RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 155 – 27 October 2021

Ransomware: ASEAN Leaders Should Seize the Momentum

By Sithuraj Ponraj

SYNOPSIS

Increasing ransomware attacks have the potential to undermine daily lives by crippling critical infrastructure and disrupting essential services. ASEAN's increasingly integrated digital economy makes it especially susceptible to fallout from such potential attacks. As ASEAN leaders meet in summit this week, they should take decisive measures to address the ransomware scourge.

COMMENTARY

RANSOMWARE WAS high on the agenda at the Singapore International Cyber Week and GovernmentWare (GovWare) Conference held earlier this month from 4-8 October. Will it be among the talking points on cybersecurity of ASEAN leaders who are meeting virtually in summit this week, hosted by Brunei as ASEAN chair?

Recent high profile ransomware attacks across the world against energy grids, water plants, government agencies, hospitals as well as major fuel and food suppliers have highlighted the damage that can be done by malicious actors when they gain access to computer networks and lock their owners out until they pay a ransom. Such attacks have the potential to cripple critical infrastructure, disrupt the delivery of essential services and affect the functioning of a large number of businesses across geographic boundaries at the same time.

Growing Trend

Many ransomware attacks also include a double extortion or 'hack and leak' element where attackers threaten to leak hacked data unless a ransom is paid – thus putting large swathes of sensitive and confidential government and business data at risk of public exposure, with an accompanying erosion in public trust and confidence.

Despite the heightened attention, ransomware attacks are expected to increase rather than decrease in the short-term future. Speaking at Mandiant's Cyber Defence Summit on 5 Oct 2021, US National Security Agency (NSA) Director General Paul Nakasone said the rate of ransomware attacks would not slow down for the next five years and added that the United States would face ransomware attacks 'every single day' during this period.

While ransomware itself is not new – ransomware attacks have been reported since at least the early 2000s – several key factors have come together to make ransomware an urgent national security, economic and social threat facing the international community.

Drivers of Ransomware's Growing Threat

Firstly, the increasing pace of digitalisation and the migration online of government and business activity spurred by the COVID-19 pandemic and the generally less stringent security posture that accompanies work from home arrangements have significantly increased the attack surface available for cyber-attacks.

Secondly, the growing complexity of international supply chains and the increased sophistication of ransomware attacks have both made ransomware an especially difficult problem to address. Ransomware attacks exploiting supply chain vulnerabilities such as the Kaseya attack have an ability to quickly propagate and cripple the delivery of a very large number of critical and essential services as well as business operations at the same time.

The development of Ransomware-as-a-Service (RaaS) business model where cybercriminals organise themselves to provide hacking tools and support to would-be hackers at relatively affordable prices has lowered the technical entry bar and cost for potential hackers to enter the field. At the same time it provided hackers with the possibility of tapping on resources and support made available by these criminal organisations to conduct more sophisticated attacks.

Thirdly, prosecuting cybercriminals located across various jurisdictions and the recovery of ransom amounts paid remain a challenge. Law enforcement efforts continue to be bedevilled by the lack of effective international and regional cross-jurisdictional arrangements to pursue and bring malicious cyber actors to justice; worsening it is the complicity of some governments with criminal actors and the lack of resources and capacities in others to take decisive action.

Similarly, the relative anonymity of cryptocurrency transactions and the current lack of effective measures to regulate cryptocurrency continue to be serious challenges.

Ransomware Threat in ASEAN

Countries in the ASEAN region are not immune to the ransomware threat. A 2021 ASEAN Cyberthreat Assessment by INTERPOL lists ransomware as one of the top five cyber threats facing the region in 2020 and beyond. In July this year, Singapore reported that it had seen a 154% increase in ransomware attacks over 2020.

With an increasingly integrated digital economy expected to grow to US$300 billion by 2025, ASEAN as a region can leverage the many strong regional cybersecurity initiatives already in place to better position itself to address the ransomware threat in coming years.

This is especially so given the existing cyber policy and operational capacity gaps in countries across the region that may prove to be a point of vulnerability as the regional economy becomes more integrated. From a policy perspective, ASEAN could consider developing a coordinated and coherent regional ASEAN strategy for addressing and mitigating ransomware threats.

This could be done as part of the upcoming second iteration of the ASEAN Cybersecurity Cooperation Strategy likely to be tabled at the next ASEAN Digital Ministers' Meeting. It is expected to include a recognition of the need for strong international and regional collaboration as well as guidance on regional policy, operational, diplomatic, and capacity building coordination needed in addressing the ransomware threat.

Time for an ASEAN Working Group on Ransomware

Given the cross-cutting nature of ransomware attacks, it would be useful to consider the setting up of a cross-sectoral Working Group on Ransomware that could oversee the operationalisation of the strategy. The Working Group could potentially be formed under the aegis of the ASEAN Cyber Coordinating Committee which already enjoys the mandate for such cross-sectoral coordination.

Working closely with multi-stakeholders in industry and academia, the Working Group could comprise both security and economic sectoral representatives and develop guidance on issues such as technical standards for the management of third party vendors and supply chains and cryptocurrency regulation, taking into account regional and national needs and priorities.

Operationally, ASEAN could also build on existing regional CERT-CERT cooperation and information sharing mechanisms to facilitate the real-time exchanges of information on potential and on-going ransomware attacks. CERT is the Computer Emergency Response Team. Existing cooperation could also be enhanced to maintain a registry of known ransomware actors and their modus operandi as well as assist in the dissemination of ransomware-related alerts and advisories.

The dissemination of real-time information concerning the Colonial Pipeline ransomware attack in May which disrupted fuel supplies in the US has been credited with helping to mitigate its impact.

A mechanism allowing such information exchanges would be invaluable in supporting national ASEAN CERTs and businesses in addressing ransomware attacks. This is especially so if such information exchanges are combined with regular drills and capacity building programmes tailored to equip ASEAN operators and analysts in responding to ransomware attacks.

The soon-to-be-established ASEAN CERT would be ideally placed to play a leading

role in these operational efforts. Ransomware has the potential to affect us all – from governments to the man in the street. ASEAN leaders can – and should – seize the momentum of their current summit to address it.

Sithuraj Ponraj is Senior Visiting Fellow at the RSIS Centre of Excellence for National Security (CENS). He was previously Director of the International Cyber Policy Office in Singapore's Cyber Security Agency, where he played a key role in the development of Singapore's international cybersecurity strategy.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg