Perkasa sistem keselamatan siber negara elak digodam

Hubungan diplomatik antara Korea Utara dengan Malaysia terputus sebagai tindak balas terhadap tindakan negara ini mengekstradisi rakyat mereka ke Amerika Syarikat (AS), membuka kemungkinan berlaku ancaman siber.

Korea Utara membangunkan tentera siber secara aktif sejak tahun 2000 dengan kekuatan dianggarkan 7,000 orang. Tujuan utamanya adalah menjamin kelangsungan rejim, mempamerkan kekuatan dan mempertahankan reputasinya pada peringkat antarabangsa, sekali gus mengekalkan kawalan domestik.

Qamarul Nazrin Harun

Melihat sifat serangan siber sentiasa berubah, corak serangan dapat dilihat dengan tiga tujuan utama. Pada peringkat awal, serangan siber hanya untuk menyebabkan gangguan Penolakan Perkhidmatan Terdistribusi (DDoS).

Ia berkembang dan berubah menjadi operasi pengintipan serta pencurian maklumat (espionage), manakala peringkat akhir, bertujuan mendapatkan keuntungan kewangan.

Biasanya, serangan DDoS berupaya melumpuhkan jaringan komputer dengan cara membanjirkan data secara serentak. Serangan DDoS pertama kempen *4th of July* pada 2009 menjadikan Korea Selatan dan AS sebagai sasaran rejim Pyongyang.

Mereka menyasarkan Rumah Putih, Pentagon dan *Washington Post* sehingga laman web Pejabat Presiden dipenuhi permintaan akses dihasilkan perisian hasad (malware).

Pada Mac 2011, kempen *Ten Days of Rain* berlaku dengan serangan siber besar-besaran terhadap Pejabat Presiden, Kementerian Luar, Perkhidmatan Perisikan Negara dan beberapa institusi kewangan di Korea Selatan.

Perisian hasad disuntik pada dua laman web perkongsian fail *peer-to-peer* sehingga menjejaskan kira-kira 40 laman web dan 11,000 komputer peribadi.

Serangan siber ke atas Bank Nonghyup memusnahkan 273 daripada 587 pelayan bank dengan penggodam menyusup masuk ke dalam komputer peribadi bank lebih tujuh bulan sehingga dapat meletakkan kod jahat di seluruh rangkaian.

Serangan siber terburuk pernah direkodkan ialah *Dark Seoul Attack* terhadap Korea Selatan pada 20 Mac 2013. Sistem komputer Bank Shinhan dan Bank Nonghyup terpaksa ditutup sementara, malah Bank Jeju melaporkan penutupan rangkaian di beberapa cawangannya.

Institusi kewangan terbabit terpaksa mengambil masa berminggu-minggu untuk memulihkan sistem sepenuhnya dengan hanya 10 peratus laman web berfungsi dalam dua hari, manakala hampir 48,000 mesin perbankan tidak dapat digunakan.

Serangan DDoS terakhir direkodkan pada 25 Jun 2013, iaitu ulang tahun ke-63 meletusnya Perang Korea.

Penjenayah siber menyasarkan laman web Pejabat Presiden dan beberapa laman media rasmi sehingga merosakkan 69 pelayan komputer. Data peribadi anggota tentera AS dan Korea Selatan digodam serta dimuat naik ke laman web umum.

Aktiviti pengintipan dan pengumpulan maklumat, terutama strategi ketenteraan turut disasarkan dalam serangan siber Korea Utara. Serangan pengintipan pertama direkodkan ialah *Kimsuky* pada September 2013.

Ia menyasarkan kumpulan pemikir Korea Selatan seperti Institut Sejong, Institut Analisis Pertahanan Korea Selatan, Kementerian Penyatuan dan syarikat pelayaran Hyundai Merchant Marine.

Serangan siber dilakukan dalam bentuk penyebaran perisian hasad ke dalam sistem menggunakan teknik *spear-phishing* terhadap e-mel peribadi dengan tujuan mencuri kata laluan dan perincian keselamatan.

Sebulan selepas serangan siber terhadap Sony Pictures, penjenayah menyasarkan Korea Hydro and Nuclear Power (KHNP). Kira-kira 10,000 maklumat pekerja, dokumen mengandungi reka bentuk dan manual reaktor dicuri daripada KHNP.

Sebanyak 5,986 e-mel pancingan data dihantar bertujuan menyebarkan kod berbahaya ke sistem teknologi maklumat (IT) loji kuasa.

Modus operandi mempunyai persamaan dengan serangan *Kimsuky*. Malah, ia lebih terperinci dan sulit berbanding serangan DDoS yang dilakukan terang-terangan.

Secara tidak langsung, serangan siber itu menimbulkan kebimbangan terhadap kemampuan tentera siber Pyongyang melumpuhkan infrastruktur sasaran.

Pada Mac 2016, 40 telefon pintar pegawai Korea Selatan digodam tentera siber Korea Utara. Mereka mengakses perbualan telefon, mesej teks dan pelbagai maklumat sensitif lain.

Ini menunjukkan taktik serangan siber Korea Utara berkembang dan diperluaskan domain operasinya ke teknologi mudah alih.

