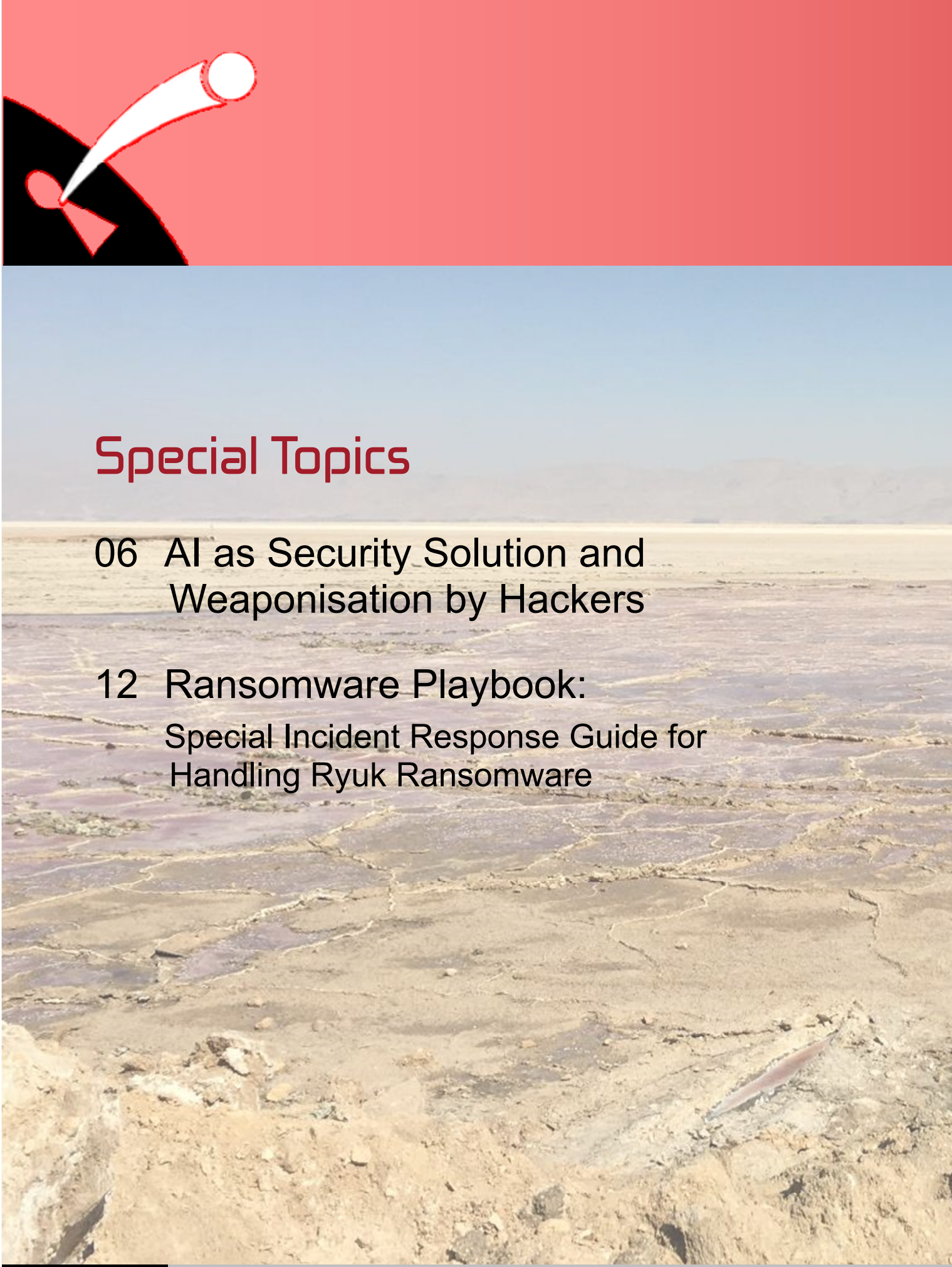
PISA Journal

AI as Security Solution and Weaponisation by Hackers

Ransomware Playbook

www.pisa.org.hk

Issue 30



Special Topics

Editor: editor@pisa.org.hk

Intranet

Message from the Chair

Perhaps one of the most frequent words we hear or watch from the media in recent months is "independent XXXXX". No matter what colour one is alleging, independence seems a wild card that can be placed in most of the slogans.

Being trained security professionals, our PISA members are required to have an independent mindset when preforming our duty. Regardless who sponsors the security assessment, audit or project, we have to perform unbiased investigations to uncover vulnerabilities, locate the root cause of the issue, and then give prudent recommendations for improvement.

Given the recent social movement happening in Hong Kong in the last 6 months, let's apply our independent mindset to help people around us, not only to deal with tons of messages from the social media, but also differentiate fake messages, using another popular term "Fact Check". Misinformation is becoming a serious topic in information security arena. One of the three pillars of information security is "Integrity" and we are trained to identify and analyse tampered information and spoofed identity. Perhaps this is another value we can add to the Hong Kong community.

Wish we all have a merry and peaceful Christmas and a prosperous 2020.

Ando Ho

Chair

The New PISA EXCO and (ISC)2 HK Chapter EXCO

PISA EXCO

Chair: Mr. Andy Ho

Vice-Chair: Mr. Frank Chow (External Affairs)

Vice-Chair: Mr. Frankie Wong (Internal Affairs)

Vice-Chair: Mr. Otto Lee (Membership & Constitution)

Hon. Secretary & Treasurer: Ms. Joyce Fan

Program Director: Mr. Frankie Leung

Program Director: Mr. Mike Lo

(ISC)2 HK Chapter EXCO

President: Andy Ho *

Secretary: Joyce Fan *

Treasurer: Frankie Leung

Membership Chair: Otto Lee *

Professional Development: Eric Moy

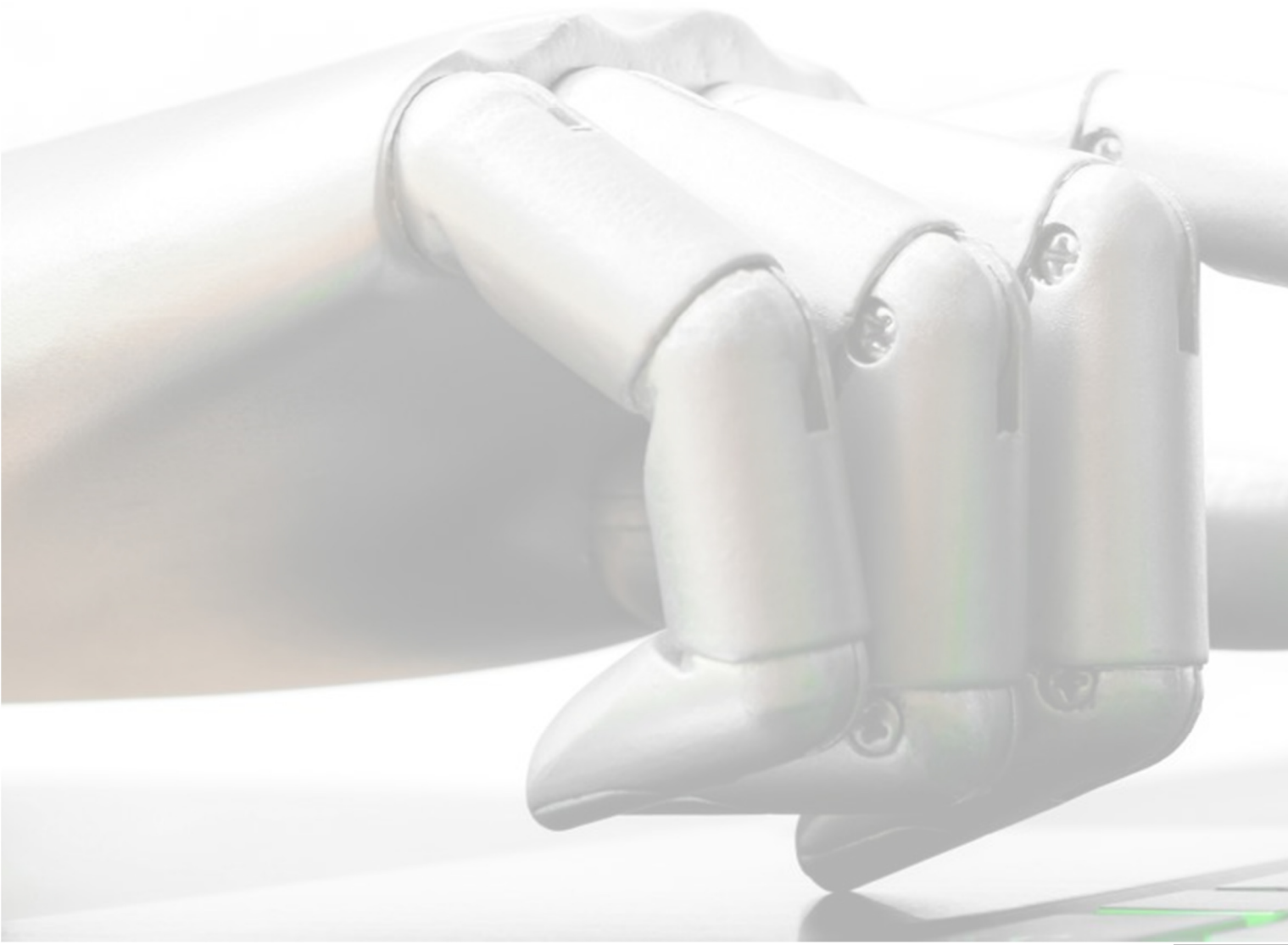
Program Director: Eve Chow

Program Director: Jim Shek

Liaison: Frank Chow *

* Automatically transferred from PISA EXCO

AI as Security Solution and Weaponisation by Hackers



Artificial intelligence is a double-edged sword that can be used as a security solution or as a weapon by hackers. AI entails developing programs and systems capable of exhibiting traits associated with human behaviours. The characteristics include the ability to adapt to a particular environment or to intelligently respond to a situation. AI technologies have extensively been applied in cyber security solutions, but hackers are also leveraging them to develop intelligent malware programs and execute stealth attacks.

AI as a Security Solution

Security experts have conducted a lot of research to harness the capabilities of AI and incorporate it into security solutions. AI-enabled security tools and products can detect and respond to cyber security incidents with minimal or zero input from humans. AI applications in cyber security have proved to be highly useful. 25% of IT decision-makers attribute security as the primary reason why they adopt AI and machine learning in organisational cyber security [1]. AI not only improves security posture, but it also automates detection and response processes. This cuts on the finances and time used in human-driven intervention and detection processes.

[1] https://www.cpomagazine.com/cyber-security/artificial-intelligence-a-cybersecurity-solution-or-the-greatest-risk-of-all

Applications of AI in cyber security

1. Modeling User Behaviour

Organisations use AI to model and monitor the behaviour of system users. The purpose of monitoring the interactions between a system and users is to identify takeover attacks. These are attacks where malicious employees steal login details of other users and use their accounts to commit different types of cyber crimes. AI learns the user activities over time such that it considers unusual behaviour as anomalies [2]. Whenever a different user uses the account, AI-powered systems can detect the unusual activity patterns and respond either by locking out the user or immediately alert system admins of the changes.

