RAMAI rakyat Malaysia menggunakan telefon.

Metro 6/3/13 MS A

Ancam pengguna

Telefon pintar dan tablet adalah sasaran utama penjenayah siber

FOKUS IT

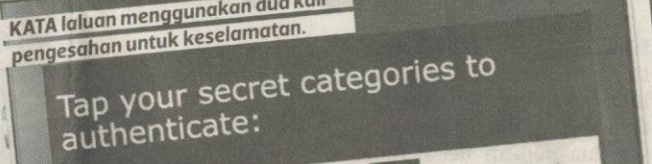
Oleh Afiq Hanif
afiq@hmetro.com.my

Kita sudah memasuki bulan ketiga tahun 2013 yang cukup mencabar bukan saja bagi negara namun

saran ringkas (SMS) atau mesej dengan nombor kod tertentu bagi tujuan kese-

yang gemar memasuki sistem telefon pintar versi seperti Android, Windows Mobile dan BlackBerry berasaskan

KATA laluan menggunakan dua kali pengesahan untuk keselamatan.



2. Telefon bimbit mangsa menerima mesej SMS atau mesej berkod dengan permintaan untuk memasang keselamatan, perakuan yang dikemas kini atau beberapa perisian lain yang perlu. Walau ba-

trend mudah alih di-
jangka meningkatkan
seiring pertumbuhan
telefon pintar dan gajet
mudah alih sama ada di
Malaysia atau dunia.

Ditambah pula kandungan digital kini boleh diakses terus di telefon atau tablet misalnya rancangan televisyen, 'stream' video hinggalah kepada paparan berita yang dilanggan dari agensi tertentu.

Ia bermakna anda perlu memasukkan data, membuat bayaran langganan dan mendaftar maklumat peribadi dalam gajet masing-masing yang diaplikasikan untuk menjadikan transaksi lebih mudah.

Namun, dalam kita menikmati kemudahan terbabit, timbul pula penyangak siber yang menunggu durian runtuh apabila mereka bakal meningkatkan akses kepada kegiatan godaman bagi memantau maklumat peribadi anda.

Apabila kita melakukan transaksi melalui Internet mudah alih dalam telefon atau tablet, pihak tertentu pada kebiasaannya akan menghantar khidmat pe-

lamatan sebelum menge-
ahkannya.

Hingga kini, sistem keselamatan terbabit disifatkan antara ciri paling selamat bagi mengelakkan sebarang penipuan dan pencerobohan akaun tanpa disedari.

Transaksi pengesahan nombor mudah alih atau digelar mTAN yang digunakan sepatutnya menjadi salah satu mekanisme perlindungan perbankan dalam talian yang paling boleh dipercayai.

Bagaimanapun, dengan kemunculan sejenis virus dinamakan Trojan Zeus yang mensasarkan pengguna telefon pintar – Zeus-inthe-Mobile atau ZitMo membuatkan kita meragui status keselamatan mTAN yang tidak lagi dapat menjamin data pengguna daripada jatuh ke tangan penjenayah siber. Ia pertama kali dikesan pada akhir September 2010 yang mana ZitMo direka untuk mencuri kod mTAN yang dihantar oleh bank ke sistem SMS dan ia disifatkan sebagai salah satu contoh baru virus melalui telefon bimbit.

Sehingga kini, virus

platform melintang (cross platform).

Ia sehingga kini masih mengalami evolusi dengan penggodam dikhabarkan cuba menyesuaikan kod godaman berdasarkan ciri mudah alih telefon atau gajet.

Virus terbabit boleh dikatakan salah satu jenis Trojan dengan pengkhususan yang sangat kompleks berdasarkan modus operandinya ialah menggemukakan mesej teks yang masuk dengan kod mTAN kepada pengguna dengan niat jahat sebelum pantas mencuri nombor rahsia.

Malah, anda mungkin tidak sedar apabila memasukkan maklumat peribadi ketika mendaftar dan sebagainya, penggodam juga mempunyai salinan maklumat sama.

Dalam keadaan tertentu ia turut mempengaruhi sistem pelayan apabila membabitkan peranti berasaskan Android sebelum menguruskan urus niaga kewangan secara haram yang menggunakan akaun bank digodam atau mencuri sese-

tengah maklumat dianggap berharga.

