JENAYAH DIGITAL

Malathi Letchumanan dan Muhammad Rezal Kamel Ariffin (Foto Penulis)

ANCAMAN JENAYAH SIBER

Menurut Polis Diraja Malaysia, jenayah siber ialah jenayah yang paling bergaya dan menguntungkan sejak kebelakangan ini. Jenayah ini dilaporkan telah mengatasi jumlah kes penagihan dadah di Malaysia. Yang lebih mengejutkan, statistik menunjukkan bahawa 70 peratus kes jenayah komersial, kini dikategorikan sebagai jenayah siber.

Pada 28 Februari 2018, Trend Micro Incorporated, sebuah syarikat yang menawarkan perkhidmatan penyelesaian masalah berkaitan dengan keselamatan siber melaporkan bahawa Malaysia berada pada kedudukan tertinggi di Asia Tenggara (SEA) bagi kes *Malware* yang melibatkan 16 juta ancaman sepanjang tahun. Di samping itu, Malaysia juga dikategorikan sebagai sasaran ancaman siber paling popular di rantau ini yang melibatkan hampir 350 000 *Uniform Resource Locator* (URL) berbahaya dilancarkan di dalam negara. Dalam hal ini, hampir 10.5 juta orang telah menjadi mangsa. Malaysia juga menduduki tempat kedua selepas Singapura yang menerima ancaman *Business Email Compromise* (BEC).

Menurut Pegawai Kanan, Kementerian Komunikasi dan Multimedia (KKMM), pada suku pertama tahun 2019, rakyat Malaysia melaporkan sebanyak 2207 kes jenayah siber melibatkan RM67.6 juta. Tiga aktiviti jenayah siber yang paling popular antaranya termasuklah penipuan melalui panggilan telefon, 773 kes (RM26.8 juta kerugian); penipuan pembelian dalam talian, 811 kes (RM4.2 juta); dan *African Scam*, 371 kes (RM14.9 juta).

Berdasarkan jadual, kes jenayah siber yang dilaporkan di Malaysia dari tahun 2010 hingga 2019 oleh MyCERT terdiri daripada insiden seperti laporan kerentanan (*vulnerabilities report*), penolakan perkhidmatan (*denial of service*), gangguan siber (*cyber harassment*), percubaan pencerobohan (*intrusion attempt*), peniruan kandungan (*content related*), kod hasad (*malicious code*), *pencerobohan* (*intrusion*), *spam*, dan penipuan (*fraud*).

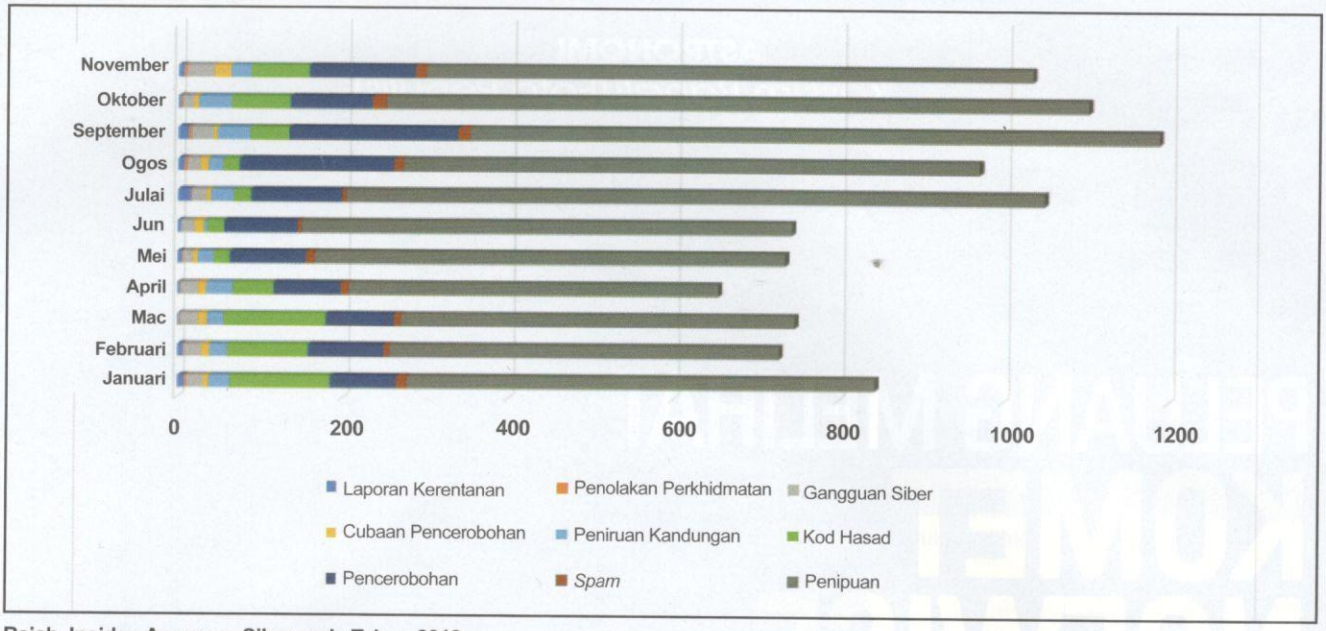
Berdasarkan data, kes jenayah siber yang dilaporkan di Malaysia berkisar antara 7900 hingga 16 000 kes menunjukkan ancaman jenayah siber di Malaysia berada dalam keadaan kritikal dan memerlukan penyelesaian yang berkesan. Namun begitu, ada sesetengah pihak yang berpendapat bahawa jumlah sebenar jenayah siber di Malaysia adalah lebih tinggi berbanding dengan laporan oleh MyCERT. Hal ini demikian kerana tidak semua mangsa yang melaporkan insiden kepada pihak berkuasa.

