the organization. VM (Vulnerability Management) solutions automate the processes of asset identification and management and the detection and fixing of vulnerabilities in infrastructure components, depending on their level of severity. For companies involved in the development of software products, we recommend considering source code analysis tools to identify vulnerabilities and design flaws during the development phase.

- Incident monitoring and response

Monitoring events allows cybersecurity specialists to swiftly detect attack indicators and take countermeasures against the APT group. A SIEM (security information and event management) system can help with this task. It enables you to monitor and analyze security events from various sources, detect anomalies, and receive prompt alerts about them. It's important that sources for monitoring events are selected taking into account typical entry points into the company's infrastructure. For groups targeting Southeast Asia, one of these typical points is Microsoft Exchange servers.

Industrial and energy companies are recommended to consider specialized solutions for analyzing ICS traffic. They help detect malicious activity without negatively impacting production processes.

Properly established processes for responding to initial penetration indicators help prevent or localize and eliminate the consequences of APT attacks. Combining a SIEM system with XDR (Extended Detection and Response) solutions can provide effective protection.

To swiftly detect APT attacks and respond to them, a tool for deep network traffic analysis is also indispensable. NTA (Network Traffic Analysis) solutions can help address this challenge. These tools detect malicious activity on the perimeter and inside the network, including in encrypted traffic. All APT groups have malware in their arsenal.

- Cybersecurity training

The human factor is a weak link in the cyberdefense chain, and even a single error can open doors to attackers. To prevent this, it's necessary to increase employee awareness through effective training programs. Training programs should include the following topics: recognizing phishing emails and websites, choosing strong passwords, security of mobile devices and public Wi-Fi networks, and security principles of remote work. It's also useful to periodically test employees' knowledge, for example, by conducting phishing attack simulations.

- Security assessment

Regular security assessment activities, such as penetration testing, help to promptly identify gaps in the cybersecurity system. The most effective option is APT attack simulation (red teaming). This involves specialists simulating possible actions of APT groups, starting with detailed reconnaissance, scanning the company's external perimeter, and collecting information useful for the attack from public sources. When preparing to simulate the active phase of the attack, possible vectors are considered, such as penetration through the external perimeter or using phishing. Additional tools may be developed and applied, mimicking the behavior of malware. Simulating APT attacks is extremely useful in assessing the security of critical infrastructure.

Independent security assessment programs (industry bug bounty) are also worth considering. They help organizations build a process for continuous analysis of service security and optimize their security spending.

## Brief description of APT groups

### APT10

APT10 has been active since at least 2006. The group became widely known for the long-term cybercampaign Operation Cloud Hopper, aimed at IT providers worldwide to steal intellectual property and use their infrastructure for further attacks. Currently, the group's targets are the aerospace industry, mechanical engineering, telecommunications, and pharmaceutical companies. In attacks, the group uses both publicly available and proprietary malware.

### APT23

Activity has been observed since 2011. The group attacks the sectors of government administration, healthcare, transportation, high-end technology, as well as military-industrial complexes in Taiwan, the Philippines, and Hong Kong. Trend Micro experts also note navy authorities, military hospitals, and the national bank among the victims. The group uses a variety of malware, including the USBferry tool, designed to steal data via USB drives.

### APT32

The group has been operating since at least 2012. According to various researchers, it operates in the interests of the Vietnamese government. It attacks government and corporate networks in East and Southeast Asian countries. Vietnamese organizations and human rights defenders often become the targets of attacks. For initial penetration, the group frequently uses watering hole and spear-phishing techniques. The group uses a unique set of malware combined with publicly available tools.

### APT40

According to researchers, this group is of Chinese origin. Active since at least 2009. Targets industries such as machine engineering, transportation, defense, science, and education. Typically attacks countries of strategic importance to the Belt and Road Initiative. Uses its own malware and open-source tools, most of which are also used by other APT groups.

### APT41

Researchers believe that APT41 is sponsored by China for cyberespionage purposes and also conducts financially motivated attacks for its own gain. Cybercriminal activity has been observed since 2012. Victims span numerous industries, including government organizations, telecommunications, software development companies, computer hardware manufacturers, and other sectors worldwide. For initial penetration, the group uses phishing, supply chain attacks, and watering hole attacks.