2. Applying AI in Antivirus Products

Antivirus tools with AI capabilities detect network or system anomalies by identifying programs exhibiting unusual behaviour. Malware programs are coded to execute functions that differ from standard computer operations. AI antiviruses leverage machine learning tactics to learn how legitimate programs interact with an operating system. As such, whenever malware programs are introduced to a network, AI antivirus solutions can immediately detect them and block them from accessing systems resources. This contrasts from signature-based traditional antiviruses which scans a signature database to determine whether a program is a security threat.

[2] https://www.sciencedaily.com/releases/2019/04/190408114325.htm

3. Automated Network and System Analysis

Automated analysis of system or network data ensures continuous monitoring for prompt identification of attempted intrusions. Manual analysis is nearly impossible due to the sheer volume of data generated by user activities. Cyber criminals use command and control (C2) tactics to penetrate network defenses without being detected. Such tactics include embedding data in DNS requests to bypass firewalls and IDS/IPS. AI-enabled cyber defenses utilise anomaly detection, keyword matching, and monitoring statistics. As a result, they can detect all types of network or system intrusion.

4. Scanning Emails

Cyber criminals prefer email communication as the primary delivery technique for malicious links and attachments used to conduct phishing attacks. Symantec states that 54.6% of received email messages are spam and may contain malicious attachments or links. Anti-phishing email solutions with AI and machine learning capabilities are highly effective in identifying phishing emails. This is done by performing in-depth inspections on links. Additionally, such anti-phishing tools simulate clicks on sent links to detect phishing signs. They also apply anomaly detection techniques to identify suspicious activities in all features of the sender. These include attachments, links, and message bodies, amongst other items.

AI Weaponisation by Hackers

Hackers are turning to AI and using it to weaponise malware and attacks to counter the advancements made in cyber security solutions. For instance, criminals use AI to conceal malicious code in benign applications [3]. They program the code to execute at a specific time, say ten months after the applications have been installed, or when a targeted number of users have subscribed to the applications. This is to maximise the impact such attacks will cause. Concealing such code and information requires the application of AI models and deriving private keys to control the place and time the malware will execute.

Additionally, hackers can predefine an application feature as an AI trigger for executing cyber-attacks. The features can range from authenticating processes through voice or visual recognition to identity management features [4]. Most applications used today contain such features, and this provides attackers with ample opportunities of feeding weaponised AI models, deriving a key, and attacking at will. The malicious models can be present for years without detection as hackers wait to strike when applications are most vulnerable.

AI technologies are also unique in that they acquire knowledge and intelligence to adapt accordingly. Hackers are aware of these capabilities and leverage them to model adaptable attacks and create intelligent malware programs. Therefore, during attacks, the programs can collect knowledge of what prevented the attacks from being successful and retain what proved to be useful. AI-based attacks may not succeed in a first attempt, but adaptive abilities can enable hackers to succeed in subsequent attacks. Security communities thus need to gain in-depth knowledge of the techniques used to develop AI-powered attacks to create effective mitigations and controls.

Also, cyber adversaries use AI to execute intelligent attacks that self-propagate over a system or network [5]. Smart malware can exploit unmitigated vulnerabilities, leading to an increased likelihood of fully compromised targets. If an intelligent attack comes across a patched vulnerability, it immediately adapts to try compromising a system through different types of attacks.

Lastly, hackers use AI technologies to create malware capable of mimicking trusted system components. This is to improve stealth attacks. For example, cyber actors use AI-enabled malware programs to automatically

[3] https://www.techrepublic.com/article/how-weaponized-ai-creates-a-new-breed-of-cyber-attacks

[4] Ibid

[5] https://www.zdnet.com/article/this-is-how-artificial-intelligence-will-become-weaponized-in-future-cyberattacks/

learn the computation environment of an organisation, patch update lifecycle, preferred communication protocols, and when the systems are least protected [6]. Subsequently, hackers can execute undetectable attacks as they blend with an organisation's security environment. For example, TaskRabbit was hacked compromising 3.75 million users, yet investigations could not trace the attack [7]. Stealth attacks are dangerous since hackers can penetrate and leave a system at will. AI facilitates such attacks, and the technology will only lead to the creation of faster and more intelligent attacks.

[6] https://www.cnbc.com/2018/07/20/ai-cyberattacks-artificial-intelligence-threatens-cybersecurity.html
[7] https://www.analyticsindiamag.com/5-artificial-intelligence-based-attacks-that-shocked-the-world-in-2018/

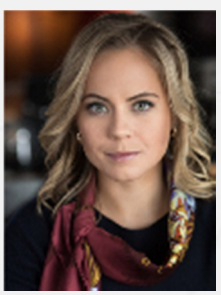
Ransomware Playbook

A Special Incident Response Guide for Handling Ryuk Ransomware (Tripe-Threat) Attack

Frankie Li

Chief Security Analyst - DAT

Frankie Li is the Chief Security Analyst at Dragon Advance Tech (DAT). He had been a speaker in various security conferences: US Blackhat, Cyber Security Consortium (HK), HITCON (Taiwan), (ISC)2 Security Congress (APAC), CyberCrimeCon 2018 (Russia) and High-Tech Crime Investigation Association (HTCIA, APAC) and Founder of Dragon Threat Labs, DragonCon.