Kadar jenayah siber di Malaysia dikatakan semakin meningkat pada setiap tahun. Menurut Barclay, R.A dalam "Regulatory economics: Cyber security who cares? Threats and apathy worldwide outlook uncertain, *Nat, gas electricity* 30, 30–32", satu sebab utama

Jadual Kes Ancaman Siber yang dilaporkan di Malaysia.

Tahun	Bilangan Kes
2019	9805
2018	10699
2017	7962
2016	8334
2015	9915
2014	11918
2013	10636
2012	9976
2011	15218
2010	8090

(*Sumber*: MyCERT)



Rajah Insiden Ancaman Siber pada Tahun 2019.

ialah kurangnya kesedaran pengguna tentang ancaman tersebut.

Menurut Ketua Pegawai Eksekutif, Cybersecurity Malaysia, Datuk Dr. Amirudin Abdul Wahab, sebanyak 99 peratus serangan siber berjaya di Malaysia kerana kesilapan manusia. Manusia dikatakan mudah melakukan kesilapan seperti membuka lampiran e-mel yang mencurigakan dan mengaktifkan pautan *phishing*.

Amirudin turut menegaskan bahawa pemilikan teknologi terbaik sahaja tidak dapat menghalang serangan siber, tetapi mendidik orang awam termasuk pelajar sekolah rendah, sekolah menegah, universiti, orang awam, suri rumah, dan generasi emas tentang cara melindungi ruang siber ialah faktor yang paling penting.

Menurut Sophos dalam *The Future of Cybersecurity in Asia Pacific and Japan–Culture*, *Efficiency*, *Awareness* (2019) pada tahun 2019 di Malaysia, kebanyakan golongan eksekutif sering menganggap bahawa syarikat mereka "tidak akan dapat diserang, akan mendapat serangan, tetapi mereka tidak dapat melakukan apa-apa; keselamatan siber adalah mudah, dan profesional keselamatan siber membesar-besarkan ancaman dan isu". Kenyataan ini agak membimbangkan dan menunjukkan bahawa kesedaran tentang keselamatan siber dalam kalangan golongan profesional yang berpendidikan tinggi di Malaysia masih rendah dan perlu ditingkatkan untuk melindungi ruang siber mereka.

Zainudin, Z. S. dan Molok, N. N. A. dalam "Advanced Persistent Threats Awareness and Readiness: A Case Study in Malaysian Financial Institutions. In *2018 Cyber Resilience Conference (CRC)* (pp. 1–3) IEEE" telah menyiasat tahap kesedaran pengurus keselamatan siber mengenai *Advanced Persistent Threat* (APT) di institusi kewangan di Malaysia.

Hasil kajian menunjukkan bahawa faktor yang mempengaruhi kesedaran APT dalam kalangan pekerja institusi kewangan, ialah penekanan terhadap pembelajaran tidak rasmi APT, motivasi kewangan penyerang, risiko reputasi institusi kewangan, dan ketersediaan keperluan pengawalseliaan kewangan untuk melindungi institusi kewangan daripada risiko.

Selain itu, kajian yang dilakukan terhadap pelajar sekolah rendah, sekolah menengah dan institut pengajian tinggi juga menunjukkan tahap kesedaran mereka terhadap ancaman siber amat rendah dan perlu dipertingkatkan. Pelajar ini gian menggunakan alam siber tanpa menitikberatkan ancaman siber yang menanti mereka.

Berdasarkan kajian yang dilakukan oleh Ariffin, Mokhtar, Hood, Tiun, dan Jambari dalam "Parental Awareness on Cyber Threats Using Social Media. *Jurnal Komunikasi*: *Malaysian Journal of Communication*, 35, 485–498", mendapati bahawa ibu bapa kurang peka dengan aktiviti dalam talian anak-anak mereka. Hal ini secara langsung boleh menyebabkan anak-anak mereka mudah terdedah kepada ancaman siber.

Secara keseluruhannya, tahap kesedaran ancaman siber dalam kalangan masyarakat Malaysia amat rendah dan perlu ditingkatkan. Pihak kerajaan dan Badan Bukan Kerajaan perlu menganjurkan pelbagai program yang boleh mendidik masyarakat Malaysia tentang kesan ancaman siber dan kaedah untuk menghindari ancaman siber.

Dr. Malathi Letchumanan, Pensyarah di Institut Penyelidikan Matematik, Universiti Putra Malaysia Serdang, Selangor.