Waspada Kejahatan Cyber ala WannaCry

O l e h

AUGUSTINUS SIMANJUNTAK*

DUNIA tiba-tiba dibuat heboh oleh serangan *cyber* bernama *ransomware* WannaCry. Serangan itu telah membuat National Health Service (NHS) di Inggris kelabakan melayani pasiennya karena WannaCry tiba-tiba mengunci komputer. Bahkan, akibat serangan itu, beberapa rumah sakit terpaksa mengalihkan pasien ke rumah sakit lain. Serangan WannaCry juga menyebar ke berbagai negara di dunia, termasuk Indonesia.

Biasanya, sasaran utama uang tebusan *ransomware* WannaCry adalah lembaga kesehatan, pendidikan, jasa keuangan, dan badan-badan pemerintah. Rupanya, para penjahat *cyber* lebih memilih ragam perusahaan itu sebagai tempat maraup tebusan yang menggiurkan. Menurut perusahaan keamanan komputer, Kaspersky, lebih dari 45.000 serangan via *e-mail* terjadi di 99 negara. Termasuk Inggris, Amerika Serikat, Rusia, Ukraina, India, Tiongkok, Italia, dan Mesir. Di Spanyol, perusahaan telekomunikasi besar Telefonica juga terinfeksi.

Uang tebusan yang diminta pelaku kejahatan USD 300 untuk mengembalikan *file* data para pengguna. Bahkan, ada dugaan uang tebusan bisa dinaikkan si pelaku setelah jangka waktu tertentu. *Ransomware* WannaCry merupakan bentuk *malware* (program yang diciptakan untuk mencari kelemahan *software*) yang bertujuan memblokir akses ke sistem komputer. Mengunci semua atau beberapa konten pada sistem komputer sampai jumlah uang tertentu dibayarkan ke operator perangkat lunak perusak.

Begitu uang tebusan dalam bentuk *bitcoin* (mata uang virtual) telah dibayar lewat serangkaian transaksi *online*, *file* dan akses ke sistem komputer si pengguna (korban) akan dibuka kembali. Modusnya, biasanya ada kiriman *e-mail* yang dikirim ke sasaran (pengguna komputer), baik individu maupun perusahaan. *E-mail* yang dikirim si penjahat tampak sah dan tepercaya dengan mengingatkan pengguna untuk memperbarui perangkat lunaknya ke versi terbaru.

Si pelaku akan memberikan instruksi kepada si korban untuk mengeklik tautan tertentu atau si korban diminta membuka tautan *website* tertentu untuk informasi lebih lanjut tentang produk terbaru yang ditawarkan si penjahat. Artinya, pelaku kejahatan hanya butuh satu orang untuk mengeklik *link* di *e-mail* untuk menginfeksi seluruh komputer si pengguna. Termasuk jaringan yang diikutkan pada *workstation* (perangkat keras komputer).

Korban akan tahu bahwa komputernya (atau *file* tertentu pada sistem komputernya) telah terjangkit virus setelah perangkat lunaknya tidak bisa lagi dioperasikan akibat ulah *software* dari si penjahat. Dalam kondisi komputer terblokir itulah, si penjahat meminta uang tebusan lewat perangkat lunak yang dibangunnya. Si pelaku telah memberikan petunjuk bagi korban mengenai jumlah uang yang harus dibayar dan cara-cara penyelesaian transaksi.

Apabila uang tebusan tidak dibayar si korban dengan tepat waktu, konten yang diblokir bisa saja dihancurkan. Bahkan, meski si korban telah membayar uang tebusan, ada pula operator *malware* (penjahat) yang ternyata tidak pernah mengirimkan kode yang diperlukan untuk membuka sistem komputer si korban yang telah terblokir. Sungguh sangat jahat.

Keamanan sejak Dini

Sebenarnya, kejahatan dunia maya (*cyber crime*) ala *ransomware* sudah terjadi jauh sebelum internet diadopsi secara luas (1980-an). Caranya, si penjahat menyebar virus *ransomware* ke dalam komputer lewat *floppy disk*. PC Cyborg Trojan merupakan jenis *ransomware* pertama dengan meminta uang tebusan dari korban.

Kali ini penjahat *cyber* mengembangkan metode mengunci data korban *strain* lanjutan (*ransomware* WannaCry) yang melakukan enkripsi (metode mengirim pesan rahasia) data di jaringan perusahaan atau mengunci pengguna. Lalu, si pelaku menuntut tebusan untuk mengembalikan data kembali normal. Symantec (perusahaan jasa antivirus) pernah menyatakan bahwa *ransomware* seperti Trojan Ransomlock biasanya ada di situs berbagi *file peer-to-peer* (P2P) dan sering dikemas dalam perangkat lunak bajakan.

P2P, artinya, sistem terkomputerisasi *client-server* bahwa suatu komputer berfungsi sebagai *client* sekaligus sebagai *server*. Akibatnya, bisa terjadi komunikasi dan pertukaran *resource* antara dua komputer secara langsung (*real time*). Karena itu, *ransomware* adalah ancaman yang serius bagi banyak negara. Di Amerika Serikat saja sejak 2005–2006 diperkirakan ada lebih dari 4.000 serangan setiap hari dan para peneliti telah membuat analisis tentang tren meningkatnya uang tebusan pada sekitar 20.000 perusahaan di Negeri Paman Sam itu.

Virusnya bernama Gpcoder Trojan dan Archievus Trojan. Perusahaan terpaksa membayar tebusan demi kepentingan pemegang saham, karyawan, konsumen, dan para mitra bisnis. Di negara kita belum ada riset mengenai korban *ransomware*. Aksi pelaku *cyber crime* itu memang rumit sehingga butuh upaya serius dari pengguna komputer untuk mencegahnya. Staf keamanan IT (*information technology*) di setiap perusahaan perlu rutin memperbarui sistem keamanan perangkat lunak komputernya. Lalu, waspada terhadap setiap transaksi atau kiriman pesan elektronik yang tak dikenal, termasuk pihak yang mengaku vendor.

Selain rutin memantau jaringan internet, setiap individu dan lembaga perlu cermat dalam mengidentifikasi potensi *ransomware* lewat *e-mail*. Karena itu, badan-badan publik maupun swasta perlu melakukan pelatihan bagi seluruh staf dan karyawannya mengenai material *e-mail* yang mencurigakan dan berbahaya bagi sistem komputernya. Sementara itu, pihak yang telanjur kena virus bisa masuk kategori *force majeure* yang mengakibatkan terhalang/terlambatnya pelayanan transaksi. (*)

*) *Dosen Universitas Kristen Petra Surabaya*