MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING

Dedi Irawan, S.Kom., M.T.I 1)*
[1*)]S1 Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhamamdiyah Metro
Jl. Gatot Subroto No.100, Yosodadi, Kec. Metro Tim., Kota Metro, Lampung 34381
e-mail : dedi.mti@gmail.com [1)]

ABSTRAK

Phising bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. Kata lain dari Phising adalah *Password Harvesting* yang artinya sebuah tindakan kejahatan untuk memancing mengumpulkan password. Tindakan Phising ini adalah mengarahkan pengguna untuk memasukkan data akun seperti username dan password di sebuah website palsu (*fake webpage*). Hebatnya lagi website Phising akan didesain dengan tampilan serta nuansa yang menyerupai situs aslinya (*spoofed webpage*). Misal seperti logo, alamat domain dan seterusnya. Sehingga jika tidak cermat mengamati, mereka yang menjadi target penjahat siber akan memberikan informasi mereka seperti username, password dan informasi penting lainnya secara sukarela. Salah satu metode paling umum yang digunakan untuk mendapatkan informasi terkait akun adalah metode "phising". Metode ini digunakan untuk menipu pengguna agar menyerahkan data mereka secara suka rela. *Fake Webpage* memang masih digunakan untuk mendapatkan akun social media seperti facebook. Hal tersebut karena pembuatan nya yang sangat mudah dan tingkat keberhasilan nya yang masih tinggi. Cara kerjanya adalah dengan mengirimkan tautan (link) phising facebook di media social atau langsung mengirimkan link tersebut ke target. Bagi pengguna awam, mengira bahwa itu adalah situs web facebook yang asli sehingga memasukkan username dan password, situs web sedang mengirimkan informasi yang diterima dari pengguna seperti user name dan pasword ini ke pelaku, yaitu hacker. Setelah pelaku mendapatkan user name, email dan password korban maka akun korban akan digunakan untuk hal yang tidak baik.

Kata Kunci – phising facebook, mencuri akun facebook, fake login facebook

1. PENDAHULUAN

Perusahaan keamanan siber Kaspersky baru saja merilis laporan terbarunya tentang upaya phising di Asia Tenggara. Ada sekitar 14 juta upaya phishing terhadap pengguna internet di Asia Tenggara selama paruh pertama 2019. Selama periode ini di Asia Tenggara, menurut laporan Kaspersky, upaya phising di Vietnam menjadi yang tertinggi, diikuti oleh Malaysia dan Indonesia. Angka korban phising di Indonesia periode ini naik menjadi 14,316 persen dari 10,719 persen tahun lalu.

Upaya phishing merujuk pada frekuensi bahwa pelaku kejahatan siber mencoba mengarahkan para pengguna untuk mengunjungi situs web palsu dengan tujuan untuk mencuri informasi. Fake login pada prinsipnya adalah page palsu yang dibuat semat-mata persis sama dengan halaman aslinya. Tapi bedanya fake login akan menjaring user name dan password yang ada masukan di form login menuju file yang berisikan password korban. Halaman utama (*fake login*) dibuat dengan cara mengcopy seluruh halaman utama (*web page complete*) website tertentu. Facebook merupakan jejaring sosial paling populer bagi para pelaku untuk disalahgunakan. Situs web Facebook sering dipalsukan oleh pelaku untuk mencuri data pribadi melalui serangan phishing. Tindakan ini menjadi bagian dari tren jangka panjang. Pada Q1 2017, Facebook menjadi salah satu dari tiga sasaran teratas untuk phishing yakni sebesar 8 persen, diikuti Microsoft Corporation 6 persen dan PayPal 5 persen. Data Q2 2018 juga menempatkan Facebook kembali di posisi teratas kategori phishing jaringan sosial. Posisi kedua dan ketiga adalah VK dan LinkedIn. Facebook sebagai target populer karena layanan ini memiliki lebih dari dua miliar pengguna aktif. Pengguna yang mengakses aplikasi dengan akun Facebook, juga mempermudah pejahat siber menyadap akun personal. Hal ini membuat penguna Facebook

yang lalai menjadi target menguntungkan bagi para pelaku phishing jaringan sosial.

Selanjutnya memodifikasi link form login asli ke login.php yang dibuat sendiri menuju file/database yang juga telah disiapkan.

Tahap berikutnya adalah dengan mengupload page utama yang telah di copy dan dimodifikasi tersebut pada file penyimpaman (*hosting*). Cara kerja selanjutnya adalah dengan mengirimkan tautan (*link*) phising facebook di media social atau langsung mengirimkan link tersebut ke target.

2. TINJAUAN PUSTAKA

Menurut Vyctoria (2013:214) "Phising (*Password Harvesting Fishing)* adalah tindakan penipuan yang menggunakan email palsu atau situs web palsu yang bertujuan untuk mengelabui user sehingga pelaku bisa mendapatkan data user tersebut". Istilah phishing dalam bahasa inggris berasaldari kata *fishing* (memancing), dalam hal ini berarti memancing informasi pengguna seperti akun facebook.

Yeo Siang Tiong selaku General Manager untuk Asia Tenggara, Kaspersky, mengatakan, "Sangat mengkhawatirkan bahwa trik phishing masih sangat efektif dalam melakukan penipuan kepada para pengguna internet di Asia Tenggara.

Pada pasal 35 UU ITE tahun 2008 "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik. (Phising = penipuan situs)."

3. METODE PENELITIAN

Phising merupakan salah satu cara penipuan agar si penipu bisa mendapatkan informasi detail dari akun tertentu dengan cara ilegal. Seperti misalnya website tiruan, atau pop-up yang mirip website resmi seperti paypal, ebay, dan lain sebagainya. Sekarang ini banyak sekali cara para pelaku penipuan tipe ini untuk membohongi korbannya. Ada dua teknik yang paling sering dilakukan, yakni phising email dan website, seperti pada gambar 1.1 dibawah ini.

Gambar 1.1 Merode Phising

Phising telah banyak memakan korban di media sosial, hal itu dikarenakan Media sosials merupakan akun harian yang sering dan bahkan setiap hari digunakan oleh penggunanya, tanpa sadar pengguna memasuki halaman jebakan yang menyebabkan pengguna bisa saja terjebak memasuki halaman palsu tersebut. Tidak hanya itu, phising juga terkadang bisa terjadi manipulasi dimana komputer yang terinfeksi bisa saja memanipulasi beberapa hal yang membuat halaman itu merupakan halaman aslinya, sehingga perlu diperhatikan dan dipastikan bahwa komputer anda tidak terkena virus untuk menghindari kasus ini.

User yang jadi korban bisa saja tak menyadari telah dirugikan akibat phising ini.

Adapun metode yang dugunakan dalam penelitian ini adalah sebagai berikut:

- Membuat web phising facebook
  Secara singkat, untuk membuat web phising facebook hanya perlu masuk ke cpanel hosting dan bisa gratis. Lalu memilih domain (alamat/link) untuk dijadikan link phising. Dan terakhir upload Script phising facebook ke domain yang sudah dibuat.
  Berikut detail tentang cara membuat web phising facebook:
  - ✓ Login Cpanel
    Untuk mendapatkan login cpanel harus melakukan registrasi pada akun hosting.
  - ✓ Upload file web palsu
    Buatlah desain/tampilan web palsu dengan semirip mungkin supaya korban merasa yakin asli bahwa situs yang dikunjunginya asli, seperti pada gambar 1.1 dibawah ini.

Gambar 1.1 Upload file web palsu

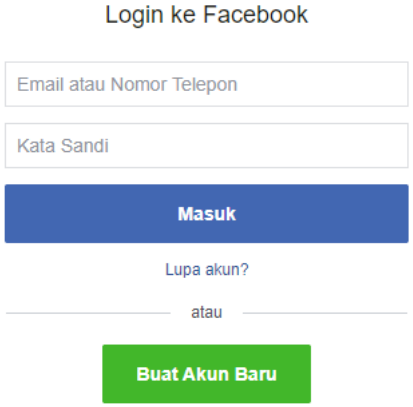
Adapun penjelasan diri file tersebut yaitu:

- File index.html
  Adalah halaman utama yang dituju saat diakses oleh korban.

- Login.php
  Adalah script untuk melakukan eksekusi dari teknik phising.

- Simpan.txt
  Merupakan file yang menyimpan data akun facebook korban.

✓ Tampilan website palsu facebook
Lakukan preview site untuk melihat hasilnya, seperti pada gambar 1.2 dibawah ini.



Gambar 1.2 Tampilan Facebook palsu

4. HASIL DAN PEMBAHASAN

Setelah berhasil membuat tampilan/desain web dan menguploadnya ke hosting, maka langkah selanjutnya adalah melakukan ujicoba sebagi berikut:

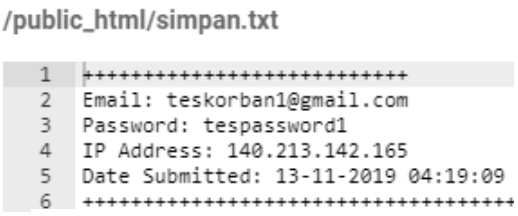
1) Mengirimkan link phising ke korban
Setelah web phising facebook berhasil dibuat. Selanjutnya hanya perlu mengirim link ke korban/target. Apabila ingin mendapatkan hasil yang lebih banyak, bisa memasang link tersebut di media sosial.

Agar tidak terlalu dicurigai, ubah link phising kita menggunakan shortener link seperti bit.ly atau sejenisnya.

2) Mengisikan username dan password
Melakukan simulasi dengan mengisikan username dan password. Seperti pada gambar 1.3 dibawah ini.

Gambar 1.3 Mengisikan username dan password

3) Melihat Hasilnya
Langkah terakhir adalah melihat hasil phising, apabila berhasil maka hasilnya dapat dilihat pada gambar 1.4 dibawah ini.



Gambar 1.4 Akun Korban disimpan

Adapun staregi yang digunakan supaya berhasil dalah teknik phising adalah sebagai berikut:

✓ Pada saat membuat web phising facebook, usahakan tawarkan atau beri pancingan hadiah yang menarik perhatian korban. Contohnya seperti hadiah yang dibuat berupa banner.

Untuk memasukkan pancingan hadiah tersebut, maka carilah script phising facebook yang sesuai. Apabila ingin memberikan pancingan game. Maka cari script digoogle "script phising gamelogin facebook".

✓ Pada saat mengirim/memasang link phising sebaiknya sertakan beberapa beberapa logo/foto yang sesuai dengan web Phising tersebut.

Dengan adanya logo/foto maka calon korban akan semakin percaya dan mereka akan melakukan login di web Phising yang sudah dibuat.

✓ Gunakan dengan bijak. Karena apabila digunakan secara berlebihan hosting yang digunakan untuk membuat web phising bisa disuspend/blokir.

5. KESIMPULAN

Dari hasil dan pembahasan diatas datat disimpulkan bahwa metode phising sangat berbahaya jika kita sebagai user tidak cermat dalam mengakses internet khususnya facebook. Namun ada beberapa cara mencegah atau menghindari diri dari upaya phising, yaitu:

- ✓ Perhatikan tautan/link yang akan kunjungi. Apakah situs web yang akan dikunjungi itu asli atau tidak.
  Semisal adress/alamat facebook yang asli adalah: https://facebook.com . apabila mengunjungi halaman facebook yang berbeda maka itu adalah situs web palsu, misalnya : https://cooklook.000webhostapp.com/.
- ✓ Kenali tanda giveaway yang ada dalam email phising:
  - Jika hal itu tidak ditujukan secara personal kepada anda.
  - Jika anda bukan satu-satunya penerima link/email.
  - Jika terdapat kesalahan ejaan, tata bahasa atau sintaks yang buruk atau kekakuan lainnya dalam penggunaan bahasa.
- ✓ Menginstall anti fake login seperti: Phistank siteChecker, FirePhish, TrustBar, SpooftStick dan lainya
- ✓ Ganti kata sandi secara berkala
  Merupakan cara untuk mengamankan akun agar tidak dicuri oleh penipu yang berpotensi menyalahgunakannya untuk menghubungi kerabat dan teman Anda.
- ✓ Ambil tindakan dan laporkan ke penyedia layanan media sosial
  Jika menerima email atau yang terlihat aneh dan janggal, jangan membukanya hingga melihat lampirannya. Jika menemukannya di Facebook, laporkan temuan tersebut ke phish@fb.com.

6. DAFTAR PUSTAKA

[1] Cyber Defense Magazine, 2019. The impact of usability on phishing [Online] (Updated 1 Mei 2019) Available at: https://www.cyberdefensemagazine.com/the-impact-of-usability-on-phishing/ [Accessed 13 November 2019]

[2] CNN indonesia, 2019. Indonesia Jadi Salah Satu Negara Target Phising [Online] (Updated 1 Oktober 2019) Available at: https://www.cnnindonesia.com/teknologi/20190930151156-185-435364/indonesia-jadi-salah-satu-negara-target-phising [Accessed 13 November 2019]

[3] Forbes, 2017. The Dangers Of Phishing [Online] (Updated 14 September 2017) Available at: https://www.forbes.com/sites/forbestechcouncil/2017/09/14/the-dangers-of-phishing/#6b3b1b925078 [Accessed 13 November 2019]

[4] Info Komputer, 2019. Asia Tenggara Masih Jadi Wilayah Target Serangan Phising Terbesar [Online] (Updated 30 September 2019) Available at: https://infokomputer.grid.id/read/121869132/asia-tenggara-masih-jadi-wilayah-target-serangan-phising-terbesar?page=all [Accessed 13 November 2019]

[5] Liputan6, 2018. Facebook Palsu Jadi Phishing Jaringan Sosial Paling Populer [Online] (Updated 6 Jan 2018) Available at: https://www.liputan6.com/tekno/read/3550580/facebook-palsu-jadi-phishing-jaringan-sosial-paling-populer [Accessed 13 November 2019]

[6] TechnAsia, 2018. Cara Menghindari Penipuan Phishing di Internet [Online] (Updated 5 Jan 2018) Available at: https://id.techinasia.com/cara-menghindari-phishing [Accessed 13 November 2019]

[7] Tirto, 2017. Waspada Pencurian Data Lewat Phising [Online] (Updated 23 April 2017) Available at: https://tirto.id/waspada-pencurian-data-lewat-phising-cnbt [Accessed 13 Novemver 2019]