FireEye
SECURITY REIMAGINED

Singtel

SPECIAL REPORT

# SOUTHEAST ASIA: CYBER THREAT LANDSCAPE

# CONTENTS

# INTRODUCTION

Advanced persistent threat (APT) actors remain one of the biggest challenges for companies and governments alike. Breaches continue while firms invest in cyber security and national governments develop new cyber strategies.

This report discusses trends in the cyber security environment in Southeast Asia from January to June 2015. We will review some recent cases of attempted breaches on companies and governments, and provide an update on a group we first identified in 2013 as APT.Nineblog.

Key Findings:

- In the first half of 2015, FireEye products helped 29 percent of our customers in Southeast Asia detect malware used by APT groups and other cyber threat actors targeting their networks.
- Countries in the region face the risk that territorial disputes, particularly across the South China Sea, will expand into cyber operations.

**Figure 1:**
**Southeast Asian countries with FireEye customers.**


[1] For this report we identify Southeast Asia as Thailand, Malaysia, Vietnam, Brunei, the Philippines, Indonesia, and Singapore.

# CYBER TRENDS IN SOUTHEAST ASIA

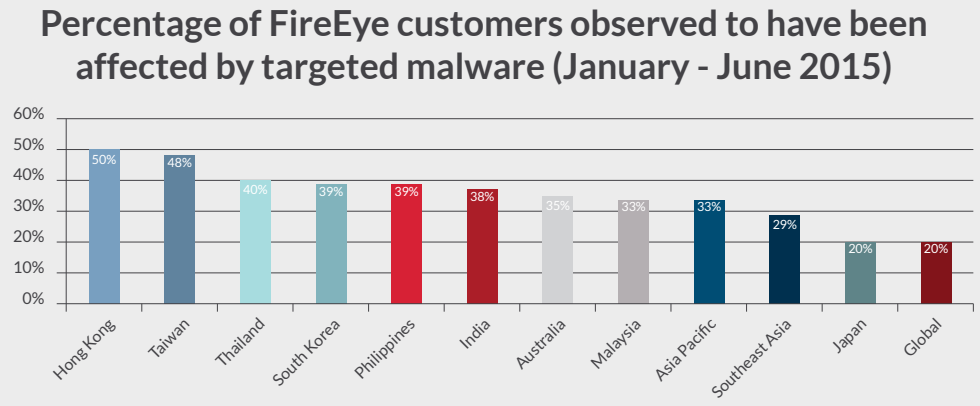
Southeast Asia faces numerous unique challenges with regards to cyber security. The region's extraordinary pace of economic development and growing military expenditures constitute two major reasons why APT actors target governments and businesses. APT groups seek to obtain intelligence to provide their sponsoring government with diplomatic, military, and economic advantages across the negotiating table or on the seas.

Countries in the region continue to face the risk that persistent territorial disputes, particularly across the South China Sea, will expand into cyber operations. China, the Philippines, Brunei, Vietnam, Taiwan, and Malaysia all contest territory in the area. These disagreements have lingered for decades in some cases. Rival governments often employ APT groups to conduct cyber espionage to obtain valuable political or military intelligence. We routinely observe APT groups stealing information that deals with South China Sea disputes and their economic effects from the networks of governments and companies involved.

During the first half of 2015, about 29 percent of our customers in Southeast Asia detected malware associated with APT groups.[2] That remains higher than our global average of about 20 percent.

Thailand and the Philippines are among those countries in Southeast Asia most often targeted with malware associated with APT groups.

**Figure 2:**




Southeast Asia includes customers in Thailand, Vietnam, Malaysia, the Philippines, Brunei, Indonesia, and Singapore.
Asia Pacific includes customers across Asia, from India to Australia, Japan to New Zealand.

### Gaining Global Insights into Cyber Threats

FireEye Dynamic Threat Intelligence (DTI) allows us to gain insights into cyber threat activity by gathering real-time information about the latest cyber threats worldwide. DTI uses millions of FireEye sensors to perform more than 50 billion analyses over 400,000 unique malware samples every day. Through these sensors and the FireEye Managed Defense and incident response services, FireEye DTI can develop a picture of the current threat landscape.

[2] We use "malware associated with APT groups" and "APT and targeted malware alerts" interchangeably in this report. The terms refer to malware detected at customer locations that FireEye threat intelligence has characterized as being associated with APT activity. These statistics are generated by customers who have opted to share anonymized data with FireEye.

