KERATAN AKHBAR-AKHBAR TEMPATAN
TARIKH: 5 MEI 2015 (SELASA)

Bil	Tajuk	Akhbar
1.	The Mask dikesan mengintip 7 tahun	Berita Harian
2.	Latih pakar tempatan sekat penggodam siber	Berita Harian
3.	Pengundi diminta keluar lebih awal elak hujan	Berita Harian
4.	Wet mornings in the peninsula	The Star
5.	Amaran ribut petir sehingga lewat petang	BERNAMA

KERATAN AKHBAR
BERITA HARIAN (NASIONAL) : MUKA SURAT 6
TARIKH : 5 MEI 2015 (SELASA)

The Mask dikesan mengintip 7 tahun

Kuala Lumpur: Perisian jahat (malware) yang dikenali 'The Mask' boleh menjalankan pengintipan bertahun-tahun atau selama mana yang diperlukan di ruang siber sesebuah negara atau organisasi, tanpa disedari.

Taktik The Mask ditemui firma keselamatan antarabangsa Kaspersky Labs selepas tujuh tahun ia menjalankan pengintipan di ruang siber sasaran.

BH difahamkan, taktik sama amat berbahaya kerana ia boleh mengambil alih sistem kawalan pesawat yang sedang terbang dengan mudah dari bumi, malah sebuah negara maju dikatakan dapat mengalahkan negara lain selepas sistem pertahanannya diambil alih dari jauh.

Pakar Kajian Strategik Keselamatan Siber, CyberSecurity Malaysia, Lt Kol (B) Sazali Sukardi, berkata malware berkenaan sudah menyasarkan beberapa organisasi kerajaan, kedutaan dan korporat di 31 negara.

Intip maklumat negara

"Pengintipan siber berlaku kerana negara atau organisasi terbabit mahu mencapai keunggulan maklumat, bagi mendapat kelebihan strategik dalam politik, ekonomi dan ketenteraan. Pengintipan industri pula dilakukan untuk mengatasi pesaing dalam perniagaan global yang semakin kompetitif.

"Pengintipan atau perisikan di peringkat strategik berkait dengan doktrin sesebuah negara. Jadi, isu ini tidak dibincangkan secara terbuka. Malah, mana-mana negara akan menafikan pembabitan mereka.

"Aktiviti pengintipan siber kini semakin meluas dengan menggunakan teknologi digital digunakan sebagai medium dan ejen pengintipan. Ciri-ciri tanpa nama dan tanpa sempadan yang wujud di ruang siber serta penciptaan malware membolehkan pengintipan dilakukan dari mana-mana lokasi di dunia ini tanpa dikesan," katanya kepada *BH*.

Sazali berkata, serangan siber seperti pencacatan web dan Penafian Perkhidmatan Teragih sering diisytiharkan oleh penggodam dan impaknya boleh dilihat.

Bagaimanapun, pengintipan siber ini lebih bahaya kerana ia tidak diisytiharkan dan impaknya tidak dapat dilihat.

Katanya, sesetengah organisasi atau negara mungkin bertindak secara langsung atau menaja kumpulan penggodam yang mempunyai kepakaran tinggi untuk bertindak bagi pihak mereka.

Penyerang sukar dikesan

"Penyerang siber sukar dikesan kerana mereka berselindung di sebalik infrastruktur botnet (sekumpulan program yang saling terhubung melalui internet dan berkomunikasi dengan program seumpamanya bagi melakukan tugas tertentu). Dalam konteks ini, infrastruktur botnet digunakan sebagai pangkalan untuk melancarkan serangan siber global.

"Botnet yang terdiri daripada semua komputer yang dijangkiti malware boleh dirampas dan dikawal oleh penyerang siber untuk menyerang sasaran mereka," katanya.

KERATAN AKHBAR
BERITA HARIAN (RENCANA): MUKA SURAT 24
TARIKH: 05 MEI 2015 (SELASA)

Minda Pengarang

Latih pakar tempatan sekat penggodam siber

Kita wajar bimbang dengan pendedahan CyberSecurity Malaysia bahawa hampir setiap hari ruang siber negara diserang atau cuba diserang penggodam antarabangsa. Banyak laman web sama ada kerajaan atau swasta terjejas teruk sejak kebelakangan ini selepas beberapa pusat pelayan data diasak beribu-ribu pengintip siber asing. Pengintip siber tanpa nama yang berpangkalan di Asia ini dipercayai menjadikan agensi kerajaan, sektor pertahanan yang kritikal dan industri tertentu sebagai sasaran dengan tujuan mengumpul dan mencuri maklumat. Tidak hairanlah, banyak fail sulit didedahkan kepada umum, sebahagiannya digunakan untuk menyerang kerajaan. Soal serangan itu bersifat peribadi atau tidak, apa yang penting ialah bagaimana data sulit itu boleh terlepas ke tangan pihak yang tidak sepatutnya. Lebih menakutkan jika maklumat itu digunakan untuk melemahkan sistem pertahanan atau sebagai ancaman kepada negara walaupun setakat ini belum ada petanda ke arah itu. Negara kuasa besar seperti Amerika Syarikat (AS) sendiri menerima padah apabila organisasi WikiLeaks pada 27 Februari 2012 menggunakan maklumat penggodam Anonymous untuk mendedahkan kepada masyarakat antarabangsa lebih lima juta e-mel Fail Perisikan Global dari ibu pejabat syarikat Stratfor di Texas, mengenai kerja dalaman syarikat itu yang menyediakan perkhidmatan risikan sulit kepada firma besar seperti Dow Chemical Co, Lockheed Martin, Northrop Grumman, Raytheon, Jabatan Keselamatan Dalam Negeri AS, Marin AS dan Agensi Perisikan Pertahanan AS.

Dalam konteks negara kita, beberapa laman web tempatan pernah diserang penggodam Bangladesh termasuk Microsoft, Dell, Kapersky, MSN, Skype dan Bing cawangan Malaysia. Mereka memberi amaran kepada rakyat Malaysia supaya menghormati warga Bangladesh yang bekerja di sini. Itu cuma sebahagian daripada situasi bagaimana mudahnya penggodam bertindak. Bagaimana menghadapinya? CyberSecurity mengakui sukar menjejak penjenayah ini kerana menggunakan ratusan alamat dan nombor Protokol Internet (IP) beberapa negara. Jadi, tiba masanya Malaysia melatih dan mempunyai pakar sendiri dalam bidang ini, bukannya sekadar menjadi pengguna program sedia ada, tetapi selaku pencipta. Sebabnya, kita sedia maklum, beribu-ribu aplikasi yang diguna pakai hari ini dibeli dari luar negara dan tentu pencipta atau syarikat yang mengawalnya tahu kelemahan dan kekuatan sistem yang mereka cipta. Tidak mustahil aplikasi dalam telefon pintar itu juga boleh dieksploitasi. Kita perlu kurangkan kebergantungan dari segi itu, cuma tiada kemampuan menahannya masuk ke pasaran tempatan. Memang diakui ia proses yang sukar, tetapi bukanlah sesuatu yang mustahil jika kena pada caranya. Mungkin juga bijak pandai teknologi atau 'hackers' tempatan boleh kongsi idea bagaimana ia boleh diaplikasikan untuk kebaikan bersama. Sudah terbukti, penjenayah tidak perlu lagi merompak atau mengancam masyarakat dengan memecah masuk rumah kerana teknologi kini membenarkan mereka melakukannya dari jauh.