Maklumat sensitif paling berharga biasanya nombor telefon, alamat e-mel, tarikh lahir atau foto sebelum menjualnya kepada pihak ketiga.

Bukan setakat itu, ciri yang paling menonjol dalam pergerakan virus jenis Trojan ini ialah 'perkongsian' klasik dengan Trojan Zeus yang dicipta khusus untuk menular ke dalam komputer peribadi (PC).

Jika ia berlaku, ZitMo bukan lagi semata-mata spyware yang mampu menghantar mesej teks.

■ Secara umumnya, serangan dirancang seperti berikut:

1. Penjenayah siber menggunakan Zeus berasaskan PC untuk mencuri data yang diperlukan untuk mengakses akaun perbankan online dan nombor telefon bimbit pelanggan.

gaimanapun, pautan
lam SMS atau pautan lain
sebenarnya akan membawa kepada versi mudah alih Zeus.

3. Jika mangsa memasang perisian dan ia secara tidak langsung menjangkiti telefon, penjenayah siber boleh menggunakan data peribadi yang dicuri dan cuba untuk membuat urus niaga tunai dari akaun pengguna tapi akan memerlukan kod mTAN untuk mengesahkan transaksi atau memilih menyalin maklumat peribadi lain.

4. Untuk kes perbankan, bank menghantar mesej SMS dengan kod mTAN kepada telefon bimbit pelanggan.

5. ZitMo akan memintas teks terbabit yang digabungkan bersama kod mTAN telefon pengguna.

6. Penjenayah siber kemudiannya mampu untuk menggunakan kod mTAN untuk mengesahkan transaksi.

Serangan yang membabitkan ZitMo atau program berniat jahat lain dengan fungsi sama yang direka bertujuan untuk mencuri kod mTAN atau maklumat sulit akan diteruskan pada masa hadapan.

Oleh yang demikian, pengguna telefon pintar harus mengikut beberapa langkah keselamatan mudah alih, sentiasa mengkaji semula kebenaran permohonan pada bila-bila masa apabila transaksi dilakukan dan tidak melakukan 'jailbreak' pada peranti.

Jika anda memasang perisian Android dari sumber yang lain dari Android Market, pastikan ia datang dari sumber bereputasi.

Jangan klik URL yang anda terima dalam SMS serta pasangkan perisian antivirus bereputasi dalam telefon anda dan sentiasa kemas kininya.

Beberapa laporan sebelum ini menyebut penemuan virus baru ZitMo yang direka itu khusus untuk menyerang sistem operasi Android.

ZitMo juga akan menyebarkan malware untuk ke seluruh platform mudah alih lain seperti Windows Mobile, Symbian dan BlackBerry yang semakin popular.

Meskipun ia mula dikesan pada sistem operasi Symbian pada September 2010 lalu yang bertujuan untuk menyusup masuk dalam sistem pengguna, tahap kompleksnya kini beralih kepada Android.

Pada tahun ini, kebanyakan syarikat dijangka akan menggunakan dua faktor pengesahan yang digunakan bank untuk mengesahkan identiti pemegang akaun ketika 'log in'.

Namun ZitMo dikhabarkan boleh memintas dua kos serentak jika tidak berhati-hati.

Walaupun pengguna mudah alih tidak bergantung pada kaedah dua faktor pengesahan terbabit bagi perbankan, ZitMo boleh menyelinap masuk dan mengintip semua khidmat pesanan ringkas (SMS) menjadikannya ancaman yang tidak boleh dipandang ringan.

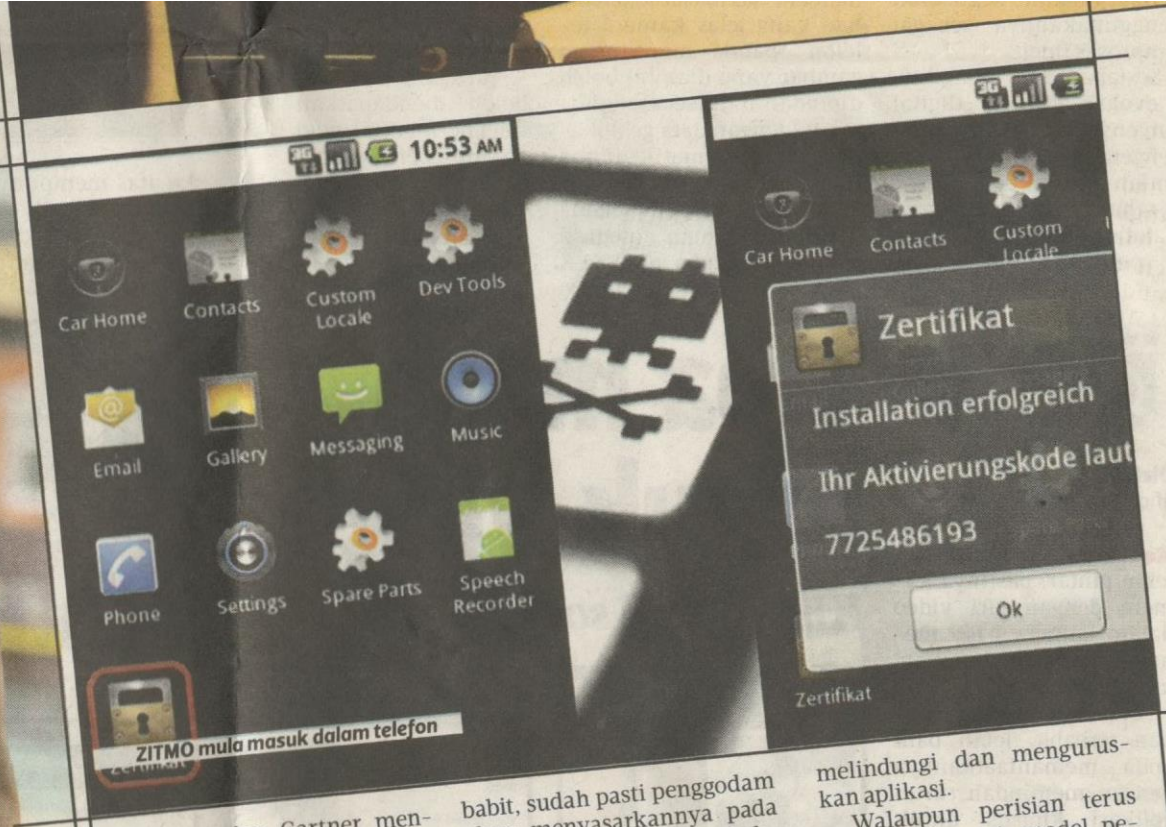
Kebanyakan jangkitan yang kita lihat seperti ini di kebanyakan makmal keselamatan hampir menyamai W32/Exchanger dan dikenali sebagai 'loaders'.

Firma penganalisis IDC meramalkan penghantaran peranti mudah alih baru meningkat sebanyak 55 peratus dalam tempoh

Mstar 6/3/13

PENGGUNAAN *tablet yang meluas memudahkan ia diceroboh.*

PENGGODAM cuba daftar masuk mahu maklumat peribadi.



ZITMO mula masuk dalam telefon

setahun dan Gartner mengunjurkan bahawa dalam tempoh masa yang sama, 1.2 bilion orang akan menggunakan telefon mudah alih untuk berhubung menerusi web.

Walaupun penjenayah siber sebelum ini tidak begitu berminat dengan peranti mudah alih, disebabkan peranti seperti ini yang semakin canggih dan pasaran kini dikuasai oleh platform terbabit, sudah pasti penggodam akan menyasarkannya pada 2013 sebagai sumber data rahsia.

Menambah lagi kerumitan ialah penggunaan media sosial yang dikatakan menambah baik komunikasi dan produktiviti di seluruh organisasi.

Walaupun media sosial akan terus mengubah kaedah kita berkomunikasi pada 2013, organisasi IT juga perlu memahami kaedahnya untuk melindungi dan menguruskan aplikasi.

Walaupun perisian terus memacu inovasi, model penyampaian baru akan dilaksanakan pada 2013 untuk keperluan pelanggan yang mempermudahkan operasi IT.

Perkomputeran cloud, perkhidmatan dan peranti dihos adalah contoh model penghantaran menarik yang akan mengubah landskap pusat data hari ini dengan memberikan organisasi fleksibiliti dan kemudahan penggunaan.