Kaspersky 2019 APT Report: Cyberspying groups hunt intelligence in SEA

By Digital News Asia

Published: 2020-03-01 · Archived: 2026-04-05 17:57:15 UTC

- ***Geopolitics is one of main factors that shape the SEA cyber threat landscape***
- ***Cooperation best way to get upper hand against cyberespionage groups***

Kaspersky's investigations into APT attacks targeting the region last year show the main attack motivation as being economical and geopolitical intelligence gathering.

On 27 Feb Kaspersky unmasked the cybercriminal groups who operated and are still operating in Southeast Asia (SEA). Findings of the cybersecurity company reveal a major trend in SEA's threat landscape – increased activity of major Advanced Persistent Threat (APT) groups waging sophisticated cyberespionage.

APT are complex attacks, consisting of many different components, including penetration tools (spear-phishing messages, exploits etc.), network propagation mechanisms, spyware, tools for concealment (root/boot kits) and other, often sophisticated techniques, all designed with one objective in mind: undetected access to sensitive information. APTs target *any* sensitive data; you don't have to be a government agency, major financial institution or energy company to become a victim. Even small retail organizations have sensitive client information on record; small banks operate remote service platforms for customers and businesses of all sizes process and hold payment information that is dangerous in the wrong hands. As far as attackers are concerned, size doesn't matter: it's all about the information. Even small companies are vulnerable to APTs

Hungry for intelligence and data, 2019 was a busy year for cybercriminals as they launched new attack tools, including spying through mobile malware to achieve their goal to steal information from government and military entities and organisations across the region.

“Geopolitics is one of the main factors that shape the cyber threat landscape in Southeast Asia. A number of our investigations into APT attacks targeting the region last year show the main attack motivation as being economical and geopolitical intelligence gathering. Inevitably the main victims are mostly government organisations, diplomatic entities, and political parties,” says Vitaly Kamluk ***(pic, right)***, Director for Global Research and Analysis Team (GReAT) Asia Pacific at Kaspersky.

“The region is home to countries with very diverse ethnicities, political views, and economic development. This shapes the diversity of cyberattacks in Southeast Asia. What is common for most of the countries is the intent to develop capacity to launch cyberattacks. We see how APT attackers have been running their operations for years, developing better tools, becoming more attribution-cautious, technically more advanced and eager to go for higher targets,” explains Kamluk.

“Our findings on the threat landscape of SEA last year revealed a growing need for both public and private institutions to beef up their cybersecurity capabilities. These various groups, with covert infiltration schemes and attack methods, waging espionage campaigns in the region show that security has to go beyond the usual anti-virus and firewall solutions. At Kaspersky, we believe in a cybersecurity structure founded on in-depth and real-time threat intelligence,” says Yeo Siang Tiong, General Manager for Southeast Asia at Kaspersky.

“Combining machine learning and human knowledge through our GReAT researchers, we are currently monitoring over 100 APT groups and operations globally, regardless of their origin,” says Kamluk. “Our organic, technical reports give companies, governments, and non-commercial organizations a comprehensive look at the current threat landscape, which eventually guide them in mapping their defences better. We also advocate

information sharing in the industry, like the intelligence-sharing pact we renewed last year with the Interpol, as we believe that cooperation is the best way to get the upper hand against these cyberespionage groups," he adds.

In the following, Kaspersky further shares the main APT groups and the types of malware which defined the threat landscape in SEA in 2019 until 2020.

FunnyDream

(Targets in SEA: Malaysia, Philippines, Thailand, Vietnam)

In early 2020 Kaspersky published a report based on its investigation of an ongoing attack campaign called "FunnyDream". This Chinese-speaking actor has been active for at least a few years and possesses different implants with various capabilities.

Since mid-2018, researchers at Kaspersky saw continuing high activity from this threat actor and among their targets were a number of high-level government organisations as well as some political parties from various Asian countries including the Philippines, Thailand, Vietnam, and Malaysia.

The campaign comprises a number of cyber espionage tools with various capabilities. As of the latest monitoring of the global cybersecurity company, FunnyDream's espionage attacks are still ongoing.

Kaspersky Threat Portal users have access to the most updated information on this actor.

Platinum

(Targets in SEA: Indonesia, Malaysia, Vietnam)

Platinum is one of the most technologically advanced APT actors with a traditional focus on the Asia Pacific (APAC) region. In 2019, Kaspersky researchers discovered Platinum using a new backdoor which was dubbed "Titanium", named after a password to one of the self-executable archives.

Titanium is the final result of a sequence of dropping, downloading and installing stages. The malware hides at every step by mimicking common software — protection related, sound drivers software, DVD video creation tools.

Diplomatic and government entities from Indonesia, Malaysia, and Vietnam were identified among the victims of this new sophisticated backdoor discovered from Platinum actor.

Cycldek

(Targets in SEA: Laos, Philippines, Thailand, Vietnam)

Another APT group which targeted SEA countries in 2019 was the Chinese-speaking actor called "Cycldek". Although the main targets of Cycldek's new activities suggest extensive foothold in government networks in Vietnam and Laos, Kaspersky has also observed 3% of the group's targets were from Thailand. The global cybersecurity company has also identified one victim in the Philippines during its 2018-2019 wave of attacks.

Cycldeck is also known as Goblin Panda and is infamous for conducting information theft and espionage across the government, defence, and energy sectors in the region using PlugX and HttpTunnel malware variants.

HoneyMyte

(Targets in SEA: Myanmar, Singapore, Vietnam)

In 2019, Kaspersky published a number of reports regarding attacks from HoneyMyte threat actor. This group started a new spear phishing campaign in mid-2018 which continued through 2019 and targeted different government organisations from Central and SEA countries with victims also remotely located in other countries and regions. Among these remote victims, Kaspersky has detected entities based in Singapore to be targeted by this wave of attacks.

Government organisations of Myanmar and Vietnam were also among the main targets of HoneyMyte which uses malicious Lnk samples, PlugX, powershell and .Net malware.

Finspy

(Targets in SEA: Indonesia, Myanmar, Vietnam)

FinSpy is spyware for Windows, macOS, and Linux that is sold legally. It can be installed on both iOS and Android with the same set of functions available for each platform. The app gives an attacker almost total control over the data on an infected device.

The malware can be configured individually for each victim and in such a way that provides the attack mastermind with detailed information about the user, including contacts, call history, geolocation, texts, calendar events, and more. It can also record voice and VoIP calls, and intercept instant messages.

It has the ability to eavesdrop on many communication services — WhatsApp, WeChat, Viber, Skype, Line, Telegram, as well as Signal and Threema. Besides messages, FinSpy extracts files sent and received by victims in messaging apps, as well as data about groups and contacts.

In early 2019, Kaspersky reported about the new version of FinSpy iOS implant and later in the year detected new Android implant from this cyberespionage solution provider in the wild and another RCS (Remote Control System) implant from another company providing cyberespionage solutions.

According to Kaspersky's telemetry, individuals in Indonesia, Myanmar, and Vietnam were found among the targets of these two types of malware.

PhantomLance

(Targets in SEA: Indonesia, Malaysia, Vietnam)

Another mobile malware which affected several nations in SEA is PhantomLance, a long-term espionage campaign with spyware Trojans for Android deployed in different application markets including Google Play. After discovering samples, Kaspersky has informed Google who has removed it as well.

RCS (Remote Control System) developed by a company providing cyberespionage solutions were both found targeting Indonesian, Malaysian, and Vietnamese entities.

Zebrocy

(Targets in SEA: Malaysia, Thailand)

Zebrocy is a Russian-speaking APT which initially shared limited infrastructure, targets, and interests with Sofacy. It also shared malware code with past BlackEnergy/Sandworm; and targeting, and later very limited infrastructure with more recent BlackEnergy/GreyEnergy.

The group's Nimcy backdoor developed in Nimrod/Nim programming language targeted Malaysian and Thai entities. Nimcy is the new addition to Zebrocy's collection of languages to develop their main functionalities in new backdoors.

In order to avoid falling victim to a targeted attack by a known or unknown threat actor, Kaspersky researchers recommend implementing the following measures:

- Provide your Security Operations Center (SOC) team with access to the latest threat intelligence, to keep up to date with the new and emerging tools, techniques and tactics used by threat actors and cybercriminals.
- For endpoint level detection, investigation and timely remediation of incidents, implement EDR solutions such as Kaspersky Endpoint Detection and Response.
- In addition to adopting essential endpoint protection, implement a corporate-grade security solution that detects advanced threats on the network level at an early stage, such as Kaspersky Anti Targeted Attack Platform.
