

FIREEYE THREAT INTELLIGENCE

# SOUTHEAST ASIA: AN EVOLVING CYBER THREAT LANDSCAPE

MARCH 2015

SECURITY  
REIMAGINED

# CONTENTS

---

**MARCH 2015**

<b>Introduction</b>	<b>3</b>
Key Findings	4
Detecting Targeted Threats in Southeast Asia and Beyond	4
Malware Hitting Southeast Asian Targets	5
Targeted Malware, Industry Breakdown	6
Detecting Non-Targeted Threats	6
<b>Southeast Asia's Leading Industry Sectors Attract APT Actors</b>	<b>7</b>
<b>Regional Governments and Militaries: In APT Groups' Crosshairs</b>	<b>12</b>
APT Groups and the South China Sea: Territorial Disputes with a Digital Edge	12
Threat Groups Target Southeast Asian Governments and Militaries over Territorial Claims	13
APT Groups Gather Political Intelligence	13
<b>Conclusion</b>	<b>14</b>

# INTRODUCTION



**W**hile many of the headline-grabbing cyber security breaches of 2014 involved major U.S. companies, Southeast Asia quietly dealt with its share of cyber attacks. Like the U.S., companies in this region face a complex threat landscape filled with advanced cyber attackers intent on stealing corporate data and state secrets.

Advanced persistent threat (APT) actors are one of the biggest challenges for the region. Leading companies that do business in the energy, telecommunications, high-tech, finance, and transportation sectors are targets of APT groups.

## THE MISSION IS TWO-FOLD:



Steal intellectual property and inside information from leading companies.



Obtain intelligence on rival governments during long-running political disputes, especially those involving the disputed South China Sea.

This report describes malware detected at commercial and government entities across Singapore, Malaysia, Thailand, Vietnam, Philippines, Indonesia, and Brunei. It also discusses advanced threat groups behind many of these attacks and their unique motives in this region.

## KEY FINDINGS

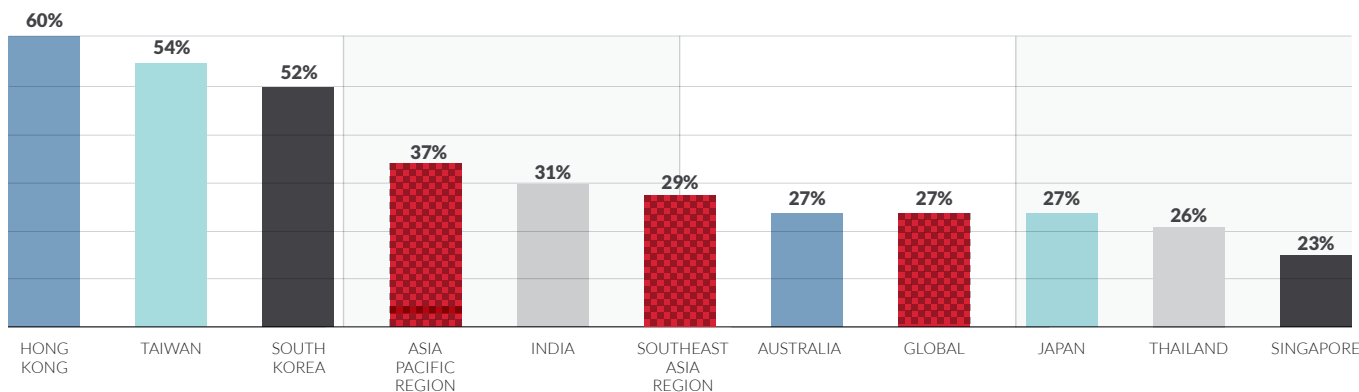
DETECTING MALWARE ACROSS SOUTHEAST ASIA	CYBER THREATS TO KEY INDUSTRIES	CYBER THREATS TO GOVERNMENTS
<p style="font-size: 48pt; text-align: center;">29%</p> <p>From July to December 2014, FireEye products helped 29 percent of our customers in Southeast Asia detect malware used by APT groups and other actors targeting their networks.</p>	<p style="text-align: center;"></p> <p>Southeast Asian companies regularly attract the interest of cyber spies and criminals looking to steal information about the region's growing industry sectors—energy, telecommunications, high-tech, transportation, and finance.</p>	<p style="text-align: center;"></p> <p>Territorial disputes in the South China Sea drive cyber espionage activity in Southeast Asia. Both government and private industries are targets of threat actors seeking to steal information in these disputes.</p>

### Detecting Targeted Threats in Southeast Asia and Beyond

From July to December 2014, FireEye products helped 29 percent of our customers in Southeast Asia detect malware used by APT groups and other attackers targeting their networks. When factoring in the rest of our Asia-Pacific clients, that percentage jumps to 37 percent—significantly higher than the global average of 27 percent. (These statistics are generated from customers who have opted to share anonymized data through FireEye.)

In the Asia-Pacific region, FireEye products **helped 37% of our customers detect malware.**

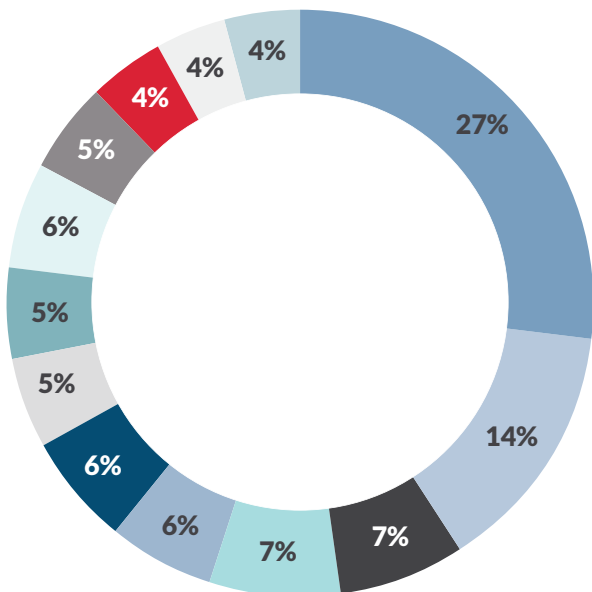
PERCENTAGE OF FIREEYE CUSTOMERS' TARGETED MALWARE ALERTS  
JULY - DECEMBER 2014



### Malware Hitting Southeast Asian Targets

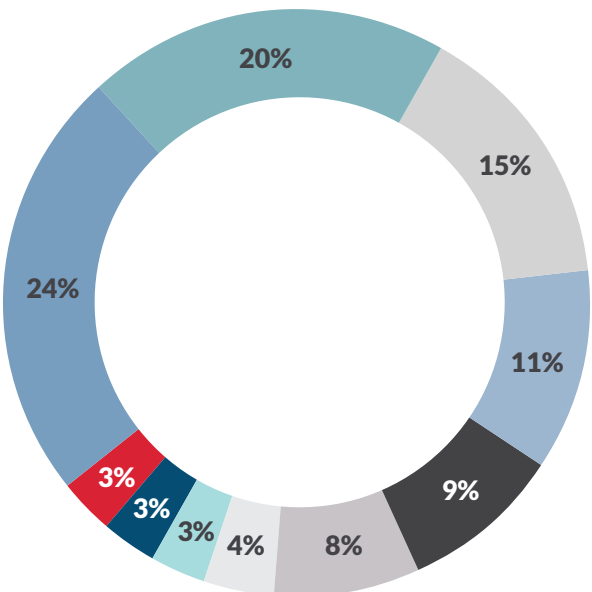
Lecna, Mirage, CannonFodder, and Leouncia were among the most frequently detected malware families.

#### APT AND TARGETED MALWARE DETECTIONS JULY - DECEMBER 2014: SOUTHEAST ASIA



Lecna	27%
Gh0STRAT	14%
Mirage	7%
Page	7%
Downloader.Pnaip	6%
CannonFodder	6%
Leouncia	5%
Kaba (aka SOGU)	5%
LV (aka NJRAT)	6%
Houdini	5%
XtremeRAT	4%
NetEagle	4%
1qaz	4%