## The Most Prevalent Malware in Southeast Asia

The top five targeted malware alerts in first half of 2015 in Southeast Asia were:

- Kaba (aka SOGU)[3]
- LV (aka NJRAT)
- RegSubDat (aka NOISEPACK)
- CANNONFODDER
- Lecna (aka BACKSPACE)

Detections of LV and Kaba constitute over 30 percent of all APT malware hits in Southeast Asia and globally. Kaba is closely associated with China-based cyber threat groups. RegSubDat, CANNONFODDER, Lecna, and Backdoor.APT.Page are among the top threats detected in Southeast Asia, but are not as frequently observed globally.

**Figure 3:** APT and Targeted Malware Detections in Southeast Asia January - June 2015

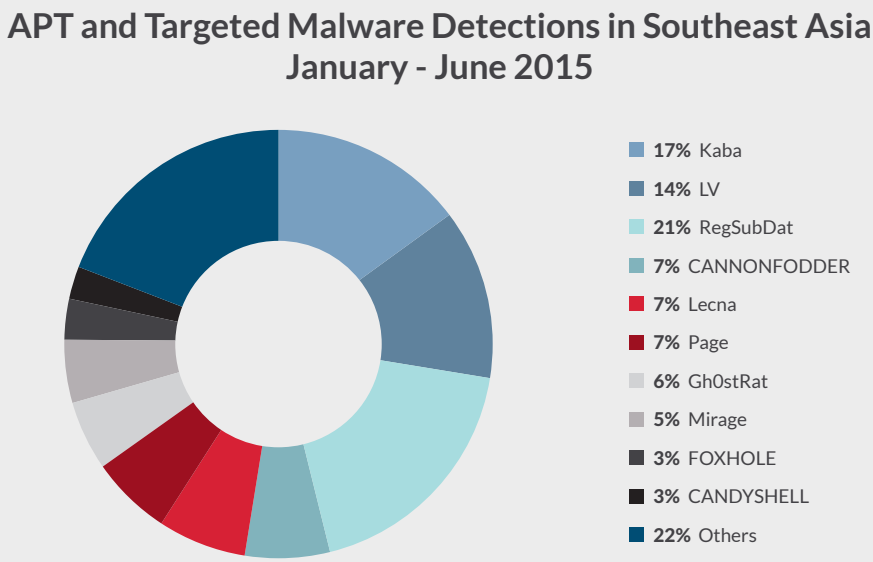
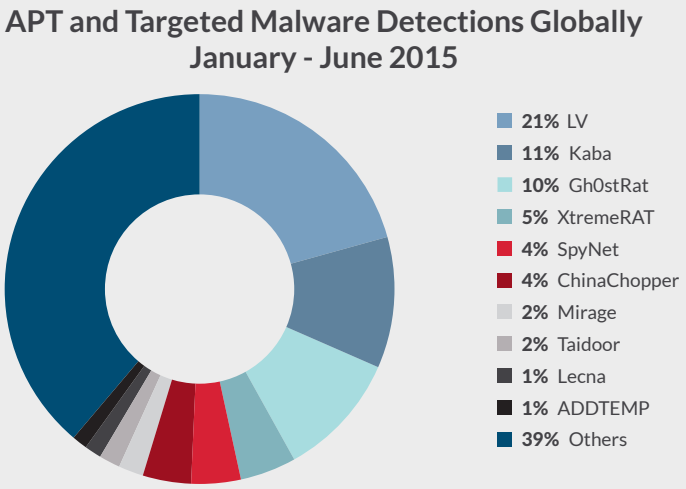



**Figure 4:** APT and Targeted Malware Detections Globally January - June 2015




[3] Additional information on the malware in this section is available in the Appendix.

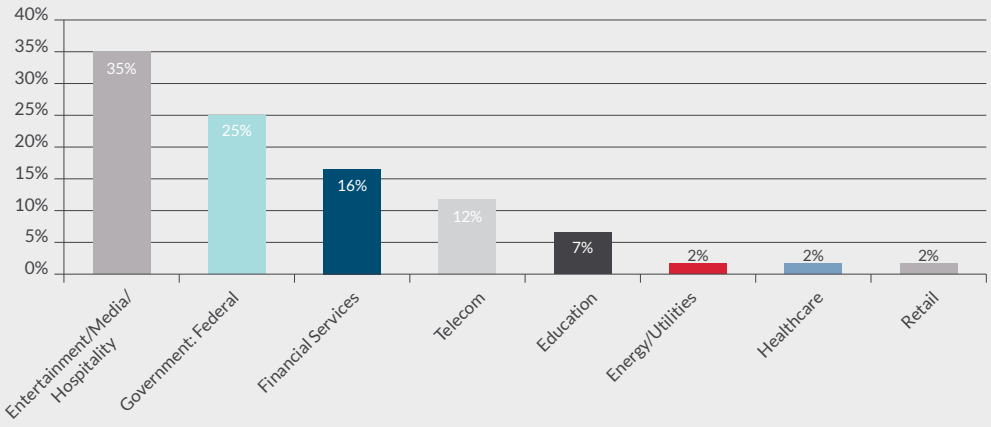
## Southeast Asia's Leading Industries Attracting APT Malware

More than one-third of malware detections associated with APT groups originated from customers in the Entertainment/Media/Hospitality industry. We have observed at least 12 APT groups target this industry globally. APT groups likely target media companies because of their role in shaping public opinion. In addition, the sponsors of APT groups often seek early warning about reporting that is critical of their government.

Governments in the region continue to be among the most targeted by APT malware in Southeast Asia—nearly 25 percent. Many of these could be from rival governments. We have observed at least four APT groups targeting regional or state governments (subdivisions internal to a single country) and at least 13 APT groups targeting national government organizations.

**Figure 5:**

### Top Industry Verticals in Southeast Asia by Percentage Share of APT and Targeted Malware in Southeast Asia January - June 2015




These statistics do not account for the number of appliances at a customer site or the number of FireEye customers in a given industry.

# REGIONAL CASE STUDIES

## Media Companies Subject to Spear Phishing

In early 2015, suspected China-based cyber threat actors targeted a media firm in Asia and attempted to compromise it via a malicious phishing email. The email contained an attachment that deployed a MONKEYTILT backdoor.
The media company may have been targeted because it had published commentary supportive of an opposition group. The cyber threat group may also have sought information that would help authorities monitor public opinion and gain advanced notice of articles that portrayed the government negatively.

## Targeting Government Organizations Through Foreign Nationals

In early 2015, we observed continuous attempts by a suspected China-based cyber threat actor to compromise a governmental organization in Southeast Asia with a malicious software backdoor that we call DIRTNAP. Another iteration of this campaign also targeted foreign nationals working with the government. The foreign nationals received email messages with a Microsoft Word attachment containing an embedded Visual Basic for Applications macro that dropped the DIRTNAP sample once opened.

## State-Owned Banks in the Crosshairs

FireEye has observed the CANNONFODDER backdoor being used consistently throughout the Southeast Asia region during the past year. We believe China-based threat groups use CANNONFODDER to collect political and economic intelligence. In early and mid-2015, we observed CANNONFODDER implants beacon from a Southeast Asian state-owned bank. Targeting this bank would provide the threat actors insights into the country's growth priorities and likely a competitive edge in business.

In addition to the bank, we have seen other instances of the malware. In late 2014, we identified CANNONFODDER implants beaconing from an Asian telecommunications company. In mid-2014, we observed cyber threat actors sending spear phishing emails with malicious attachments to employees of an Asian government. Once opened, the attachments installed the CANNONFODDER implant.

[4] Additional information on this malware is available in the Appendix.
[5] Additional information on this malware is available in the Appendix.
[6] Additional information on this malware is available in the Appendix.

# APT.NINEBLOG RETURNS

FireEye has been tracking ongoing activity associated with a unique and relatively stealthy group we first identified in 2013 using the name "APT.NineBlog." The name NINEBLOG refers to a specific backdoor used by the threat group; some versions of the backdoor use the string 'nineblog' in their command and control (CnC) URI path.[7]

We have observed this group targeting organizations primarily in South Asia and the Middle East. The threat group is notable because it employs Visual Basic Scripts (VBScripts) as a backdoor, a tactic we do not often observe. The group can maintain a low profile probably because the VBScripts are small and stealthy in their execution. The NINEBLOG malware is difficult to detect because the VBScripts are encoded and the actors employ SSL network communications. We have observed intermittent activity from this group since we first identified it in 2013, and we saw a spike in activity during mid-2015.