Mika Devonshire

CISM, CEH, CompTIA Security+ and Network+, AccessData Certified Examiner

Mika Devonshire has 7 years of experience in information security, specialising digital forensics, vulnerability management and offensive security. She has a Master degree in digital forensics from the George Washington University and Bachelors degree from Princeton University

Ken Wong

CISSP, CISA, OSCP and AVSE

Ken has been researching on mobile and IoT security. He has solid red team and blue team experience and recently research on purple teaming which includes malware analysis and reverse engineering, TTPs, security monitoring and operation, cyber threat intelligence, big data analytics, protocol reverse engineering, cyber security incident response, and digital forensics.

Overview

Ransomware is a very simple, but effective malicious software that affects both home users as well as government departments, courts, hospitals, universities, large enterprises, small medium enterprises or even non-government organisations (NGOs). Since 2013, it has become a key financial resource of choice for cybercriminal organisations. It performs malicious actions to encrypt personal files (such as images, movies, documents, or text files) on the infected systems, encrypt files on shared network drives (including connected NAS or storage devices), lock system access, crash systems, or even display disruptive and indecent messages containing pornographic images to embarrass users and force victims to pay a ransom through bitcoin (or other crypto-currencies) by using elaborate techniques.

The return on investment (ROI) is so high that it has been turned into a business model known as the Ransomware-as-a-Service industry. Developers recruit affiliates to spread the ransomware in return for a cut of the profits. Researchers have published several ransomware projects in the name of education and freedom of knowledge that unfortunately allow novice hackers to easily acquire and run successful ransomware campaigns.

Ransomware is difficult to defend against because it uses common tools native to the Windows operating system, such as the standard Windows crypto API, PowerShell, Windows Management Instrumentation (WMI) or even JavaScript. It also makes use of exploit kits to deploy ransomware through web browsers, Adobe Flash plug-ins and even Microsoft Office documents.

Unlike common malicious software, ransomware does not try to hide. Immediately after the infection, a ransom note is usually displayed to inform the victims that their machines were infected. Sometimes, a visible running timer, a bitcoin address to send payment, and instructions on how to buy bitcoin will be displayed on the victim machines. This note asks for ransom payment (either a few hundred US dollars or more in the case of government attacks) and in turn the attacker promises a key to decrypt their data.

Traditional preventive measures can be very useful to reduce damage from this kind of attack. Procedures such as backing up all critical data frequently, installing updated anti-virus, and maintaining good user awareness do help protect organisations from ransomware attacks. Additional prevention advice or even decryption tools can be found from an online project called: NO MORE RANSOM [1].

Before 2017, the infection vectors mainly came from phishing emails or vulnerable browser plug-ins contacting compromised web servers. The WannaCry ransomware, like a network worm, was an exception in that it used ETERNALBLUE to exploit SMB services running inside the Windows kernel on unpatched Windows systems.

Since 2018, some advanced cybercriminals have changed their tactics and now direct their efforts toward sophisticated, longer-term attacks against specific enterprises to seek a larger ransom. We have encountered incidents of ransomware infections on internal servers through carelessly configured remote desktop (RDP) [2] connections. Ransomware, like Ryuk, has been used in the final stage of tailored attacks after the target's systems or networks have been compromised for a period of time. The attacker then manually plants Ryuk to encrypt only crucial assets in the target environment. In a security blog published

[1] https://www.nomoreransom.org/en/ransomware-qa.html

[2] https://dragonadvancetech.com/reports/SME-RDP-final-draft-31.pdf and https://dragonadvancetech.com/reports/SME-RDP-RCE-final.pdf

on October 9, 2019, the researcher provides the following insight into Ryuk ransomware:

> *Many of these organisations have paid hefty fees to recover their files following a Ryuk attack, only to find that any number of files have been stolen, and some of the data left behind is beyond repair. What many people don't understand about Ryuk is that it is not the beginning of the attack, it is the end of the attack.*

On October 4 2019, a Toronto media [3] firm published that the same ransomware hit three Ontario hospitals, causing a delay for patients and creating a headache for the staff.

Cybercrime analysts and specialised bloggers found this kind of ransomware is difficult to defend against because Ryuk is like a comic book character who "cannot be harmed by conventional human weapons" and traditional incident handling procedures, like "reimaging" computers to reset them to their previous configurations, do not always work because the malware has the ability to come back, called "persistence" mechanisms.

On October 17, 2019, the global shipping and ecommerce giant Pitney Bowes [4] revealed that their recent service disruptions were caused by Ryuk. The incident impacted the company's critical servers, including: mailing services, customer account access, the supplies web store, software and data marketplace downloads, and some commerce services.