### Dark Pink

This group's first activity was noticed in mid-2021. Most attacks have targeted organizations in the Asia-Pacific region, but incidents have also been recorded in European countries. Confirmed victims include numerous organizations in Southeast Asian countries. To steal information, the attackers used legitimate tools and their own malware, such as TelePowerBot, KamiKakaBot, Cucky, and Ctealer.

### Earth Estries

This group has been active since 2020. Victims of Earth Estries include government institutions and technology companies in the Philippines, Taiwan, Malaysia, South Africa, Germany, and the USA. Trend Micro researchers believe that the group's tactics and techniques indicate a connection with the FamousSparrow group. The group's arsenal includes various backdoors and infostealers, including Zingdoor, TrillClient, and HemiGate.

**Earth Krahang**

This group's activity has been tracked since 2022. Trend Micro researchers believe the group closely collaborates with the Earth Lusca group and may be associated with the Chinese company I-Soon. Attacks are mainly aimed at government organizations in Southeast Asia, but other countries have also been targeted. The group uses phishing, exploits web server vulnerabilities, and employs malware such as PlugX and ShadowPad.

**Earth Lusca**

According to researchers, the group has been active since at least 2019 and may be linked to China. The attacks are primarily conducted for espionage purposes and target organizations worldwide. The group's targets include government institutions, educational organizations, religious movements, pro-democracy groups, media, as well as casinos and cryptocurrency projects.

**Evasive Panda**

A Chinese-speaking APT group active since at least 2012. Attacks organizations in Africa, East, and Southeast Asia, including government entities. Conducts espionage against private individuals. Has a wide range of tools and uses various initial penetration techniques, including supply chain and watering hole attacks.

**Gallium**

The group attacks telecommunications, financial institutions, and government organizations in Southeast Asia, Europe, and Africa. Activity has been observed since 2012. Researchers suggest that Gallium has Chinese origins.

**Gelsemium**

The group has been operating since 2014 at least. Targets government, educational, and religious institutions, as well as electronics manufacturers, in East and Southeast Asia, Africa, and the Middle East. The group uses both rare and publicly available tools in its attacks.

**GhostEmperor**

According to researchers, this group has Chinese origins. Activity is related to cyberespionage and has been tracked since 2021. GhostEmperor mainly targets organizations in Southeast Asia, although their attacks may extend to other regions. For initial penetration, the group uses phishing emails and exploits vulnerabilities in Microsoft Exchange servers. Uses a previously unknown Windows kernel-mode rootkit.

**Goblin Panda**

Researchers from CrowdStrike believe this group operates in the interests of China. Activity has been observed since 2013. The activity is related to espionage in Southeast Asian countries, with a particular interest in Vietnam. Targets government organizations, the military-industrial complex, and the energy sector. The group has both self-developed tools and various remote access trojans.

**Lancefly**

This group has been active since at least 2020, specializing in cyberespionage. Lancefly targets government organizations, aviation, and telecommunications companies in South and Southeast Asia. The group's arsenal includes its own backdoor, Merdoor, which enables the attackers to directly interact with infected devices, monitor activities on them, and capture keystrokes. The cybercriminals also use the trojans PlugX and ShadowPad. Researchers have not yet established the exact origin of the group.

**Mustang Panda**

Crowdstrike researchers believe that this group has Chinese origins. Its activity has been recorded since at least 2014. Initially, it attacked countries neighboring China. Since 2022, they have actively attacked European countries, primarily embassies and diplomatic missions. The group uses tracking pixels in phishing campaigns. They have various tools in their arsenal, including Cobalt Strike and modified versions of PlugX, as well as self-developed malware.

**Naikon**

The group has been active since at least 2015, targeting government, military, and private organizations in Southeast Asia. Researchers from ThreatConnect link Naikon to the People's Liberation Army of China. The attackers use both self-developed and publicly available malware, exploiting known vulnerabilities. It has been established that in each targeted country, the group has its own operator—a person adapting the attack to various specific features of the particular region.

**Sharp Panda**

According to researchers from Check Point, this group has Chinese origins. It targets government organizations in Southeast Asia for cyberespionage. Additionally, the group has conducted campaigns aimed at high-ranking officials from G20 countries.

