FireEye
SECURITY REIMAGINED

SPECIAL REPORT

# REGIONAL ADVANCED THREAT REPORT:

## Asia Pacific 1H 2015

# INTRODUCTION

We appreciate the opportunity to provide you with unique insight into Asia Pacific's threat landscape for the first half of 2015. For years we have been stating that over 95% of businesses unknowingly host compromised PCs within their corporate networks, and that has not changed. During our assessment, we identified all types of threat actors compromising our customers' networks, including suspected nation state-backed actors conducting cyber espionage, cyber criminals, and hacktivists looking to make a statement.

# EXECUTIVE SUMMARY

This FireEye Advanced Threat Report for APAC provides an overview of the advanced attacks that FireEye detected targeting computer networks in the first half of 2015.

Since the start of the year, FireEye has seen a significant increase in the number of attacks across the region. 96 percent of global organizations are unknowingly breached as threat actors of all kinds increasingly evade traditional security products. This report summarizes data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud.

Over the past six months, from January - June 2015, we found:

- In Southeast Asia, organizations are now 45% more likely to be attacked than the global average
- Previously, enterprises in this region were only 7% more likely to be attacked
- Organizations in Thailand were previously less likely to be attacked than the global average. Their exposure to advanced attacks is now more than double the global average
- Asia's institutions of higher education are facing attacks at a higher level than traditionally popular targets such as high-tech and financial services

**Disclaimer:** This report only covers computer network activity of targeted FireEye customers who share their metrics with FireEye. It is by no means an authoritative source for all APT activity targeting the Asia Pacific region or elsewhere. In this dataset, we take reasonable precautions to filter out "test" network traffic as well as traffic indicative of manual intelligence sharing among our customer base within various closed security communities. We realize that some popular APT tools, techniques and procedures (TTPs) can be reused and repurposed by many different threat actors. To address this issue, we employ conservative filters and crosschecks to reduce the likelihood of misidentification.

# DEFINITIONS

**Advanced Persistent Threat (APT):** A distinct set of cyber tools, techniques, and procedures (TTPs) that are employed directly or indirectly by a nation-state or a sophisticated, professional criminal organization for cyber espionage or the long-term subversion of adversary networks. Key qualifying APT characteristics include regular human interaction (i.e., not a scripted, automated attack), and the ability to extract sensitive information, over time, at will.

**Callback:** an unauthorized communication between a compromised victim computer and its command-and-control (CnC) infrastructure.

**Remote Access Tool (RAT):** software that allows a computer user (for the purposes of this report, a threat actor) to control a remote system as though he or she had physical access to that system. RATs offer numerous features such as screen capture, file exfiltration, etc. Typically, an attacker installs the RAT on a target system via some other means such as spearphishing or exploiting a zero-day vulnerability, and the RAT then attempts to hide from the system's legitimate owner.

**Security Event:** FireEye regularly discovers a wide variety of web, email and file-based threats, including the opening of a malware attachment, a click on a malicious hyperlink, or the callback of an infected machine to its CnC network.

**Targeted attack:** a unique, malicious event conducted between an APT threat actor and a specific victim network.

**Threat Actor:** the perpetrator behind cyber activity. This actor could be part of a broader group such as a military unit, an intelligence agency, a contractor organization or a non-state actor with indirect state sponsorship.

**Tools, Techniques, and Procedures (TTPs):** the characteristics specific to a threat actor's actions and tools (like malware) employed against a victim network. APT actors normally employ multiple TTPs, and multiple APT actors can also use the same TTPs. This dynamic frequently complicates cyber defense analysis.

**Vertical:** one of FireEye's distinct industry categories: Aerospace, Chemicals, Construction, E-Commerce, Education, Energy, Media/Entertainment, Finance, Government, Healthcare, High-Tech, Insurance, Legal, Manufacturing, Other, Retail, Services, Telecom, Transportation and Wholesalers.

**Target:** the recipient of a threat actor's attack. In most cases, the low "false positive" rates inherent in FireEye alerts suggest that the discovered attack was successful.