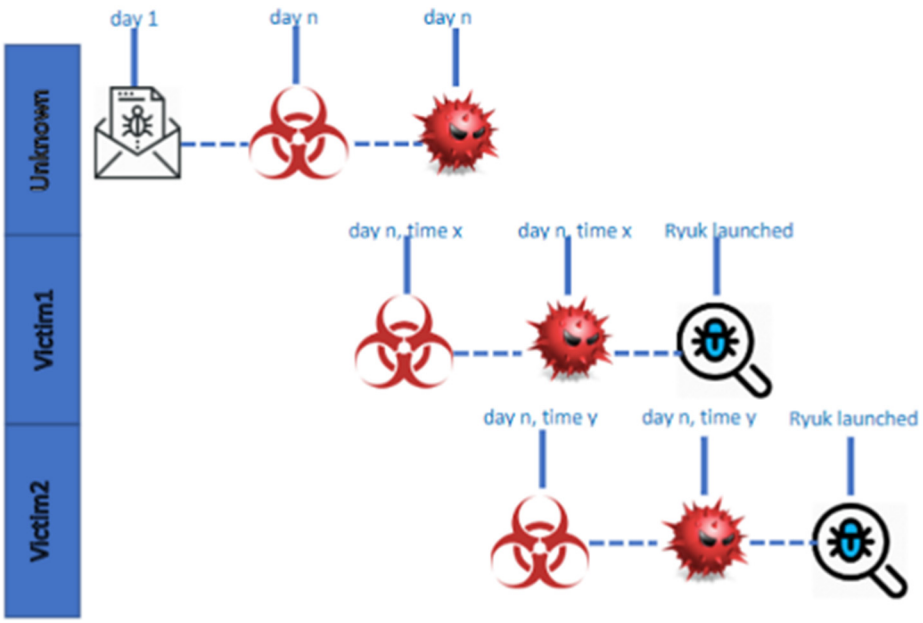


Fig 1 Recent Emotet, Trickbot and Ryuk ransomware attack

[3] https://www.cbc.ca/amp/1.5308180?__twitter_impression=true
[4] https://maintenance.pb.com/pbcom/outage.html

This Ransomware Playbook is intended to be used as a general guideline for organisations faced with ransomware attacks. If you are currently experiencing a ransomware incident, it is highly recommended you immediately review the containment section below. If your organisation is infected with ransomware like Ryuk, we can provide a detailed checklist upon request to help you to handle the incident in an expedited manner – this is crucial as you will not only have to handle Ryuk [5], but also two forms of malware called Trickbot and Emotet (Fig 2 – reproduced based on the findings from Kryptoslogic [6]).

Incident Lifecycle

The incident response cyber is made up of many steps including intrusion detection, and intrusion response. By making reference to the model of NIST SP800-61 Computer Security Incident Handling Guide, the incident lifecycle (Fig. 2) can be classified into several phases. The initial phase involves the identification of security program's hygiene issues, this includes a comprehensive analysis of the environment focused on finding evidence of ongoing or past compromises, assessment of systemic risks and exposures, establishing and training an incident response team, and acquiring necessary tools and resources. During preparation, the organisation

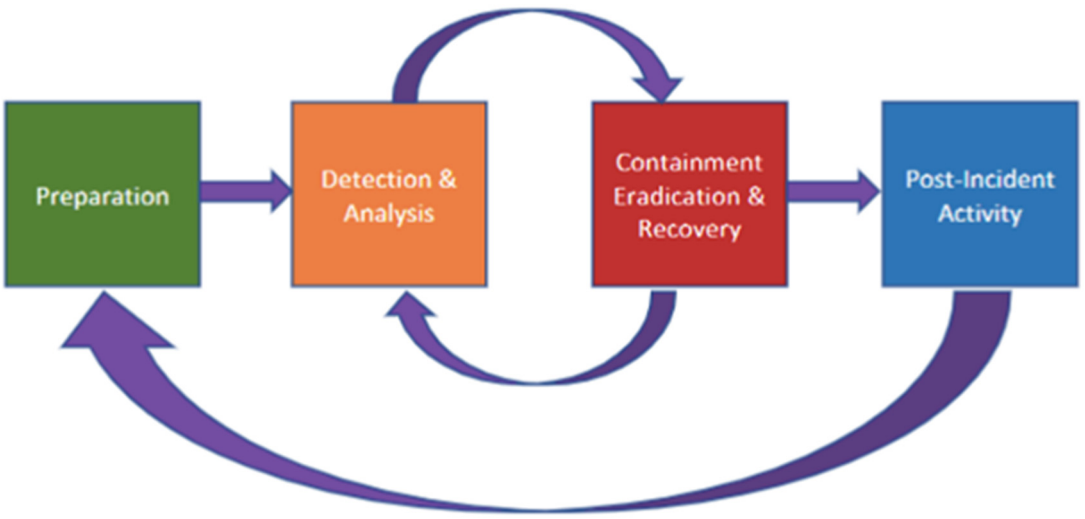


Fig. 2 – Incident Response Life Cycle

IR phase B and C may need to be performed iteratively and recursively.
The time window for the incident handling ransomware ***usually is limited to 48-72 hours***

[5] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
[6] https://www.kryptoslogic.com/blog/2019/01/north-korean-apt-and-recent-ryuk-ransomware-attacks/

should attempts to limit the number of incidents based on the results of the risk assessments.

The detection of security breaches is heavily dependent upon the protection solutions deployed, whether on premise or in the cloud. A baseline needs to be established to detect anomalies, for example, and events need to be monitored continuously to alert the organisation the moment an incident occur. During the analysis phase of an incident, the incident response team will analyse endpoint, network, and log data to attempt to identify the root cause and pinpoint any compromised systems. After analysing the event and confirming the severity of the incident, the organisation should perform necessary actions to limit the impact of the incident by containing the infection or behaviour and ultimately begin recovering from it.

After the incident is adequately handled, the organisation should prepare a report that details the attackers' activities, a summary of the incident, procedures for remediation, and the steps the organisation should take to prevent a future incident. The post-incident phase contains important organisation-wide lessons to learn and apply across the people, processes, and technologies in place.

Preparation

This is the initial phase where organisations will perform preparatory measures to ensure that they can response effectively to the incidents if and when they are discovered. It involve all planning works such as: develop policy and procedures, setting up cyber incident response team (CIRT), setting incident reporting mechanism, issue tracking system, preparing systems (or a jump kit) that are installed with all necessary tools and acquire hardware to acquire forensics images for the organisation's different kinds of computing systems, including: RAID-5 servers and virtual machines created on Microsoft Hyper-V or VMware EXSI environment.

