ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 7/25 (July)

Why Threat Intelligence Matters

INTRODUCTION

1. An increasingly digital world has brought about both opportunities and threats. The threats we face have grown in both scale and sophistication. Cybersecurity is no longer just a technical concern - it is strategic, operational, and national. From amateur "script kiddies" to organised crime groups, the range of cyber adversaries is broad, each with their own motivations and targets.

2. This report introduces readers to the foundational concepts of threat intelligence, including the types of threat actors, impacts of cyber threats, classification of cyber threat intelligence, and processes involved in threat response and threat hunting. Knowledge of these concepts can help organisations move towards proactive cybersecurity approaches, in turn building more resilient defences.

3. This report will draw insights from the Cybersecurity Course on Cyber Incident Response and Threat Analysis (CIRTA) that was organised by ACICE for cyber military practitioners to help readers gain a deeper understanding of cybersecurity and exchange perspectives on cyber challenges and threats across Southeast Asia.

IMPACT OF CYBER THREATS TO ORGANISATIONS

4. According to the United States' National Institute of Standards and Technology (NIST), a cyber threat is any circumstance or event with the potential to adversely impact organisational operations, organisational assets, or

individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. It is also the potential for a threat-source to successfully exploit a particular information system vulnerability.

5. The impact of cyber threats extends beyond the files stolen and systems disrupted. When threat actors obtain Personally Identifiable Information (PII) - which includes credit card numbers, Protected Health Information (PHI), and Personal Security Information (PSI), they can commit fraud or impersonate individuals. These cyberattacks can therefore cause monetary losses, legal liabilities, and reputational damage.

6. Additionally, cyberattacks targeting intellectual property (IP) can pose a serious threat to business innovation and competitiveness. IP may be stolen by competitors seeking strategic advantages, or by malicious actors seeking to demand ransom for the stolen data. Beyond immediate financial losses, IP theft can lead to reduced competitive edge, loss of stakeholder confidence, and lasting harm to organisations' reputation.

7. Threat actors may also target critical information infrastructure (CII), which refers to any computer or computer system necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or system will have a debilitating effect on the availability of the essential service in a nation. Threat actors may launch cyberattacks on CIIs as part of state-sponsored campaigns to destabilise or exert pressure on states, or to gain geopolitical leverage.

8. The impact of cyber threats on CIIs can be severe and cascading. A distributed denial of service (DDoS) attack on service providers may disrupt internet access, and a ransomware attack on a national health system may compromise patient safety. Disruption of these services and activities can devastate a nation's economy, trigger public panic, and erode trust in national institutions. In extreme cases, successful cyberattacks on CIIs can cause national security crises, especially if emergency services or defence establishments are affected.

IMPORTANCE OF CYBER THREAT INTELLIGENCE TO ORGANISATIONS

9. Cyber threat intelligence plays a critical role in helping organisations move from a reactive to a proactive posture. Rather than waiting for breaches to occur, threat intelligence allows organisations to anticipate threats, understand the behaviour of adversaries, and craft responses even before damage is done.

Case in point:
According to *Global Times*, SkyEye – the threat perception system that was used to help secure the 2022 Winter Olympics in Beijing – made use of cyber threat intelligence, machine learning, and other technologies to discover known advanced network attacks and unknown new types of hosts and servers in the network. SkyEye includes a traffic sensor that can retrieve and detect threats from network traffic, an analysis platform that can analyse network logs and offer threat summaries, as well as a honey pot to attract access from attackers to collect information for attack tracing. This was crucial in ensuring minimal disruption from cyberattacks during the high-profile event.

10. Cyber threats can be identified using Indicators of Compromise (IOCs) and Indicators of Attack (IOAs):

a. IOCs are the evidence that a cyberattack has occurred, and each attack has unique identifiable attributes. IOCs include malware file hashes, internet protocol addresses of servers that are used in attacks, domain names, as well as file names. Such IOCs help cybersecurity personnel identify what has happened in an attack and develop countermeasures.

b. IOAs focus on the motivation behind a cyberattack and the strategies attackers use to gain access to assets. IOAs help cybersecurity personnel generate a proactive security approach that can be reused across contexts and attacks. This helps defenders stop threats before damage is done.

11. Cyber threat intelligence also aids attribution efforts. While identifying the perpetrator of a cyberattack can be complex, the use of IOCs and IOAs can help cybersecurity personnel paint a picture of the threat actor involved in the cyberattack.

Case in point:
The 2020 SolarWinds Orion supply chain compromise demonstrated how cyber threat intelligence could support attribution. Analysts identified the SUNBURST backdoor which facilitated follow-on activities, including the deployment of additional payloads such as TEARDROP and Cobalt Strike. These IOCs and the broader tactics, techniques, and procedures (TTPs) allowed analysts to attribute it to APT29, also known as Cozy Bear. This intelligence was mainly generated retrospectively, as no intelligence about SUNBURST had been available before the supply chain compromise.