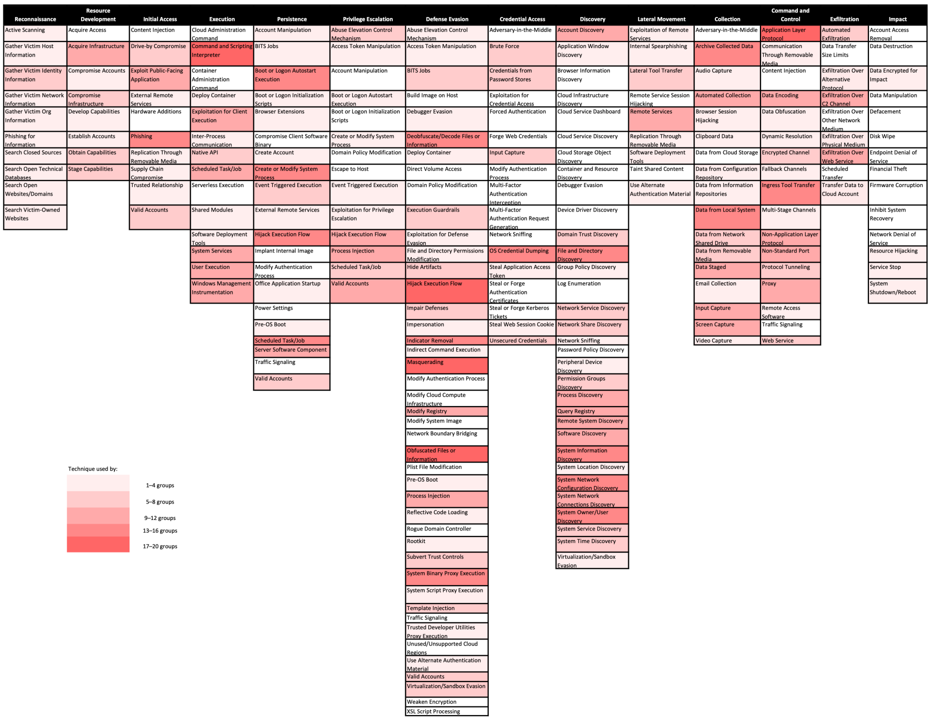
**SideWinder**

Many researchers believe this cybercriminal group to have Indian origins. Active since at least 2012. SideWinder mainly targets government, military, and commercial entities in Southeast and South Asia. Since 2019, it has shown particular interest in military facilities and targets in Pakistan. For initial access, the attackers primarily use phishing.

**ToddyCat**

According to some researchers, this group is linked to China. The group's activity has been tracked since 2020. In its attacks, it uses various tools, including two previously unknown ones named Samurai and Ninja. The group's victims include government organizations, telecommunications companies, and defense sector enterprises in Asia and Europe.

## Heat map of APT tactics and techniques in Southeast Asia



| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion |
|---|---|---|---|---|---|---|
| Active Scanning | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism |
| Gather Victim Host Information | Acquire Infrastructure | Drive-by Compromise | Command and Scripting Interpreter | BITS Jobs | Access Token Manipulation | Access Token Manipulation |
| Gather Victim Identity Information | Compromise Accounts | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution | Account Manipulation | BITS Jobs |
| Gather Victim Network Information | Compromise Infrastructure | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts | Boot or Logon Autostart Execution | Build Image on Host |
| Gather Victim Org Information | Develop Capabilities | Hardware Additions | Exploitation for Client Execution | Browser Extensions | Boot or Logon Initialization Scripts | Debugger Evasion |
| Phishing for Information | Establish Accounts | Phishing | Inter-Process Communication | Compromise Client Software Binary | Create or Modify System Process | Deobfuscate/Decode Files or Information |
| Search Closed Sources | Obtain Capabilities | Replication Through Removable Media | Native API | Create Account | Domain Policy Modification | Deploy Container |
| Search Open Technical Databases | Stage Capabilities | Supply Chain Compromise | Scheduled Task/Job | Create or Modify System Process | Escape to Host | Direct Volume Access |
| Search Open Websites/Domains | | Trusted Relationship | Serverless Execution | Event Triggered Execution | Event Triggered Execution | Domain Policy Modification |
| Search Victim-Owned Websites | | Valid Accounts | Shared Modules | External Remote Services | Exploitation for Privilege Escalation | Execution Guardrails |
| | | | Software Deployment Tools | Hijack Execution Flow | Hijack Execution Flow | Exploitation for Defense Evasion |
| | | | System Services | Implant Internal Image | Process Injection | File and Directory Permissions Modification |
| | | | User Execution | Modify Authentication Process | Scheduled Task/Job | Hide Artifacts |
| | | | Windows Management Instrumentation | Office Application Startup | Valid Accounts | Hijack Execution Flow |
| | | | | Power Settings | | Impair Defenses |
| | | | | Pre-OS Boot | | Impersonation |
| | | | | Scheduled Task/Job | | Indicator Removal |
| | | | | Server Software Component | | Indirect Command Execution |
| | | | | Traffic Signaling | | Masquerading |
| | | | | Valid Accounts | | Modify Authentication Process |
| | | | | | | Modify Cloud Compute Infrastructure |
| | | | | | | Modify Registry |
| | | | | | | Modify System Image |
| | | | | | | Network Boundary Bridging |
| | | | | | | Obfuscated Files or Information |
| | | | | | | Plist File Modification |
| | | | | | | Pre-OS Boot |
| | | | | | | Process Injection |
| | | | | | | Reflective Code Loading |
| | | | | | | Rogue Domain Controller |
| | | | | | | Rootkit |
| | | | | | | Subvert Trust Controls |
| | | | | | | System Binary Proxy Execution |
| | | | | | | System Script Proxy Execution |
| | | | | | | Template Injection |
| | | | | | | Traffic Signaling |
| | | | | | | Trusted Developer Utilities Proxy Execution |
| | | | | | | Unused/Unsupported Cloud Regions |
| | | | | | | Use Alternate Authentication Material |
| | | | | | | Valid Accounts |
| | | | | | | Virtualization/Sandbox Evasion |
| | | | | | | Weaken Encryption |
| | | | | | | XSL Script Processing |

| Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|
| Adversary-in-the-Middle | Account Discovery | Exploitation of Remote Services | Adversary-in-the-Middle | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Brute Force | Application Window Discovery | Internal Spearphishing | Archive Collected Data | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Credentials from Password Stores | Browser Information Discovery | Lateral Tool Transfer | Audio Capture | Content Injection | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking | Automated Collection | Data Encoding | Exfiltration Over C2 Channel | Data Manipulation |
| Forced Authentication | Cloud Service Dashboard | Remote Services | Browser Session Hijacking | Data Obfuscation | Exfiltration Over Other Network Medium | Defacement |
| Forge Web Credentials | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Dynamic Resolution | Exfiltration Over Physical Medium | Disk Wipe |
| Input Capture | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Encrypted Channel | Exfiltration Over Web Service | Endpoint Denial of Service |
| Modify Authentication Process | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository | Fallback Channels | Scheduled Transfer | Financial Theft |
| Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material | Data from Information Repositories | Ingress Tool Transfer | Transfer Data to Cloud Account | Firmware Corruption |
| Multi-Factor Authentication Request Generation | Device Driver Discovery | | Data from Local System | Multi-Stage Channels | | Inhibit System Recovery |
| Network Sniffing | Domain Trust Discovery | | Data from Network Shared Drive | Non-Application Layer Protocol | | Network Denial of Service |
| OS Credential Dumping | File and Directory Discovery | | Data from Removable Media | Non-Standard Port | | Resource Hijacking |
| Steal Application Access Token | Group Policy Discovery | | Data Staged | Protocol Tunneling | | Service Stop |
| Steal or Forge Authentication Certificates | Log Enumeration | | Email Collection | Proxy | | System Shutdown/Reboot |
| Steal or Forge Kerberos Tickets | Network Service Discovery | | Input Capture | Remote Access Software | | |
| Steal Web Session Cookie | Network Share Discovery | | Screen Capture | Traffic Signaling | | |
| Unsecured Credentials | Network Sniffing | | Video Capture | Web Service | | |
| | Password Policy Discovery | | | | | |
| | Peripheral Device Discovery | | | | | |
| | Permission Groups Discovery | | | | | |
| | Process Discovery | | | | | |
| | Query Registry | | | | | |
| | Remote System Discovery | | | | | |
| | Software Discovery | | | | | |
| | System Information Discovery | | | | | |
| | System Location Discovery | | | | | |
| | System Network Configuration Discovery | | | | | |
| | System Network Connections Discovery | | | | | |
| | System Owner/User Discovery | | | | | |
| | System Service Discovery | | | | | |
| | System Time Discovery | | | | | |
| | Virtualization/Sandbox Evasion | | | | | |

Technique used by:

1–4 groups

5–8 groups

9–12 groups

13–16 groups

17–20 groups

Download heat map