#### APT AND TARGETED MALWARE DETECTIONS JULY-DECEMBER 2014: GLOBAL

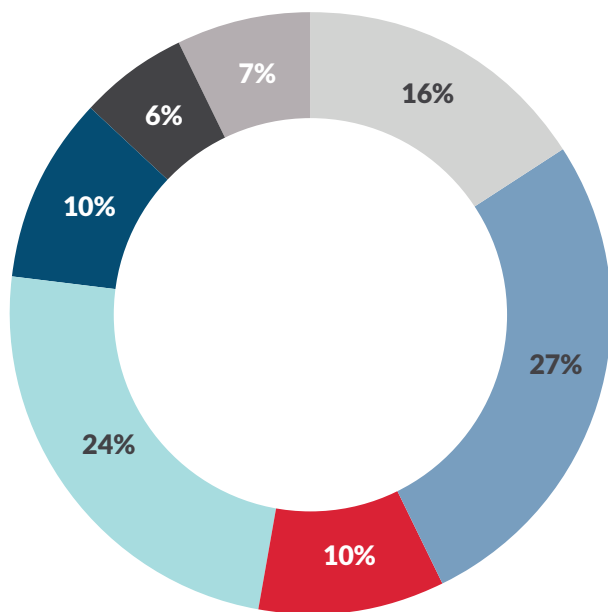


LV (aka NJRAT)	24%
Gh0STRAT	20%
Kaba (aka SOGU)	15%
SpyNet	11%
XtremeRAT	9%
ZXShell	8%
ChinaChopper	4%
PHOTO	3%
Page	3%
SAFERSING	3%

### Targeted Malware, Industry Breakdown

More than half of the targeted malware that FireEye detected in Southeast Asia came from government and telecommunications sites. (Note: these statistics do not account for the number of appliances at a customer site or the number of FireEye customers in a given industry.)

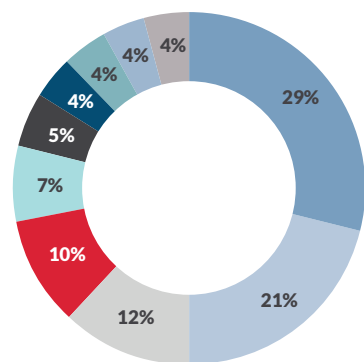
#### APT AND TARGETED MALWARE DETECTIONS BY INDUSTRY IN SOUTHEAST ASIA



Government	27%
Telecom	24%
Financial services	16%
High-tech	10%
Transportation	10%
Energy/utilities	7%
Education	6%

#### NON-TARGETED MALWARE DETECTIONS

JULY - DECEMBER 2014 GLOBALLY



Asprox	29%
Zeus	21%
Kuluoz	12%
Sality	10%
ZeroAccess	7%
Kelihos	5%
Fareit	4%
Conficker	4%
Carberp	4%
Necurs	4%

#### Detecting Non-Targeted Threats

In addition to the targeted and APT malware, organizations in the region frequently detect other threats, including banking Trojans, botnets, and other types of cyber crime.

Regionally, our customers most frequently detect Zeus (a banking Trojan) and Sality (a multi-featured Trojan) on their networks.

These commodity malware families are widely known, but dismissing the threat they pose is a mistake.

For one, they continue to evade detection by traditional security tools, making them highly effective. And advanced threat groups often use these common malware families to gain a foothold into corporate environments.

# SOUTHEAST ASIA'S LEADING INDUSTRY SECTORS ATTRACT APT ACTORS

**W**e observe APT groups routinely targeting companies in Southeast Asia to steal intellectual property (IP). We believe that once stolen, this IP often makes its way to Chinese companies. These companies can use the stolen IP to bypass years of research and development costs and get an inside edge when they deal with competitors in the region.


As increasing investments and diversifying economies spur development in the region, this growth simultaneously becomes even more attractive to APT groups.

Southeast Asia's financial sector faces a dual threat. First, standard cybercriminals are looking to steal money from them. Second, advanced threat actors are seeking sensitive financial information for a business advantage.

These industry sectors appear to be most heavily targeted by APT groups:

ENERGY	TELECOMMUNICATIONS	HIGH-TECH	TRANSPORTATION	FINANCIAL SERVICES


The following table outlines some of the targeted sectors and why APT groups would target companies' information:


Sector	Why are APT Groups Interested?	Recent Cases	Most Likely Corporate Targets
<p><b>Energy</b></p> 	<p>APT groups have long targeted U.S. and multinational corporations with strong offerings in green technology and other clean energy production. R&amp;D breakthroughs in this sector would provide tremendous value to China's energy sector, especially in light of continued international pressure to lower emissions.</p> <p>Southeast Asia is an important potential source of hydrocarbon reserves. The disputed territories in the South China Sea are estimated to contain a considerable amount of natural gas and petroleum. As rapid economic growth creates a surge in energy demand, energy resources in the disputed maritime territories have become increasingly valuable. All of these factors are likely to provoke further APT activity.</p>	<p>FireEye has observed multiple instances of APT groups breaching the networks of regional energy companies. In one case, we discovered three different threat groups attempting to gain access to the network of an oil company that conducts offshore oil exploration.</p> <p>The threat groups appeared to target affiliates of the company, as well as its infrastructure development divisions. We believe these threat groups chiefly sought data of competitive value. But they were also on the lookout for any information about the company's exploration plans and movements in the area.</p> <p>We have also observed targeted threat actors deploying malware against the networks of a major electric grid operator in the region.</p>	<ul style="list-style-type: none"> <li>• Green Energy Technology Researchers and Providers</li> <li>• Utilities</li> <li>• Oil and Gas Producers</li> <li>• Critical Infrastructure Providers and Operators</li> </ul>





Sector	Why are APT Groups Interested?	Recent Cases	Most Likely Corporate Targets
<p><b>Telecommunications</b></p> 	<p>We have observed one APT group, which we call APT5, particularly focused on telecommunications and technology companies. More than half of the organizations we have observed being targeted or breached by APT5 operate in these sectors. Several times, APT5 has targeted organizations and personnel based in Southeast Asia.</p> <p>APT5 has been active since at least 2007. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications.</p>	<p>APT5 targeted the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm’s business relationship with a national military, including inventories and memoranda about specific products they provided.</p> <p>In one case in late 2014, APT5 breached the network of an international telecommunications company. The group used malware with keylogging capabilities to monitor the computer of an executive who manages the company’s relationships with other telecommunications companies. This method allowed APT5 to collect data on topics such as:</p> <ul style="list-style-type: none"> <li>• Pricing discussions, bidding strategies and competitor pricing information</li> <li>• Schedules for contract bidding and product deployment</li> <li>• Opportunities in Asian telecommunications market</li> <li>• Business opportunities with other telecommunications companies</li> </ul> <p>APT5 also targeted the networks of some of Southeast Asia’s major telecommunications providers with Leouncia malware. We suspect that the group sought access to these networks to obtain information that would enable it to monitor communications passing through the providers’ systems.</p>	<ul style="list-style-type: none"> <li>• Regional Telecommunication Providers</li> <li>• Asia-Based Employees of Global Telecommunications and Tech Firms</li> <li>• High-Tech Manufacturing</li> <li>• Military Application Technology</li> </ul>
<p><b>High-Tech</b></p> 	<p>(This section is merged with the Telecommunications section in the original image and contains no additional text.)</p>	<p>(This section is merged with the Telecommunications section in the original image and contains no additional text.)</p>	<p>(This section is merged with the Telecommunications section in the original image and contains no additional text.)</p>

Sector	Why are APT Groups Interested?	Recent Cases	Most Likely Corporate Targets
<p><b>Transportation</b></p> 	<p>APT groups likely target the region's transportation companies to monitor the progress of high-profile projects that have the potential to fuel continued economic growth in the region.</p>	<p>In one case, a threat group that has historically focused its operations on targets in the Philippines and Malaysia spoofed the domain names of two well-known international shipping companies. One of the spoofed companies was a major commercial freight company that transports commodities around the globe. The other was a regional shipbuilding company. The plausible URLs were designed to entice potential victims within targeted industries to click.</p> <p>Another APT group targeted a major operator of container ship terminals in Southeast Asia. We suspect the group targeted the port operator to monitor its communications with regional security and military organizations that partner with the company.</p> <p>A threat group targeted a rail operator. We detected variants of the Lecna/BackSpace APT malware in the transit company's networks in early 2014.</p>	<ul style="list-style-type: none"> <li>• Shipping Companies</li> <li>• Port Operators</li> <li>• Airlines</li> <li>• Public Transit Systems</li> </ul>

Sector	Why are APT Groups Interested?	Recent Cases	Most Likely Corporate Targets
<p><b>Financial Services</b></p> 	<p>Banks in Southeast Asia appear to face a double threat. The first is the pernicious cybercrime activity we observe around the world, such as credit card fraud and the theft of banking credentials. The second threat is focused specifically on banks with a development mission in the region.</p>	<p>In one case, a threat group targeted a development bank that invests in the growth of strategic projects and industries in the region.</p> <p>In another instance, we saw two different threat groups infect the networks of a central bank. Stolen data on the country's monetary policies and banking system could be highly valuable information to someone looking to understand and anticipate broader banking and funding trends in the country and region.</p>	<ul style="list-style-type: none"> <li>• Banks</li> <li>• Companies Funding Major Regional Development Projects</li> <li>• Institutions Dealing With Monetary Policy</li> </ul>

Banks that invest in the region's strategic growth face more threats than traditional credit card fraud and financial hackers.

# REGIONAL GOVERNMENTS AND MILITARIES: IN APT GROUPS' CROSSHAIRS



**T**he APT groups that we track actively target governments and militaries for inside information into negotiations and political issues. APT groups that target governments in the region are frequently interested in topics related to the South China Sea. And they are increasingly active during times of heightened political tension or transition.

## APT Groups and the South China Sea: Territorial Disputes with a Digital Edge

FireEye routinely observes APT groups steal information dealing with South China Sea disputes and their economic effects from the networks of governments and companies involved. Control over territory in the South China Sea is a fiercely contested issue between China, the Philippines, Brunei, Vietnam, Taiwan, and Malaysia.

The territorial disputes have huge consequences for each claimant's national and economic security. The stakes are high: more than half of the world's commercial shipping passes through the South China Sea. It contains potential reserves of up to 11 billion barrels of oil, 190 trillion cubic feet of natural gas, and prime fishing areas.

Territorial disputes have lingered for decades. Along with militaries and coast guards of claimant countries, South China Sea disputes involve regional oil firms, cargo companies, and fisheries. The territory has been at the center of many international incidents, reflecting the considerable national and economic security implications for the rival claimants.

Government and military entities are frequently targeted with malware that steals sensitive security details.

### Threat Groups Target Southeast Asian Governments and Militaries over Territorial Claims

Southeast Asian government and military entities have been targeted several times in what we suspect are efforts to obtain intelligence related to territorial disputes.

- An APT group stole data from one country's government and military networks on several occasions, including a period of heightened tension over competing claims in the South China Sea.<sup>1</sup>

Some of the files that the APT group took included the following:

- General military documents
  - Internal communications
  - Equipment maintenance reports and specifications
  - Event-related materials
  - Documentation of organizational programs and initiatives
- Other threat groups have targeted a country's air force with spear-phishing emails that referenced the country's military and regional maritime disputes. These emails were designed to appear to originate from email accounts associated with other elements of the military.

- Other threat actors have used the Grillmark backdoor to attempt to gain access to the networks of two countries' government and military entities. These threat actors targeted their victims through spear-phishing emails that contained weaponized documents relating to either diplomatic or military affairs.

### APT Groups Gather Political Intelligence

In August 2014, an APT group appeared to target intelligence related to a Southeast Asia government. The threat actors sent a spear-phishing email that referenced the country's leadership and contained a document with sections extracted from related news articles. The email appeared to originate from a compromised intelligence agency email account, although the threat actors may have faked the email address. Many of the email's recipients were associated with the targeted country's government and military or were involved in intel-sharing partnerships. In either case, the recipient would likely have access to information regarding the country's security and internal stability.

<sup>1</sup> Whaley, Floyd. "A Leviathan Turns Philippine Fishermen into Desperate Darters." The New York Times. 18 May 2014. Web. 23 May 2014.

# CONCLUSION

Public and private organizations in the Southeast Asian region are prime targets for advanced threat groups. The data is clear: targeted threat actors are focused on getting into the networks of and stealing from fast-growing industries, as well as from organizations involved in territorial claims over the South China Sea.

The outcome of the dispute has major geopolitical and economic implications for multiple countries. The area is key to regional trade because of its rich energy reserves, prime fishing waters, and significance to commercial shipping routes. These issues and the region's mounting importance will likely propel state-sponsored threat groups to continue targeting Southeast Asian governments and companies for the near future.

State-sponsored threat groups will continue to target Southeast Asian governments and companies.

## ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.

To download this or other  
FireEye Threat Intelligence reports,  
visit: [www.fireeye.com/reports](http://www.fireeye.com/reports)

IMAGINING SECURITY



FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | [info@fireeye.com](mailto:info@fireeye.com) | [www.fireeye.com](http://www.fireeye.com)

© 2015 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. SP:SEA.EN-US.022015