Control Risks

CYBER THREAT IN SOUTH EAST ASIA:

ACTORS AND TARGETS

THE NUMBER AND IMPACT OF GLOBAL CYBER ATTACKS INCREASED

18%
INCREASE IN AVERAGE IMPACT OF CYBER ATTACKS

56%
INCREASE IN NUMBER OF POLITICALLY MOTIVATED CYBER ATTACKS

100%
INCREASE IN NUMBER OF CRIMINAL TARGETED ATTACKS

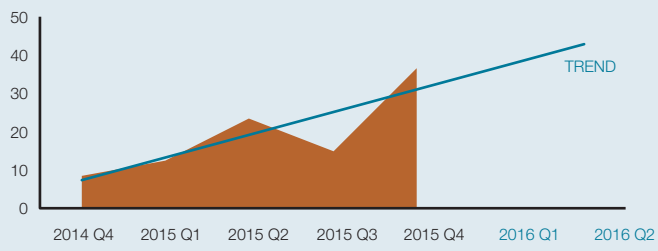
GOVERNMENT, FINANCE, AND TELECOMS SECTORS ARE THE MOST FREQUENTLY TARGETED IN SOUTH EAST ASIA (% TOTAL ATTACKS)

- 33.3% GOVERNMENT
- 19.7% FINANCIAL
- 13.6% MANUFACTURING AND ENGINEERING
- 13.6% MINING
- 19.7% TELECOMMUNICATIONS

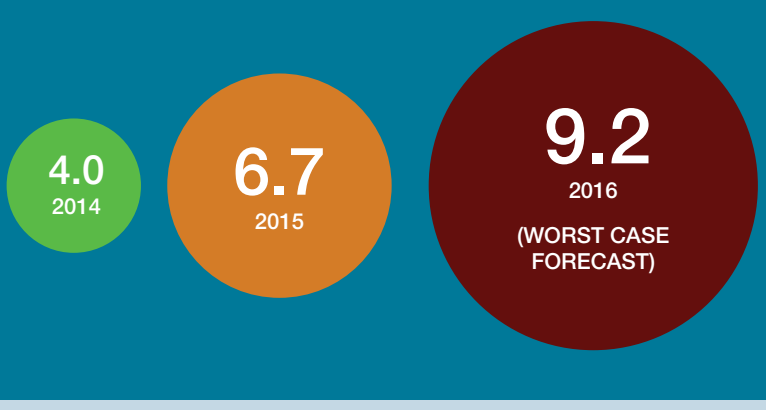
All data is sourced from Control Risks' Cyber Threat Intelligence reporting.

A GREATER NUMBER OF NATION STATES WILL CONDUCT ATTACKS, WITH A LARGER PROPORTION CAPABLE OF OPERATIONS WITH A SEVERE IMPACT. (NUMBER OF DISTINCT NATION STATES ENGAGING IN CYBER OPERATIONS EACH QUARTER)

WE FORECAST THAT IN 2016 THERE WILL BE AT LEAST
45 NATION STATES
ACTIVELY CONDUCTING CYBER OPERATIONS AND A
>15% INCREASE IN THE IMPACT OF THEIR ATTACKS.



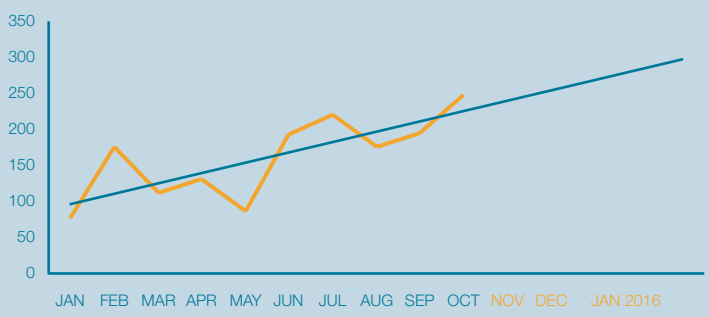
A BROADER RANGE OF THREAT ACTORS WILL TARGET INDUSTRIAL CONTROL SYSTEMS (ICS), WITH A GREATER IMPACT. (AVERAGE THREAT SCORE FOR CYBER ATTACKS TARGETING ICS)



BY THE END OF 2016 WE EXPECT A
37% RISE
IN THE SEVERITY OF CYBER ATTACKS
TARGETING ICS COMPARED WITH 2015

ATTACKERS WILL INCREASINGLY FOCUS ON MANIPULATING DATA, AFFECTING ITS INTEGRITY RATHER THAN ITS CONFIDENTIALITY OR AVAILABILITY. IMPACT OF CYBER ATTACKS ON INTEGRITY OF SYSTEMS AND DATA (INDEX, JAN 2015=100), JAN-OCT 2015

IN 2016 WE FORECAST A
40% RISE IN THE THREAT POSED TO THE
INTEGRITY OF SYSTEMS AND DATA



THE TOP FIVE MOST IMPACTFUL CYBER ATTACK TECHNIQUES OF 2016 IN SOUTH EAST ASIA

01	02	03	04	05
HARDWARE	CRIMINAL TARGETED ATTACK	DATA LEAK	APT OPERATIONS	UNAUTHORIZED ACCESS
H	H	H	M	M
9.06	7.20	7.03	6.71	5.86

Scores as at Oct 2015.
The threat score considers the actors involved, the tools used and the attack method's severity, impact and likelihood of success.
Under 5 – low-level threat: awareness important but immediate action not required.
5-7 – medium-level threat: organisations should seriously consider implementing mitigation measures.
7-10 – high-level threat: organisations must immediately take measures against the threat.

DEFINITIONS

Impact – Impact is based on the assessed magnitude of the effect of the attack on the confidentiality, integrity and availability of systems and information targeted, as well as the value of those assets.

APT campaigns – Advanced persistant threat campaigns: nation-state-led espionage operations.

Data leak – Public exposure of information with a commercial or reputational value.

DDoS - Disruption to normal operations caused by a flood of internet traffic.

Ransomware – Malicious software that prevents or limits users from accessing their system or files (often through encryption) to extort victims.

Criminal targeted attacks – Campaigns using advanced techniques to steal from specific pre-selected targets.

For more information or to speak to us about specific issues affecting your organisation, please contact us.
cyber@controlrisks.com

All data is sourced from Control Risks' Cyber Threat Intelligence reporting. Contact us for a free trial.

Information correct as of June 2016

Countries included in these statistics are Hong Kong, Indonesia, Malaysia, Singapore, Thailand, Vietnam

Copyright: Control Risks Group Limited 2015. All rights reserved. Reproduction in whole or in part prohibited without the prior consent of the Company.