Daewoo Shipbuilding and Marine Engineering Co Ltd turut menjadi sasaran pada April 2016. Hampir 40,000 dokumen termasuk 60 fail sulit mengandungi pelbagai maklumat teknologi pembinaan, cetak biru, sistem senjata dan penilaian kapal serta kapal selam.

Kumpulan penjenayah siber bertanggungjawab melakukan sebahagian besar jenayah terbabit menamakan diri sebagai Lazarus Group. Operasi itu sangat agresif berikutan pelbagai peristiwa dilihat mencabar kuasa rejim Pyongyang.

Serangan siber berbentuk pengintipan dan pencurian maklumat lebih menonjol sekitar 2013 hingga 2016.

Bagaimanapun, pada 2017 dan 2018, kuasa rejim Pyongyang menerima tekanan kerana program senjata nuklearnya. Natijahnya, Korea Utara melancarkan serangan siber terhadap institusi kewangan.

Pada April 2017, pertukaran mata wang kripto Korea Selatan, YouBit diserang sehingga mengakibatkan kecurian sebanyak bitcoin 3816.2028 (RM20.7 juta). Sekitar Disember, ia diserang sekali lagi dengan kerugian tiga kali ganda dilaporkan, iaitu kira-kira AS$15.6 juta (RM64.5 juta).

Ia dilakukan oleh sekumpulan penggodam Blunenoroff yang juga subkumpulan Lazarus dan mengakibatkan YouBit kehilangan 17 peratus asetnya sehingga memaksa untuk mengisytiharkan muflis.

Institusi pertukaran mata wang kripto Korea Selatan sekali lagi disasarkan pada Jun 2018. Coinrail dilaporkan kehilangan AS$37 juta (RM153.1 juta), manakala Bithumb pula rugi AS$40 juta (RM165.5 juta).

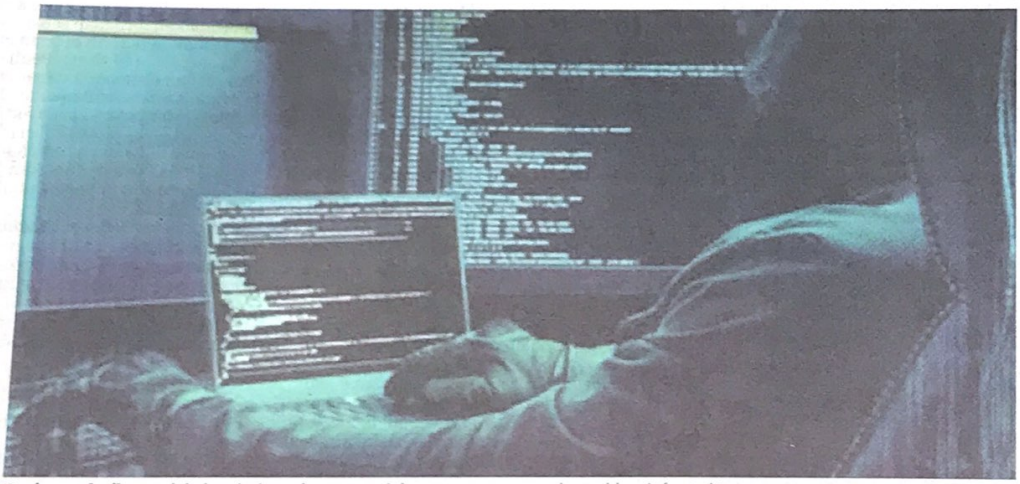
Impaknya, nilai bitcoin menurun sebanyak 5 peratus, sekali gus mencetuskan ketakutan pelabur untuk melabur di pasaran tidak terkawal. Serangan siber terhadap institusi kewangan wajar diberi perhatian khusus pada peringkat global.

Korea Utara sering dikaitkan dengan pencurian mata wang kripto terbesar dunia seperti serangan siber terhadap Bank Tien Phong, Vietnam; kecurian AS$81 juta (RM335.1 juta) daripada Bank Pusat Bangladesh; pemindahan AS$60 juta (RM248.2 juta) daripada Far Eastern International Bank di Taiwan dan beberapa serangan terhadap bank di Turki, Poland, Mexico serta Chile.

Serangan siber besar-besaran mengakibatkan kecurian hampir AS$530 juta (RM2.2 bilion).

Oleh itu, kerajaan perlu sentiasa memperkasa sistem keselamatan siber negara. Organisasi berperanan penting melindungi sistem keselamatan siber negara seperti Agensi Keselamatan Siber Negara (NACSA) dan CyberSecurity Malaysia (CSM) serta Angkatan Tentera Malaysia (ATM) perlu berganding bahu memantau, sekali gus melindungi aset siber negara.

Komponen keselamatan siber seperti manusia, proses dan teknologi perlu dikukuhkan secara holistik sebagai langkah kesiapsiagaan berhadapan risiko ancaman keselamatan siber dari pelbagai pihak termasuk Korea Utara.



Penjenayah siber *melakukan intipan dan mencuri data yang mampu melumpuhkan infrastruktur sasaran.* (Foto hiasan)

Penulis adalah *Pensyarah Fakulti Pengurusan Maklumat Universiti Teknologi Mara (UiTM) Johor*