We assess that one of the probable targets of the group's 2015 campaign is a Southeast Asian government, based on the specificity of some of the decoy documents.



## Staying Under the Radar

From mid-2013 through mid-2015, FireEye observed this group deploying numerous exploit documents. The documents were most likely used in spear phishing campaigns targeting organizations in South Asia. The group primarily uses malicious Microsoft Office documents that exploit a variety of vulnerabilities (including CVE-2012-0158, CVE-2014-1761, and CVE-2015-5119, a leaked HackingTeam exploit) to deliver an encoded VBScript backdoor.[8] We only observed this group use the CVE-2015-5119 exploit after it was made public. This may indicate that the group does not develop or obtain its own zero-day exploits, but is opportunistic and capable of adapting disclosed exploits for its own use.

When an exploit document is opened, it drops a decoy document and executes a small Portable Executable (PE) dropper. The dropper has two embedded VBScripts, one of which is encoded. The first script deletes the PE dropper file and itself. The second, encoded VBScript is a backdoor that we call NINEBLOG.

We noticed the decoded VBScript backdoors from recent activity were nearly identical (with some small changes) to the first NINEBLOG variants we observed in 2013. The minimal code changes may be due to the fact that the encoding provides enough obfuscation to prevent detection, allowing the core functionality of the backdoor to remain the same.

Additionally, newer variants of the VBScript include some code enhancements. The differences in functionality between the first variant we observed and newer variants can be viewed in the table below.

[7] Haq, Thoufique and Nart Villeneuve. "The Curious Case of Encoded VB Scripts: APT.NineBlog" 5 August 2013. https://www.fireeye.com/blog/threat-research/2013/08/the-curious-case-of-encoded-vb-scripts-apt-nineblog.html.

[8] Hacking Team is an Italian software development firm that develops tools – ostensibly sold to governments and law enforcement organizations – that can be used to remotely monitor victim computers. The company suffered a breach in mid-2015 that resulted in a massive disclosure of sensitive internal documents, including information on several previously undisclosed zero-day vulnerabilities.

| Functionality | First Identified Variant | Newer Variants |
|---|---|---|
| Persistence | Scheduled task and autorun key | Startup folder shortcut |
| Hide | Sets hidden attribute on working directory and subfiles | Sets hidden attribute on working directory |
| Collect System Information | Gets user name, computer name, and a list of processes | Gets network adapter info, user name, computer name, a list of processes, and the date |
| Anti-Analysis/Anti-Forensics | None | Exits if running processes found for process monitor, file monitor, wireshark, or windbg. Also deletes the Recent LNK file for the persistent copy of itself. Some variants also detect virtual machines. |
| Network Function | Identical (same User-Agent, same referrer) | Identical (same User-Agent, same referrer) |
| Login | Uses a login password and loops indefinitely until successful login | Uses a login password (same as earlier versions) and loops indefinitely until successful login |
| Command Execution | Upon receiving a command, breaks loop and executes in local scope | Uses nested "while" loops to stay in command mode after login and executes successfully received commands in global scope |
| Working Directory | Uses two working directories, `%APPDATA%\RECYCLER` and `%APPDATA%\Microsoft\Windows`, to which it deploys hidden, persistent copies of itself | Uses one working directory, `%APPDATA%\Microsoft\Protect`, to which it deploys a hidden, persistent copy of itself |

Upon decoding the VBScript backdoors we can observe the code used to implement these new capabilities, such as the anti-analysis technique seen below:

```
If(InStr(lall,"wireshark")>0 Or InStr(lall,"processmonitor")>0 Or
InStr(lall,"filemonitor")>0 Or InStr(lall,"windbg")>0)Then
     WScript.Quit
End If
```

In addition to the anti-analysis techniques, the group has used SSL communications since we first identified this activity in 2013. The use of encrypted SSL traffic makes it extremely difficult to develop network-based signatures to detect the malware's communications.

### Lacking Technical Details for Attribution

The group responsible for the NINEBLOG activity has used techniques that may indicate a slightly higher than average skill level and operational security. These include:

- The use of an encoded Visual Basic Script (NINEBLOG) as a backdoor, as opposed to a compiled PE binary. VBScript is less likely than a binary executable to be detected as malicious by many security products than a binary executable, and the obfuscation further masks the backdoor's purpose and functionality.
- The use of a dynamic DNS (DDNS) provider to register their CnC domains. The use of DDNS allows the group to hide the domains' registration details, and allows them to dynamically redirect their CnC communications to different IP addresses as needed.
- The use of SSL for malware CnC communications. The use of SSL for malware CnC communications makes it extremely difficult to use network-based signatures to detect malware traffic.
- The ability to identify publicly disclosed vulnerabilities and adapt them for use. This implies that the group either has some development capability, or has access to developers, tools, or forums where they can obtain weaponized documents to deploy their malware.

We assess that this group may be acting on behalf of a government based on the group's known targets and the subject matter of their phishing lures and decoy documents. However, we do not have enough information at this time to assess a possible sponsor.

# APPENDIX: DESCRIPTIONS OF TOP MALWARE FAMILIES IDENTIFIED IN SOUTHEAST ASIA AND GLOBALLY

| Backdoor.APT.Kaba | |
|---|---|
| Aliases: | APT.PlugX, SOGU |
| Summary: | SOGU is a fully featured backdoor used by APT actors that provides them with remote shell access and a custom CnC protocol. |
| Description: | The malware is a backdoor capable of file upload and download, arbitrary process execution, file system and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the CnC server with graphical access to the victim system's desktop. This backdoor provides threat actors with SQL database querying capabilities and communicates using HTTP POST requests or custom binary protocols. FireEye has observed threat actors deliver this backdoor through both strategic web compromises and phishing emails. Some phishing emails dropped decoy documents and this backdoor onto the victim system. This backdoor is frequently installed and launched by KORPLUG, a payload launcher that APT groups use. |

| Backdoor.APT.LV | |
|---|---|
| Aliases: | LV, NJRAT, Bladabindi |
| Summary: | NJRAT is a remote access trojan popular among Middle Eastern threat actors. |
| Description: | This malware is a publicly available remote access tool (RAT) capable of keystroke logging, credential harvesting, reverse shell access, file uploads and downloads, and file and registry modifications. This RAT also offers threat actors a "builder" feature, allowing them to create new variants based on configurations of CnC servers, specified filenames, options to spread via USB, designated campaign names for internal tracking, and other customization options. Additionally, this RAT gathers and sends important information about infected machines to its CnC server, possibly using a custom protocol over port 80, to include NetBIOS name, user, date, locale, and Windows OS name. Traditionally, threat actors that deploy this RAT primarily use websites hosting EXE files to propagate the malware. |

| Backdoor.APT.CANNONFODDER | |
|---|---|
| Summary: | This backdoor enables threat actors to modify, upload and download files, collect system information and grant command line access to a victim's computer. |
| Description: | This malware is capable of stealing credentials from Internet Explorer, Mozilla Firefox and Google Chrome. The malware can install a keylogger. It is capable of operating in interactive mode to allow the threat actor to perform additional investigation on the compromised system and steal data. |

| Backdoor.APT.Lecna | |
|---|---|
| Aliases: | BACKSPACE |
| Summary: | BACKSPACE is a fully featured backdoor used by APT actors that provides threat actors with remote shell access and a HTTP-based CnC protocol. |
| Description: | BACKSPACE supports commands to read, search, upload, download, and execute files; list and terminate processes; enumerate network resources; execute commands; and establish a reverse shell. Some variants of BACKSPACE are proxy-aware. Some variants may include functionality to attempt to bypass host-based firewalls. BACKSPACE variants typically contain hard-coded version information and use it to support automatic updates to the latest version. |

| Backdoor.APT.MONKEYTILT | |
|---|---|
| Summary: | This backdoor gives attackers the ability to modify, upload and download files, collect system information and grant command line access to a victim's computer. |
| Description: | This backdoor can download files, execute system commands, list directories, delete files, collect system information, and provide attackers with command line access to the infected host. It will sleep for an hour after executed, most likely as a sandbox evasion tactic. |

| Backdoor.APT.DIRTNAP | |
|---|---|
| Summary: | This Jscript-based backdoor is used by suspected China-based cyber threat actors and it communicates via Base64-encoded commands. |
| Description: | This backdoor downloader written in Jscript can download files and execute commands. It is capable of modifying the compromised system's Internet Explorer settings in the registry to disable protected mode and add the CnC server to the list of trusted sites. This malware starts by sending the victim's IP address, MAC address, hostname, and OS version in a altered Base64 encoded format to the threat actors. |

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**