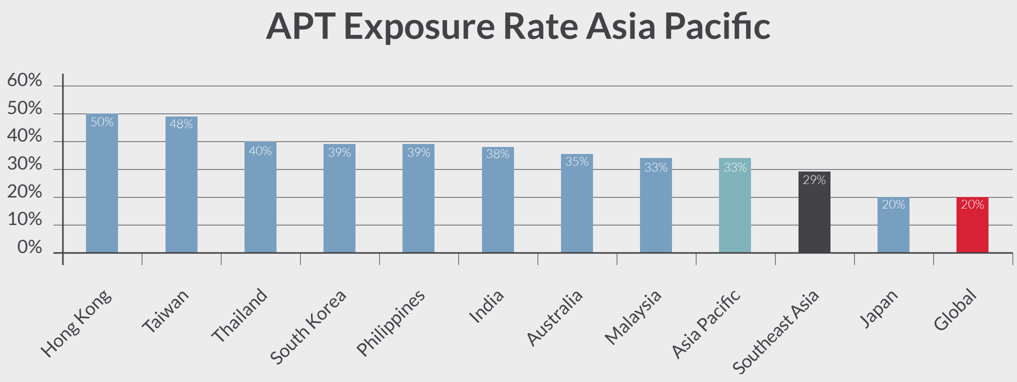
## Cyber Threats to Asia Pacific Countries

If at the start of this year, some in Asia still assumed advanced persistent threat groups were only a U.S. problem, the events of the past several months seem determined to remedy this.

The first half of 2015 was a highly eventful period for cyber security in the Asia Pacific region. In April, China was reported to have weaponized its Great Firewall, turning into what some dubbed the Great Cannon. A short time later, FireEye published our APT30 report, which revealed a decade-long cyber espionage campaign—targeting organizations across Southeast Asia and India—that sought political, economic and military information. In May, a major Australian telecommunications firm announced a firm it recently acquired had been breached. Finally, in June, the Japan Pension Service breach rocked the nation and raised awareness about these threats. And that's just a few events which were publicly disclosed. The year ahead shows no signs of slowing down.

In fact, every geography included in this report has a higher exposure rate to attacks from APT groups than the global average. The region's geopolitical tensions have steadily ratcheted up in recent months, and its cyber activity reflects this.

**Figure 1:**
APT Exposure Rate by Region

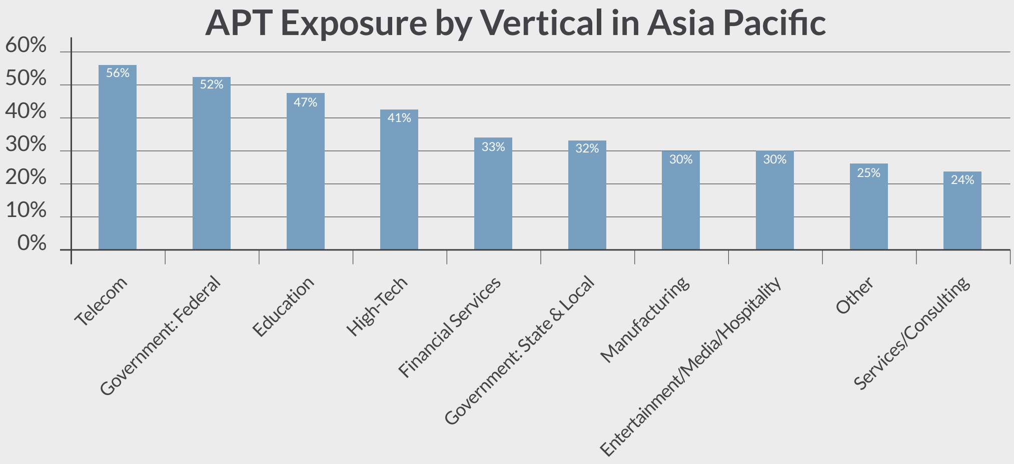


When we look at the percentage of organizations in a given region that are exposed to advanced attacks, we see significant changes. At the time of our last report, we found organizations in Thailand were less likely to be attacked than the global average. Their exposure to advanced attacks is now more than double the global average.

