ACICE Issue 1/22 (January)

ACICE Monthly Digest

A monthly round-up of significant news around the world

ACICE

ADMM Cybersecurity and
Information Centre of Excellence

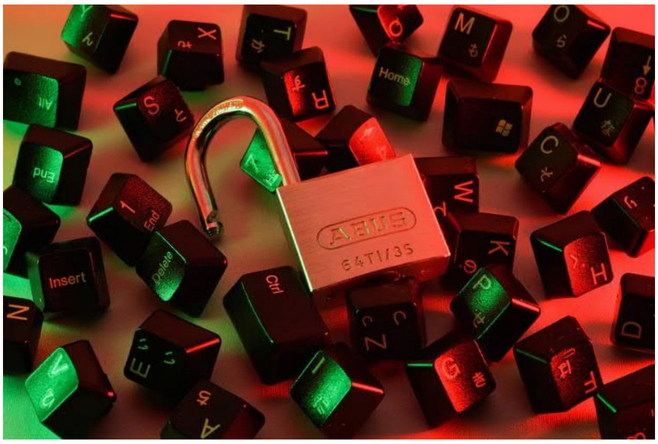
Information and Cybersecurity

Cybercriminals Discuss New Business Model For Zero-Day Exploits

- Researchers from digital threat intelligence firm Digital Shadows observed that cybercriminals were now considering renting out zero-day vulnerabilities under an “exploit-as-a-service” model.

- According to their Nov 2021 report “Vulnerability Intelligence: Do You Know Where Your Flaws Are?”, zero-day vulnerabilities are among the most expensive flaws advertised on cybercrime forums. The promise of a high impact on critical targets comes with a hefty price tag, with prices for these vulnerabilities reaching USD10m in auctions on dark web forums.

- Given the high prices, cybercriminals have developed a new leasing model to maximise their earnings - “lending” the vulnerabilities to multiple users in the interim while waiting for a definitive buyer.



- While this model lowers the barriers for cybercriminals to access sophisticated exploits, the larger number of users also increases the possibility that the vulnerability is detected early and patched, causing it to lose its “zero” status and its value.

Humanitarian Assistance and Disaster Relief

Is Blockchain The Future Of Humanitarian Aid? The World Food Programme Hopes So

- Since 2017, the World Food Programme has been working with other humanitarian organisations to improve the distribution of cash-based assistance to refugees through its *Building Blocks Programme*, which uses blockchain technology.

- Previously, multiple humanitarian organisations serving the same refugee population would operate their own systems to distribute assistance. This could lead to some beneficiaries having an excess or shortage from what they actually need due to miscommunication, oversight, or duplication in the distribution network.

- Blockchain technology could provide a single system for all humanitarian organisations to operate on, allowing for greater transparency to track, consolidate, and distribute aid to the appropriate beneficiaries. This also provides greater convenience for aid beneficiaries, who need to manage only one account for aid received from multiple organisations. Furthermore, blockchains eliminate the need for a third-party financial institution to process these transactions, removing transaction fees and allowing more aid to reach those who need it.

- One possible future use of blockchain in humanitarian aid includes providing refugees with secure digital identities and documentation as they rebuild their lives, so that such information is not lost if/when they are repatriated.

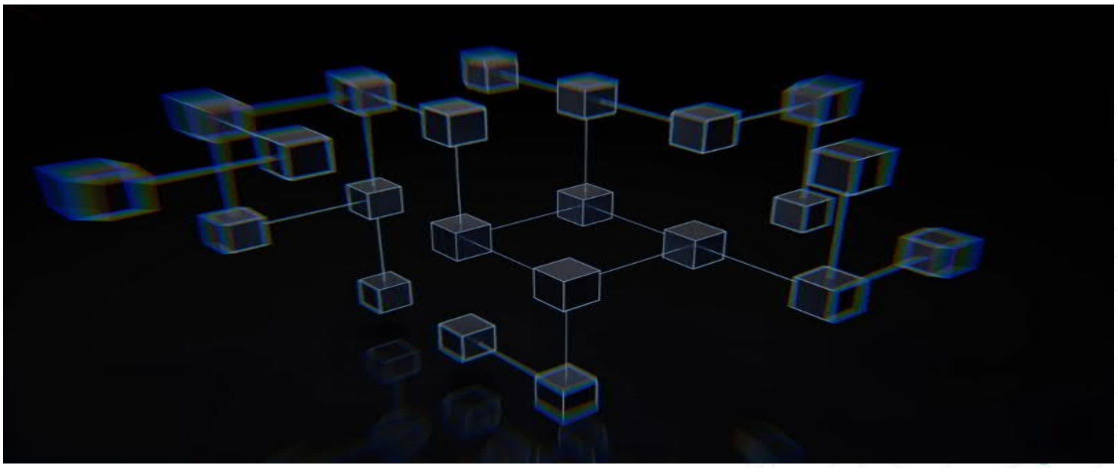
CARE Chooses Celo As First Blockchain Partner In Latin America

- Leading humanitarian organisation CARE USA has selected Celo – an open-source blockchain ecosystem focused on making decentralised financial systems and tools accessible to anyone with a smartphone – to exploit the benefits of blockchain technology to administer aid.