The first responder should be provided with the organisation's incident response (IR) plan. If such document is not available, the responder should prepare one on the spot. The IR plan and triage should contain the following documents:

- Contact information of the in-house IR team
- Communication plan
- Escalation and notification procedures and reporting mechanism
- Telemetry of the involved network – high-level network map and critical systems
- Information on how to access to images of clean OS, different versions of backups and application installations for restoration and recovery purposes
- Documents of current baselines, endpoint security, network security, malware prevention, user awareness and training, patch management and vulnerability policies
- In most of the ransomware cases we encountered in the past, the infected organisation canonly be able to provide limited information described above. In this case, the incident responder is required to obtain information as much as possible or using our Incident Report Form as a help for your triage process.

Detection, Identification & Analysis

The second phase is where organisations should strive to detect and validate incidents quickly. Infections can spread through an organisation rapidly. Taking corrective action immediately will minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident.

Detection includes monitoring endpoints, network traffic, logs and SIEM data sources. Looking for anomalies on login/logoff, spikes in network activities for data exfiltration and raise alerts on suspicious events. Not every security "event" will need to be escalated as an "alert" and not every alerts will be classified as an "incident". All alerts need to be identified or categorised (malware, system compromise, PII, spam ransomware or any other kind of attack), then prioritised after triage. Incidents can be classified into multiple categories.

Incidents can occur in many ways. Different types of incidents require different response strategies. The attack vectors (email, web, removable device, network) combined with the initial observations will help the incident reporter correctly classify the incident.

Analysis includes the study of the indicators of compromise (IoCs) and the breadth and depth of the incident need to be analysed. Analysis of an incident, either successful or failed, can provide significant insight of possible threats to an organisation. In some cases, like Ryuk ransomware, the intrusion is not an isolated case, but represents a part of the complex campaign. Before the artifacts or the signs of an incident can be analysed, we have to identify how the attacker entered the network.

- **Incident discovery (i.e signs of the incidents) - ransomware can be discovered from:**
  - Anti-spam or email filter alerts
  - Anti-virus software alerts
  - Anti-spam browser plug-in alerts
  - EDR solution – most advance threats are polymorphic to bypass anti-virus or other protection layers deployed in an enterprises environment. By focusing on generic signature detection mechanism may not good enough to detect the attacks.
  - SIEM alerts and correlated event alerts
  - File integrity checking software alerts
  - Operating system, service and application logs
  - High volume of exceptional network or hard disk activities
  - Abnormal network flows and alerts
  - Alerts of Command and Control (C2) traffic from a compromised host
  - Informed by end users when they saw the ransom note or encrypted files
  - Informed by SOC analysts or law enforcement

- **Detection and identification – ransomware usually does not try to hide:**
  - Popped-up ransom note on screen
  - Personal files (images, movie, files, documents, text files) were encrypted with unique extension

- Network drive folders or files on USB connected NAS devices encrypted
- Infected system was locked due to some system libraries was encrypted
- Infected system crashed due to some system libraries was encrypted
- Services disrupted due to some application libraries was encrypted
- Annoying message of pornographic images displayed and not able to remove
- For a Windows system that is joined to an Active Directory (AD) domain, files in a user roaming profile [7] folder may also be encrypted. Responder needs to investigate if there are any other files (images, movie, files, documents, text files) of the investigating system were encrypted. If some files are not encrypted, there is a possibility that ransomware was not executed on this system.

- **Incident validation – confirm and verify the possible delivery vectors of the ransomware**
  - For common ransomware, there are two delivery vectors, they are:
    - From a phishing email that was sent to an user's mail box, either a binary or .zip attachment was executed after a password was entered
    - From a vulnerable browser accessed a compromised web site and the ransomware was executed after automatic download
  - For WannaCry like ransomware, the unpatched system service in kernel land was exploited and the ransomware was downloaded from the C2 server or dropped from the exploits
  - For ransomware like Ryuk (online reference can be found at our website), the malware was actually downloaded or copied to a shared folder from a compromised system running inside the organisation's internal network. Sometimes the ransomware was indeed planted and executed manually by the attacker either through an valid authenticated remote session or stealthy remote access tool (RAT) coming from the Internet

- **Incident categorisation, prioritisation and scoping**
  - Follow the IR plan or any security policies of the investigating organisation.
  - Determine the infection path by asking questions to identify how it was first found and which system was first being infected
  - Scope the incident to identify the number of infected machines and ask the organisations to provide a detailed network map and complete inventory of systems, including BYOD systems, used in the organisation (for determination and allocation of the resources)
  - The scope may need to be updated after the containment and eradication phases
  - Scoping needs to consider functional and information impacts of the incident
  - Estimate the time and resources to acquire

[7] https://www.virtualizationhowto.com/2011/02/beware-roaming-profiles-malware-infection/

forensics images of the infected systems and prioritisation to acquire images for the critical systems

- Consider to initiate the organisation's business continuity plan, (BCP) and discuss all the risks on limited scoping to the IR team and involving responsible senior management

- **Incident analysis – Checking for the artifacts of IoCs**
  - For common ransomware attacks, check the ransom note, capture the ransom note screen, identify the encrypted files unique extension and hash, anti-virus alerts, the timestamp of ransomware dropped; check the hash with online scanner and if live forensics is allowed; extract the ransomware for further analysis.
  - If the ransomware was downloaded from a web session, check the browser logs for other artifacts such as: IP address, domain or URL involved in the communication.
  - If EDR or SIEM tools was available, check the process tree with timestamps to identify when or where the ransomware was executed.
  - For ransomware like Ryuk or cases without suspicious alerts found, check the timestamp of ransomware and identify how the ransomware was delivered by checking the firewall or network device logs.
  - If the ransomware was copied by a RAT or other system utilities, such as PowerShell, try checking all system or event logs from the infected system
  - Continuous searching for the executable files by the identified hash and develop signature rules (such as yara rules) to scan all other unaffected systems for further malware hunting
  - If additional infections found, consider to expand the original defined scope
  - Consider to deploy compromise assessment tools or threat hunting tools to monitoring all running endpoints
  - Consider to deploy network intrusion detection system (IDS) inside the internal subnets (not only putting the IDS at the egress point but between all internal subnets and the critical systems) to monitor the abnormal network activities between the critical systems and all desktop machines

- **Incident reporting – escalation and reporting of the incident to appropriate parties (smart recipe: don't hide)**
  - Implement the organisation's security IR plan, if any
  - Notification to appropriate persons defined by the organisation's communication and notification plan.
  - During incident handling, the IR team needs to be provided the updated status. In some extreme cases the entire organisation's need to be notified after consulting

[8] https://maintenance.pb.com/pbcom/outage.html

the responsible senior management.

- If the incident is confirmed, consider to give notification to law enforcement, insurer, employees or relevant regulatory bodies according to the IR plan (smart recipe: don't hide. Example: Pitmey Bowes [8])
- Responsible senior management needs to be advised that there are serious inherence risks before considering to pay the ransom

Containment, Eradication & Recovery

The third phase, containment, is the initial attempts to mitigate the actions of the attacker, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organisation to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in pace for making containment-related decisions that reflect the level of risk acceptable to the organisation.

Containment includes following procedures to stop spreading of the ransomware or carry out necessary procedures to prevent the exfiltration of data. Containment can be performed concurrently with Analysis. Shutting down the critical servers infected with ransomware may have a significant impact on some organisations. Incident responders need to make a quick and reliable recommendations to the responsible senior management to determine the containment and recovery procedures in details.

Eradication consists of the longer-term mitigation efforts which include steps to remove ransomware from the systems or removing unknown malware or backdoors from the compromised systems. In Ryuk ransomware (Triple-Threat) attack case, because the ransomware was planted manually by the attackers through the compromised systems within the internal network, cleaning only the infected systems or servers through anti-virus scan will found the infections again in a short operational time. The ransomware will come back and "reimaging" the infected systems also found not work.

Containment and eradication often require drastic actions, but recovery is the process of getting the organisation network back to a state before the incident. Recovery include steps to restore clean data backup back to the compromised systems after a fresh installation. Newly installed systems need to be hardened and monitored to prevent reoccurrence. Recovery should be designed to all the infected organisation return its business to "normal". The organisation should define acceptable risks in dealing with the incident when they take back the possible infected systems back online. If such decision is made, incident responder needs to consider to deploy endpoint and network threat hunting tools to keep continuous monitoring of the infected network and systems.

- Common ransomware are not known to move laterally, it is good practice to isolate affected machines from the network (by disabling the network switch port to which an infected system is connected) as soon as a ransomware infection or presence of any other threat is suspected.
- Isolating affected machines also helps prevent ransomware from encrypting data on shared folders or mapped drives through the network.
- Immediately secure backup data or systems by calling them back to onsite fro a remote backup tape storage location
- Isolate the infected computers from the network immediately or blocking access to malicious network resources such as a domain, URLs or IP addresses

- Isolate or power-off affected devices that have not yet been completely corrupted
- Temporarily lock a user accounts or even an account of administrator group (sometime the organisation may found this is an unknown account created by the attacker) to control the intruder
- Disable system services or software that the attacker has exploited
- If possible, change all online account passwords and network passwords after removing the system from the network
- Identify all autorun locations for ensure ransomware or unknown malware will not be executed after reboot
- Remove all ransomware, related malicious software and tools installed by the attacker. Please note that simply download an antivirus tool to remove a particular ransomware on a ransomware infected machine may not be able to remove the threats completely. Ryuk is an example because it comes with other malware
- Reset all infected users, third-party accounts and even services accounts
- Re-create shared secrets including, VPN tokens, passwords or certificates
- If your organisation is infected with ransomware like Ryuk, we have provided a special checklist under the appendix to help you to handle the incident in an expedited manner.

Post-Incident Activity

Because the handling of a malware incident can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after the incident to prevent similar incidents from occurring.

Post-incident refers to the process of identifying lessons to be learned after actions and review. We need to answer basic questions like: (a) what happened? (b) have we done well in protecting the organisation's network? (c) could we have done better? And (d) shall we do differently next time?

Policies and procedures may need to be modified.

- Prepare a detailed Incident Response Plan and established an Incident Response Team
- If ransomware was found coming from a phishing email, track the sender and message by marking the source of spam
- Check email header for unique X-Mailer or send IP address information and add message transport rules
- Remind end-users to move the attack email to the "junk" folder and report spam or malicious emails to the IR or Threat team
- Consider to deploy DMAC and install anti-phishing solution
- Set appropriate rules to your IDS, firewall or browsers' plug-ins to block malicious websites
- Sinkhole the C2 domain on internal DNS servers
- Ensure proper patch management policy

- Ensure proper vulnerability policy
- Deploy advance end-point solution to keep real time continuous monitoring
- Deploy SIEM for critical subnets for detail security analytic monitoring
- Deploy application white listing to critical systems
- Establish up threat hunting capability
- Consider to take a proactive defence by implementation of Cyber Threat Intelligence (CTI) as a part of the Incident Response Cycle because once CTI fits into the incident response process, it help responders understand the adversaries in order to reduce the time it takes to detect, defence and remediate intrusions. (such as: handling Ryuk threat is different from common ransomware infections)

Frankie Li, Mika Devonshire and Ken Wong ■

PISA Journal

The Editorial Board

SC Leung
CISSP CCSP CISA CBCP

Joyce Fan
CISSP CRISC CISA

Ian Christofis
CISSP

Alan Ho
CISSP CISA CISM CGEIT

You can contribute to **PISA Journal** by:

. **Joining the Editorial Board**

. **Submitting articles to the Journal**

SC Leung,
Chief Editor
editor@pisa.org.hk

Next Issue:
Issue 31 (Mar-2020)

Event Snapshot

We Share. We Progress.

PISA JAM 2019 x CSA (25 May 2019)

PISA JAM 2019 x CSA was successfully held on 25 May 2019. Andy Ho, PISA Chairperson (left) and Claudius Lam, CSA Chairperson (right) gave Opening Speech

Hon. Charles Mok, our and our honorable guest delivered the Welcome Speech.

(ISC)2 APAC representative shared (ISC)2 latest update.

Event Snapshot

We Contribute. We Achieve.

PISA JAM 2019 x CSA (25 May 2019)

In the morning, several professional shared us latest knowledge.

Topic: Introduction to Private Intelligence Agency and its use of OSINT

(Top) Animus Chow

Topic: Cyber Insurance: Determining Security Maturity for Policy Preparation

(Middle) by Dale Johnstone

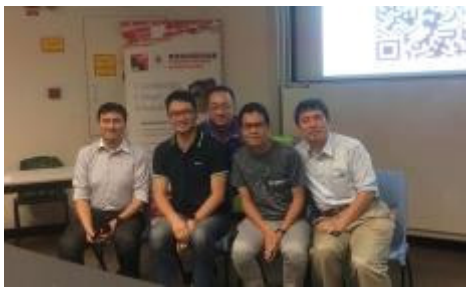
(Bottom) by Antony Ma

Event Snapshot

We Share. We Progress.

PISA JAM 2019 x CSA (25 May 2019)

More sessions and workshops are conducted.



Panel Discussion— Everything-as-a-Service in Cloud

Moderator: Otto Lee (back)

Panelist: (from left, front row) Frankie Wong, Vincent Ip, Claudius Lam, Ricci Ieong

Workshop: Wow, you have a CSOC?

by Frankie Li, Dragon Threat Labs

Workshop: Experience Sharing of Hacking Wireless HID control (keyboard & mouse)

by Daniel Yeung, AdvStar

Workshop: Digital Forensics Hands-on Practices form Korean Digital Forensics Challenge

- by Ricci Ieong, PISA Forensic SIG group leader

Event Snapshot

We Contribute. We Achieve.

Deep analysis and lessons learned from SingHealth Incident (22 Jul 2019)

In Singapore's worst cyber attack, hackers infiltrated the databases of SingHealth, the largest group of healthcare institutions here. The personal particulars of 1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong and a few ministers, were stolen. Matthew Wong of FireEye shared his research on this case and discussed the lesson learnt.

Event Snapshot

We Share. We Progress.

Joint AGMs 2019 cum Feature Talk: Seasonings to Improve Sustainability of your Information Security Programme (31 Aug 2019)

Around 40 PISA members joined PISA AGM.

Carol Lee shared her key seasoning tips to address cyber talent shortage issue and make a popular programme amongst stakeholders.

Event Snapshot

We Contribute. We Achieve.

The new Macau Cyber Security Law is on its way (26 Sep 2019)

Starting from July 2015, Macau started to prepare the law for cyber security. Eventually, the Macau Cyber Security law was published in June and will be effective in December 2019. Many people may feel cyber security law is a sensitive subject and the controls may be a bit over.

Professional Information Security Association

Vision

to be the prominent body of professional information security practitioners, and utilise expertise and

Many Ways You Can Benefit

Successful Career

Be up-to-date and be more competitive in the info-sec community – line up yourself with the resources you need to expand your technical competency and move forward towards a more successful career.

Networking

Enjoy networking and collaboration opportunities with other in-the-field security professionals and exchange technical information and ideas for keeping your knowledge up to date

Sharing of Information

Find out the solution to your technical problems from our email groups and connections with our experienced members and advisors.

Continued Education

Check out job listings information provided by members. Get information on continuing education and professional certification

Enjoy the discounted or free admissions to association activities - including seminars, discussions, open forum, IT related seminars and conferences organised or supported by the Association.

Realise Your Potential

Develop your potentials and capabilities in proposing and running project groups such as Education Sector Security, Mobile Security, Cloud Security, Honeynet, Public Policy Committee and others and enjoy the sense of achievement and recognition of your potentials

Professional Recognition

Benefit from the immediate access to professional recognition by using post-nominal designation

Membership Information

Enquiry email:
membership@pisa.org.hk

Membership Application Form:
http://www.pisa.org.hk/membership/member.htm

Code of Ethics:
http://www.pisa.org.hk/ethics/ethics.htm

Membership Requirements

Type	Fee (HK$)	Qualifications	Relevant Experience
Full	500	Recognized Degree in Computing discipline, OR other appropriate educational / professional qual.	3 years Info-Sec working experience
Associate	300	Tertiary Education	Info-Sec related experience
Affiliate	300	Interested in furthering any of the objects of the society	Nil
Student	Free	Full-time student over 18 years old	Nil

- *Relevant computing experience (post-qualifications) will be counted, and the recognition of professional examinations / membership is subject to the review of the Membership Committee.*
- *All members must commit to the **Code of Ethics** of the Association, pay the required fees and abide by the Constitution and Bylaws of the Association*