Several other regions have risen from well below the average to well above it, including Southeast Asia generally, where organizations are now 45% more likely to be attacked than the global average, where before they were only 7% more likely.

A significantly higher rate was also seen in India, which is now embarking on an ambitious Digital India project. India was a target of APT30, and the majority of the WATERMAIN campaign, an APT effort that targeted primarily governmental and educational organizations that FireEye revealed in August.

**Figure 2:**
APT Exposure Rate by Vertical



While breaches at Asia's institutions of higher education haven't made as many headlines as in the U.S., they are facing attacks at a higher level than traditionally popular targets such as high-tech and financial services

## Top five countries with alerts on malicious exploits/downloads:

1. South Korea
2. Japan
3. Taiwan
4. Australia
5. Thailand

## Top five countries exhibiting CnC infection callbacks:

1. South Korea
2. Japan
3. Thailand
4. India
5. Taiwan

## Top 10 industries with alerts on malicious exploits/downloads:

1. High-Tech
2. Financial Services
3. Government: Federal
4. Service Provider
5. Education
6. Telecom
7. Services/Consulting
8. Energy/Utilities
9. Government: State & Local
10. Entertainment/Media/Hospitality

## Top 10 industries exhibiting infection callbacks:

1. High-Tech
2. Government: Federal
3. Financial Services
4. Manufacturing
5. Education
6. Service Provider
7. Telecom
8. Services/Consulting
9. Energy/Utilities
10. Government: State & Local

## Top 10 "destination" countries for CnC callbacks:

1. South Korea
2. USA
3. China
4. Netherlands
5. Germany
6. Russia
7. United Kingdom
8. Ukraine
9. France
10. Japan

- Our previous Advanced Threat Report found that all 206 countries and territories in the world were home to advanced attack infrastructure. To contrast the top countries targeted, we show here the top 10 countries that malware beacons back to.

- These destination countries rarely, if ever, reflect the true threat actor behind the attacks FireEye detects, but they do provide us with visibility into a) how attackers utilize infrastructure in seemingly non-hostile countries to obfuscate their activities from network defenders and law enforcement and b) which nations need to be most vigilant in policing their Internet infrastructure.

- The top of this APJ list is similar to the global list of CnC callback destinations. The notable addition here is China, which does not place on the global list. Some China-linked offensive campaigns in the region use domestic CnC infrastructure; others do not.

### Top 10 signature families by infection callback count:

1. Sality
2. Conficker
3. Kelihos
4. Zbot
5. Upatre
6. Rerdom
7. CryptoWall
8. Virut
9. ZeroAccess
10. Carberp

Note the inclusion of CryptoWall, a kind of ransomware. Ransomware is present in families affecting the Asia Pacific region but absent from our global list.

### Top five APT malware families by infection callback count:

1. Backdoor.APT.LV
2. Backdoor.APT.Kaba
3. Backdoor.APT.Gh0stRat
4. Backdoor.APT.Page
5. Backdoor.APT.XtremeRAT

Backdoor.APT.Kaba was observed in a number of spear phishing attempts targeting the media industry in Hong Kong in April and May.

Backdoor.APT.Gh0stRAT source code is openly available. We have observed both APT and non-APT actors using Gh0stRAT.

# CONCLUSION AND RECOMMENDATIONS

This report demonstrates that organizations in the APAC region were increasingly targeted by advanced threats in the first half of 2015. We see significant changes since our last report, including Southeast Asia and other regions that have seen APT exposure grow from well below average to well above it. Add to that the number of organizations in Thailand where APT exposure is now more than double the global average, and it's apparent that threat actors are homing in on the APAC region for targeted attacks.

**Our recommendations include:**

1. Ensure existing security tools are up to date. Much commodity malware can be easily addressed with legacy, signature-based tools.
2. Implement an Adaptive Defense security model that can help shorten the time it takes between finding a breach and stopping it.
3. Develop new ways to collaborate with other corporations, trade groups, and governments to share threat intelligence.

To learn more about
how FireEye can help you focus
on the alerts that matter,

**visit:**
http://www.**fireeye.com**

FireEye

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