12. Cyber threat intelligence can be categorised into three types: the strategic level, tactical level, and operational level:

a. Strategic intelligence. This level of intelligence informs top decision-makers and helps them understand the threat they are up against. Strategic intelligence should give decision-makers a proper sense of what the main threat capabilities and motivations are (e.g., theft, financial gain), their probability of being a target, and potential consequences of a cyberattack.

b. Operational intelligence. This level of intelligence informs those making day-to-day decisions. These people who are in charge of defining priorities and allocating resources should have information about which groups may target the organisation and which ones have been the most recently active. An example of operational intelligence is a list of common vulnerabilities and exposures (CVEs).

c. Tactical intelligence. This level of intelligence informs those in need of instantaneous information. Recipients of this information should have a complete understanding of what behaviours they should pay attention to in order to identify threats. Example of tactical intelligence include IP addresses as well as domains and Uniform Resource Locators (URLs).

IDENTIFYING THE THREATS – THE THREAT INTELLIGENCE CYCLE

13. The threat intelligence cycle is a process to manage cyber threats. It helps organisations gather, analyse, and apply information about cyber threats. This ensures that cyber threat intelligence remains relevant and actionable.

a. Planning and targeting. This stage involves identifying intelligence requirements, which means determining information that decision-makers need but do not know enough about. An intelligence requirement is any subject upon which there is a need for the production of intelligence, and any requirement for intelligence to fill a gap in knowledge or understanding of threats. It also involves identifying key security concerns and main reasons why the organisation in question may be targeted. It is useful as well to already identify potential threats and establish priorities and frameworks.

b. Preparation and collection. This stage is about defining and developing the methods to obtain the information regarding the intelligence requirements.

c. Processing and exploiting. The data collected has to be processed to generate information. Not all data can always be processed, and the data that does not get processed may become lost intelligence.

d. Analysis and production. The fourth step involves interpreting the data, identifying patterns, and producing intelligence that is actionable. To execute this step well, cyber threat intelligence analysts need to filter biases to ensure the analysis is objective and accurate. Finished intelligence produced by analysts may include assessments and judgements about the implications of the information for the organisation.

e. Dissemination and integration. Those in charge of doing this must consider which issues need the intelligence most urgently and who should receive the intelligence, among other factors.

f. Evaluation and feedback. This final stage is difficult because there tends to be a lack of good feedback mechanisms. Establishing robust mechanisms helps intelligence producers make necessary adjustments to produce more useful and relevant information. Information can be evaluated based on criteria such as accuracy, bias, and timeliness.

Taken from Cisco Systems

14. Good cyber threat intelligence can be critical for successful threat hunting, which is meant to identify and mitigate potential threats before they can cause significant damage or data breaches. For example, according to Estonia's Ministry of Economic Affairs and Communications, Estonia's active sharing of cyber threat intelligence helped prevent successful attacks against European Union and North Atlantic Treaty Organisation member states. Threat hunting is a proactive approach that focuses on identifying threats early on. It is also an ongoing and interactive process that involves continuous monitoring of the IT environment. Without quality threat intelligence, threat hunting may become unfocused and inefficient.

15. Types of threat hunts include intel-driven hunts which are triggered by threat intelligence, entity-driven hunts which revolve around high-risk or high-value entities, and tactics, techniques, and procedures (TTP)-driven hunts which are focused on threat actors' known TTPs.

16. Effective threat hunting involves collaboration among different teams within an organisation, including security operations, incident response, and threat intelligence teams. Threat hunters should also understand core topics in cyber threat intelligence, including IOCs, IOAs, and advanced persistent threats (APTs). When properly resourced and guided by threat intelligence, threat hunting becomes a powerful capability for early detection and proactive defence.

IDENTIFYING THE THREAT ACTORS

17. Threat actors are any individuals or groups who perform cyberattacks. Their intentional malicious acts against digital systems may be motivated by a range of goals, including financial gain and industrial espionage.

18. Common categories of threat actors include:

Taken from Cisco Systems

19. Understanding who the threat actors are and what motivates them are critical components of developing effective threat intelligence and cybersecurity strategies. By recognising the various categories of attackers, organisations can better assess their risk exposure and tailor their approaches accordingly. By analysing the behaviours and intentions of these threat actors, organisations can gain the contextual awareness to prioritise threats and take effective pre-emptive actions.

CONCLUSION

20. Threat intelligence transforms cybersecurity from a reactive into a proactive process. It offers organisations the foresight needed to anticipate, detect, and respond to cyber threats quickly and precisely. By understanding the landscape, potential threat actors, and TTPs, organisations can better defend their systems and people. As digital threats evolve, organisations' threat intelligence must also improve. In an era where cyber threats are increasingly trans-boundary in nature, strong threat intelligence capabilities and continued cooperation in this domain can help enhance overall cyber defence.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

. . . . .

REFERENCES

1. Bing Dwen was used as bait for cyberattacks at Beijing 2022. https://www.globaltimes.cn/page/202202/1252043.shtml

2. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

3. SolarStorm Supply Chain Attack Timeline. https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

4. Cybersecurity Strategy 2024-2030: 'Cyber-Conscious Estonia'. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf