Social Engineering Dengan Menggunakan Pemancing URL

Budi Rahardjo

October 25, 2014

Abstrak

Makalah ini menampilkan teknik *social engineering* dengan menggunakan pemancing link (URL bait). Sebuah contoh ditampilkan untuk menunjukkan cara kerjanya.

Kata kunci: *security*

1 Pendahuluan

Dalam *security*, salah satu cara untuk mendapatkan informasi atau akses kepada sebuah sistem adalah dengan melalui *social engineering*. Pada prinsipnya penyerang mencoba mencari informasi informasi atau mencoba masuk ke sistem dengan cara menipu (atau membujuk). Keberadaan aspek sosial di dalam pendekatan inilah yang menyebabkan dia disebut *social engineering*.

Salah satu teknik penyerangan adalah dengan menyusupkan *malware*, seperti virus, *trojan horse*, atau *bot* ke komputer atau perangkat yang digunakan pengguna. Untuk memasukkan *malware* ini target harus mengunjungi sebuah halaman situs atau meng-klik sebuah link atau URL tertentu. Pada halaman tersebut terdapat *malware* yang tanpa diketahui oleh target akan diunduh ke komputernya. (Asumsi ini masih membutuhkan pembuktian.) Setelah terinfeksi, penyerang akan lebih mudah masuk ke komputer target tersebut dan melanjutkan penyerangannya.

2 Pancingan URL

URL bait atau pancingan URL adalah sebuah cara untuk memancing seseorang untuk meng-klik sebuah link (URL). Masalahnya adalah bagaimana membujuk orang agar mau meng-klik link tersebut. Ada beberapa cara untuk melakukan hal tersebut, antara lain:

1. membuat halaman dengan judul tulisan yang kontroversial atau sedang menjadi topik yang menarik (*trending topic*);

2. meminta orang yang terkenal untuk menyisipkan URL tersebut (yang ini mungkin agak sulit sehingga yang dapat dilakukan adalah dengan melakukan social engineering terhadap orang terkenal ini menjadikannya rekursif);

3. mengedit judul dari URL berita dari situs yang terkenal.

Pada saat makalah ini ditulis, di Indonesia sedang ramainya orang menunggu pengumuman susunan kabinet oleh Presiden Joko Widodo. Banyak beredar "daftar kabinet" di internet. Maka halaman yang memuat "daftar kabinet" tersebut kemungkinan disukai oleh banyak orang.

Salah satu kesulitan yang mungkin dihadapi dari pemancing URL ini adalah orang menjadi curiga dengan URL yang kita berikan. Ada cara untuk mengurangi kecurigaan adalah dengan menggunakan layanan pemendek URL (*URL shortening*) seperti yang dilakukan oleh bit.ly. URL menjadi memiliki domain bit.ly. Sebetulnya URL aslinya masih dapat dilihat tetapi cara untuk melihatnya tidak terlalu mudah, terlebih lagi jika target menggunakan smartphone.

3 Sebuah Percobaan

Pada bagian ini akan diuraikan sebuah contoh eksperimen yang saya lakukan.

Langkah pertama adalah membuat sebuah halaman yang harus dikunjungi oleh target. Pada halaman ini seharusnya ditanamkan *malware*, akan tetapi untuk sekedar pembuktian maka pada halaman ini hanya ditampilkan teks saja. Seperti sudah disebutkan sebelumnya, saat ini sedang ramai orang menanti susunan kabinet dari Presiden Joko Widodo, maka halaman yang saya buat seolah-olah berisi "bocoran" dari susunan kabinet tersebut. URL dari halaman ini adalah http://gbt.blogspot.com/2014/10/kabinet.html seperti dapat dilihat pada Gambar 1.

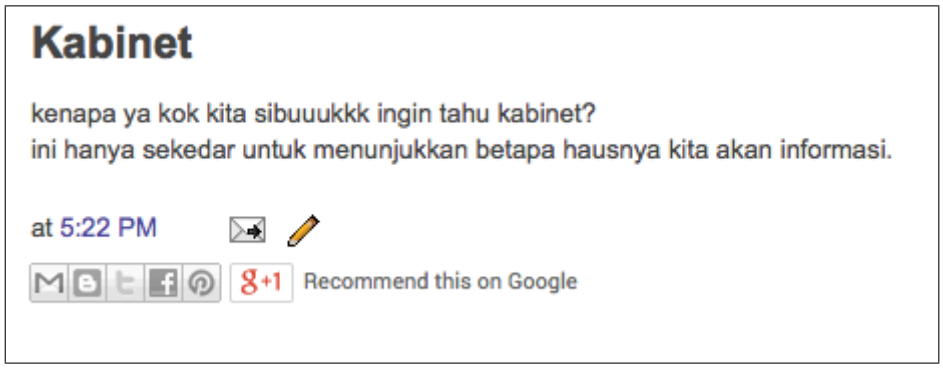

Figure 1: Tampilan halaman target

Agar target tidak terlalu curiga dengan link tersebut, maka link tersebut dipendekkan dengan menggunakan layanan bit.ly. Sebagai contoh, link yang

tadinya menunjukkan bahwa halaman tersebut merupakan blog di “blogspot.com” menjadi tersamarkan. Link yang sudah dipendekkan tersebut kemudian ditampilkan di halaman status Facebook saya sebagaimana dapat dilihat pada Gambar 2. Selanjutnya kita tinggal menunggu adanya orang-orang yang tersesat ke halaman tersebut.

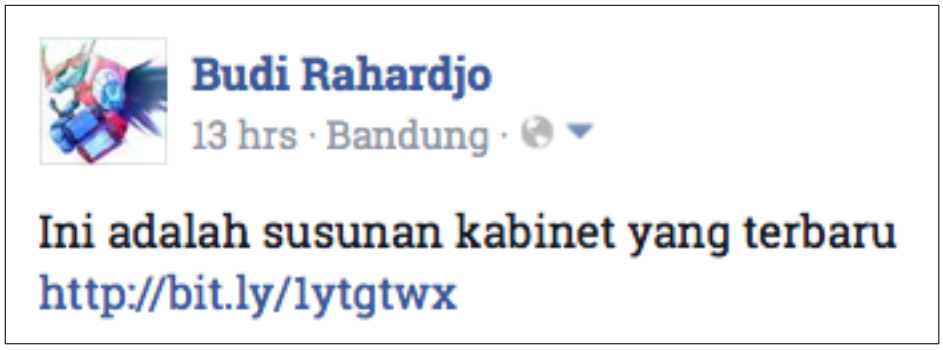

Figure 2: Tampilan URL di status Facebook

Untuk mengetahui berapa jumlah orang yang telah mengunjungi halaman tersebut melalui Facebook (klik ke link yang sudah dibuat tersebut) dapat dilakukan dengan menggunakan fitur statistik pada blogspot (blogger.com) seperti terlihat pada Gambar 3. Dapat terlihat pada statistik tersebut bahwa dalam waktu kurang dari satu hari, sudah ada 875 orang yang mengunjungi halaman tersebut.

Figure 3: Fitur statistik pada blogspot

Selain itu, layanan bit.ly juga menyediakan layanan statistik untuk menunjukkan berapa orang yang meng-klik URL tersebut. Hal ini dapat dilakukan dengan menambahkan tanda tambah (+) pada akhir dari URL. Contoh tampilannya dapat dilihat pada Gambar 4.

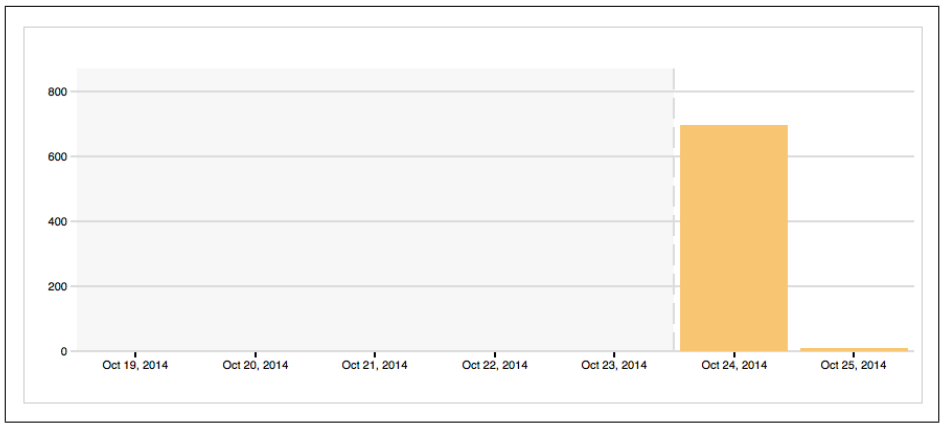

Figure 4: Fitur statistik pada bit.ly

Percobaan yang sederhana ini menunjukkan betapa mudahnya orang mengklik sebuah link. Dalam waktu yang singkat, ratusan orang sudah terpancing untuk mengunjungi link tersebut. Pada kasus ini ada asumsi bahwa orang-orang sedang haus informasi mengenai sebuah topik tertentu (dalam kasus ini adalah kabinet Presiden Joko Widodo) dan kebanyakan pengunjung adalah teman atau *follower* dari akun Facebook saya. Belum dilakukan percobaan apabila link yang sama dimasukkan ke jejaring sosial yang lain, seperti twitter, path, dan seterusnya.

4 Penutup

Tulisan ini menunjukkan sebuah teknik untuk melakukan *social engineering* dengan menggunakan pemancing link (URL bait). Contoh diberikan untuk menunjukkan betapa mudahnya melakukan pemancingan.

Melihat betapa mudahnya menipu seseorang, maka pendidikan kepada pengguna untuk tidak mudah melakukan klik atas sebuah link harus dilakukan untuk meningkatkan keamanan.