- Many centralised systems are not able to adequately track the transfer of funds from donor to beneficiary. In many instances, the process is slow, inaccurate, and vulnerable to fraud. With the Celo blockchain – which serves as an open, accessible, and easily auditable ledger that no one can edit – it is easy to trace funds from their origin to the intended recipients.

- The transparent nature of Celo's blockchain technology also allows transactions to be recorded in real-time, which allows for faster payment and real-time analytics that current systems do not provide.

- The lack of financial intermediaries in the blockchain process also eliminates the operating costs for cross-border transfers and payments, allowing a greater proportion of funds to reach recipients.



Terrorism

Update On Terrorism In Southeast Asia

- There were three reported terror attacks in the Philippines from Dec 2021 to Jan 2022.

- Notably, the attack against a transmission tower in Maguing, Lanao del Sur in Dec 2021 was claimed by ISIS-East Asia through the IS-East Asia Province media unit and the ISIS official weekly newsletter, al-Naba.

- Of note is the target of this terror attack. While attacks on electric infrastructure are common in Iraq and Syria, these are less frequently seen in Southeast Asia.

- Separately, a total of 31 Jemaah Islamiyah (JI) and Jamaah Ansharut Daulah (JAD) members were arrested in Indonesia in the same period.

- Authorities managed to uncover and foil a plot in Central Kalimantan by three JAD members, who were planning to conduct several "acts of terror" there.

JI Emerges From The Shadows, Playing The Long Game

- Regional security crackdowns on JI have forced the terrorist grouping to adapt its strategy, in favour of a "hybrid", longer-term approach towards extremism.

- JI appears to have recognised that its earlier focus on violent attacks drew significant attention and forceful responses from the authorities, which have sharply decimated its base and operations.

- As such, it has changed its tactics. Instead of resorting to violence to spread its radical ideology, it is now seeking to entrench itself in legitimate businesses, charities, religious institutions, as well as local politics to propagate its views. Such a move will allow it to also garner more resources, cultivate ground support, and seek political legitimacy in support of its eventual goal of establishing a caliphate.

- Despite JI's "gentler" approach towards extremism, it is important for the authorities to not let their guard down and continue to maintain pressure on the grouping. This will help ensure continued effective deterrence against the group.

Maritime Security

Maritime and Port Authority of Singapore (MPA), Maritime Sector Holds Inaugural Cybersecurity Exercise

- MPA held its inaugural sector-wide maritime cybersecurity exercise, “Exercise CyberMaritime 2021”, in Nov 2021, which involved port terminal operators PSA Corporation and Jurong Port, and shipping company Pacific International Lines.

- The exercise focused on the cyber-physical implications of potential cyberattacks and the increased risks in data theft and loss. Several scenarios covering data leaks, ransomware, web defacement, distributed denial-of-service (DDoS), supply chain attacks, and the compromise of critical maritime and port systems were played out. Through this exercise, MPA was able to test the sector’s operational responses – cybersecurity incident management, emergency response plans, and crisis communications – to the simulated incidents.

- With the rapid digitalisation of the maritime industry, Chairman MPA Niam Chiang Meng noted that it was “imperative” to better prepare against the threat of cyberattacks, particularly given Singapore’s position as a key node in the global supply chain.

Annex

Sources

Information and Cybersecurity

- Cybercriminals Discuss New Business Model For Zero-Day Exploits
  - https://www.techtarget.com/searchsecurity/news/252509820/Cybercriminals-discuss-new-business-model-for-zero-day-exploits
  - https://www.digitalshadows.com/blog-and-research/vulnerability-intelligence-whats-the-word-in-dark-web-forums/

Humanitarian Assistance and Disaster Relief

- Is Blockchain The Future Of Humanitarian Aid? The World Food Programme Hopes So
  - https://www.maddyness.com/uk/2021/12/16/is-blockchain-the-future-of-humanitarian-aid-the-world-food-programme-hopes-so/

- CARE Chooses Celo As First Blockchain Partner In Latin America
  - https://reliefweb.int/report/ecuador/care-chooses-celo-first-blockchain-partner-latin-america

Terrorism

- Update On Terrorism In Southeast Asia
  - https://www.philstar.com/nation/2021/12/05/2145755/pnp-probes-lanao-ngcp-tower-blast/amp/

- The Big Read: Jemaah Islamiyah Emerges From The Shadows, Playing The Long Game
  - https://www.channelnewsasia.com/singapore/jemaah-islamiyah-terrorist-group-indonesia-isd-20th-anniversary-al-qaeda-2373556
  - https://www.channelnewsasia.com/asia/jemaah-islamiyah-infiltrating-indonesian-institutions-terror-group-2332941

Maritime Security

- MPA, Maritime Sector Holds Inaugural Cybersecurity Exercise
  - https://sbr.com.sg/shipping-marine/news/mpa-maritime-sector-holds-inaugural-cybersecurity-exercise
  - https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/5c361bf4-3059-493c-af28-c6a2726ac16d

Contact Details

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

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence