WHITE PAPER

PHISING

Oleh

Sri Retno Rahayu

09011381621069

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOPUTER
UNIVERSITAS SRIWIJAYA

2019

A. Latar Belakang

Salah satu cyber crime yang sering dilakukan adalah phising. Phishing adalah kegiatan kriminal dengan menggunakan teknik rekayasa sosial. Phisher (sebutan bagi penipu Phishing) berupaya menipu untuk mendapatkan informasi sensitif, seperti username, password dan rincian kartu kredit, dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik. . Phishing menyerang semua sektor Industri berbasis online, seperti ecommerce, social networking services dan perbankan. Tindakan Phishing mengincar informasi sensitif pengguna untuk digunakan oleh pihak yang tidak berwenang. Pengguna dirugikan dalam hal privacy, penyalahgunaan (eksploitasi) dari tindakan hacking bahkan kerugian Finansial.

Secara tradisional phishing dikaitkan dengan kejahatan dunia maya perbankan online: penjahatmengirim email yang memikat Anda ke situs web yang merupakan klon visual dari halaman login bank Anda, di manaAnda memasukkan kredensial Anda ke formulir palsu dan menjatuhkannya langsung ke pangkuan para penjahat.Tapi phishing mencakup lebih dari sekadar situs perbankan palsu dan tautan ke pil penambah kehidupanatau pengiriman paket: ini benar-benar hanya tentang umpan menggantung di depan Anda dan menunggu Anda melakukannyamenelannya, memberi mereka informasi yang berguna dan berharga.

Dalam beberapa tahun terakhir, volume serangan phishing telah tumbuh secara dramatis, didorong oleh web gelaplayanan seperti kit phishing gratis dan phishing-sebagai-layanan. Ini menjadi semakinsederhana bahkan untuk penyerang yang paling tidak memiliki kecenderungan teknis untuk memanfaatkan malware tingkat lanjut itutelah diproduksi oleh seseorang yang jauh lebih pintar dari mereka.Akibatnya, serangan phishing sekarang menjadi bagian rutin dari kehidupan sehari-hari. 41% profesional TImelaporkan bahwa organisasi mereka mengalami setidaknya serangan phishing setiap hari, sementara lebih dari tigakuartal (77%) mengalami serangan setidaknya setiap bulan.

Survei terbaru terhadap 3.100 organisasi mengungkapkan bahwa email adalah serangan yang paling umumvektor, digunakan di 33% dari serangan siber yang sukses. Ini juga merupakan vektor yang sangat efektif: 53% dariorganisasi yang telah dilanda serangan cyber pada tahun lalu adalah korban phishing. 4Email phishing

seringkali merupakan tahap pertama dalam serangan multi-teknik yang kompleks. Sebagai contoh,mengklik tautan dalam email phishing terhubung ke server perintah dan kontrol,yang kemudian menginfeksi organisasi dengan perangkat lunak berbahaya.

B. Apa yang dimaksud Phising ?

Menurut wikipedia phising itu adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi rahasia, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang tepercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan.

Jadi Phising atau Fake Login adalah cara mencoba untuk mendapatkan informasi seperti username, password, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik. Sebagian besar metode phishing menggunakan beberapa bentuk penipuan teknis yang dirancang untuk membuat link dalam sebuah e-mail (dan situs web palsu itu mengarah) tampaknya milik organisasi palsu. Dalam dunia komputer pengelabuan dalam bahasa Ingrisnya phishing adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan data profil penting , dengan menyamar sebagai orang atau bisnis yang tepercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan istan.

Istilah phishing dalam bahasa Inggris berasal dari kata *fishing* (‘memancing’), dalam hal ini berarti memancing informasi data profil dan kata sandi pengguna. Metode ini sering kita jumpai di situs jejaring sosial seperti Facebook, friendster, yahoo messenger, dan lain-lainya. Jadi berhati – hatilah karena cara hack facebook dengan metode phising atau fake login sangat sulit untuk di cegah oleh pihak penyedia layanan dan bisa menyerang pengguna internet siapa saja karena sangat mudahnya dalam membuat phising dan hampir tidak memerlukan tehnik yang khusus.

C. Cara Kerja Phising

Seperti yang disebutkan, phishing mencakup lebih dari sekedar email perbankan palsu dan pengiriman paket peringatan. Ini tentang meyakinkan Anda untuk memberikan sesuatu yang berharga bagi para penyerang. Dan phishing kini telah berkembang menjadi tiga cabang serangan : klasik, mass phishing dan spear phishing, dan Business Email Compromise, bagian dari spear phishing.

- Mass Phising

  Serangan-serangan ini sebagian besar bersifat oportunistik, memanfaatkan nama merek perusahaancoba dan pikat pelanggan merek untuk memalsukan situs tempat mereka tertipu informasi kartu kredit, kredensial info masuk, dan informasi pribadi lainnya yang akan diberikan kemudian dijual kembali untuk keuntungan finansial.

- Spear phishing

  Jenis lain dari ancaman adalah berbagai phishing tombak, di mana email menyamar sebagaipengirim tertentu atau sumber tepercaya dikirim ke individu yang ditargetkan dalam organisasi untuk dicobauntuk membuat mereka mengambil tindakan tertentu, seperti mengirim uang ke akun palsu.

  - Menargetkan aset organisasi tertentu
  - Biasanya individu atau kelompok tertentu dalam suatu organisasi
  - Alamat email palsu (mirip) untuk membantu konversi
  - Menyamar sebagai sumber tepercaya dan eksekutif senior

  Serangan spear phishing semakin umum dan penjahat dunia maya terus menyempurnakan tekniknya untuk meningkatkan efektivitas. Dalam survei terbaru dari 330 It profesional,55% mengonfirmasi bahwa manajer senior mereka telah ditiru dalam phishing spear attack. Subset phishing yang lebih bertarget menggunakan rekayasa sosial untuk mengumpulkan data target dantingkatkan konversi. Ini dikenal sebagai Penipuan CEO, Penangkapan Ikan Paus, dan yang terbaru, BisnisEmail Compromise (BEC).

- Whaling

  Istilah Whaling merujuk pada serangan spear phishing yang diarahkan khusus pada eksekutif senior dan target tingkat tinggi lainnya. Dalam kasus ini, konten

akan dibuat untuk menargetkan manajer yang lebih tinggi dan peran orang tersebut di perusahaan. Konten email serangan perburuan paus mungkin merupakan masalah eksekutif seperti panggilan pengadilan atau keluhan pelanggan.

D. Teknik Phising

1. Email / Spam :

   Phisher akan mengirim email yang sama ke jutaan pengguna, meminta mereka untuk mengisi informasi pribadi. Rincian ini akan digunakan oleh phisher untuk kegiatan ilegal mereka. Phising dengan email dan spam adalah Phising scam yang sangat umum.Sebagian besar pesan memiliki catatan yang mendesak yang mengharuskan pengguna untuk memasukkan kredensial untuk memperbarui informasi account, rincian perubahan, dan memverifikasi account. Kadang-kadang, mereka mungkin akan diminta untuk mengisi formulir untuk mengakses layanan baru melalui link yang disediakan dalam email.

2. Pengiriman Berbasis Web :

   Web berbasis pengiriman adalah salah satu teknik Phising yang paling canggih. Juga dikenal sebagai “man-in-the-middle,” hacker terletak di antara situs web asli dan sistem Phising.Phisher Jejak rincian selama transaksi antara situs yang sah dan pengguna. Sebagai pengguna terus menyampaikan informasi, itu dikumpulkan oleh phisher, tanpa pengguna mengetahui tentang hal itu.

3. Pesan Instan :

   Olah pesan cepat adalah metode di mana pengguna menerima pesan dengan link yang mengarahkan mereka ke situs web Phising palsu yang memiliki tampilan yang sama dan merasa sebagai situs yang sah. Jika pengguna tidak melihat URL, mungkin sulit untuk membedakan antara situs palsu dan sah. Kemudian, pengguna diminta untuk memberikan informasi pribadi pada halaman.

4. Trojan Hosts :

   Trojan Hosts, hacker terlihat mencoba untuk login ke account pengguna Anda untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke phisher.

5. Manipulasi Tautan :

   Manipulasi link adalah teknik di mana phisher mengirimkan link ke sebuah website. Bila pengguna mengklik pada link menipu, itu membuka website phisher, bukan dari situs yang disebutkan di link. Salah satu anti-Phising teknik yang digunakan untuk mencegah manipulasi link adalah untuk memindahkan mouse ke link untuk melihat alamat yang sebenarnya.

6. Key logger :

   Key logger mengacu pada malware yang digunakan untuk mengidentifikasi input dari keyboard. Informasi ini dikirim ke hacker yang akan memecahkan password dan jenis-jenis informasi. Untuk mencegah Key logger dari mengakses informasi pribadi, situs web aman memberikan pilihan untuk menggunakan klik mouse untuk membuat entri melalui keyboard virtual.

7. Session Hacking :

   Dalam Session Hacking, phisher memanfaatkan sesi web mekanisme kontrol untuk mencuri informasi dari pengguna. Dalam prosedur sesi sederhana hacker dikenal sebagai sesi mengendus, phisher dapat menggunakan sniffer untuk mencegat informasi yang relevan sehingga ia dapat mengakses server Web secara ilegal.

8. Sistem rekonfigurasi :

   Phisher akan mengirim pesan dimana pengguna diminta untuk mengkonfigurasi ulang setting dari komputer. Pesan tersebut mungkin berasal dari alamat web yang menyerupai sumber yang dapat dipercaya.

9. Konten Injeksi :

   Injeksi Konten adalah teknik di mana phisher mengubah bagian dari konten pada halaman situs diandalkan. Hal ini dilakukan untuk menyesatkan pengguna untuk pergi ke halaman luar situs yang sah di mana pengguna diminta untuk memasukkan informasi pribadi.

10. Phising melalui Search Engine :

    Beberapa penipuan Phising melibatkan mesin pencari mana pengguna akan diarahkan ke situs produk yang dapat menawarkan produk dengan biaya rendah atau jasa. Ketika pengguna mencoba untuk membeli produk dengan memasukkan rincian kartu kredit, itu dikumpulkan oleh situs Phising. Ada banyak situs bank palsu yang menawarkan kartu kredit atau pinjaman kepada pengguna pada tingkat yang rendah tetapi mereka sebenarnya situs Phising.

11. Phone Phising :

    Dalam Phone Phising, phisher membuat panggilan telepon ke pengguna dan meminta user untuk dial nomor. Tujuannya adalah untuk mendapatkan informasi pribadi dari account bank melalui telepon. Telepon Phising banyak dilakukan dengan caller ID palsu.

12. Malware Phising :

    Penipuan Phising melibatkan malware memerlukannya untuk dijalankan pada komputer pengguna. Malware ini biasanya melekat pada email yang dikirimkan kepada pengguna oleh phisher. Setelah Anda klik pada link, malware akan mulai berfungsi. Kadang-kadang, malware juga dapat disertakan pada file download. Phisher mengambil keuntungan dari kerentanan keamanan web untuk mendapatkan informasi sensitif yang digunakan untuk tujuan penipuan.

E. Teknik umum yang sering digunakan oleh penipu

- Penggunaan alamat *e-mail* palsu dan grafik untuk menyesatkan Nasabah sehingga Nasabah terpancing menerima keabsahan *e-mail* atau *web sites*. Agar tampak meyakinkan, pelaku juga seringkali memanfaatkan logo atau merk dagang milik lembaga resmi, seperti; bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi, seperti; *password*, PIN dan nomor kartu kredit.
- Membuat situs palsu yang sama persis dengan situs resmi atau pelaku *phishing* mengirimkan *e-mail* yang berisikan *link* ke situs palsu tersebut.
- Membuat *hyperlink* ke *web-site* palsu atau menyediakan form isian yang ditempelkan pada *e-mail* yang dikirim.

F. Contoh Kasus Phising

Salah satu contoh kasus phishing di Indonesia dialami oleh pelanggan / pengguna situs internet banking milik Bank BCA yaitu “klikbca.com”. Pada saat itu tahun 2001, ada situs internet palsu yang sangat mirip penulisannya dengan situs klikbca.com, yaitu “kilkbca.com”.

Sekilas, calon korban tidak akan sadar bahwa salah tulis satu huruf saja akibatnya sangat fatal, yang akibatnya banyak pengguna internet banking Bank BCA memasukkan username, password dan nomor pin kedalam situs yang bukan seharusnya. Anda pasti tahu apa yang terjadi berikutnya, yaitu si pemilik situs palsu dengan leluasa menggunakan identitas korban untuk masuk ke situs klikbca yang sebenarnya dan mentransfer seluruh uang korban ke rekening miliknya. Kunci utama keberhasilan kejadian ini adalah tampilan situs asli dan yang palsu persis sama, sehingga korban tidak akan sadar sama sekali.

Contoh la in terjadi pada pelanggan internet banking milik Westpac Banking Corporation, sebuah bank senior di Australia. Modusnya adalah mengirimkan email spam yang berisi seakan-akan situs internet banking mereka akan melakukan upgrade software sistem, sehingga calon korban diminta meng-klik link yang tersedia dalam

email tersebut dengan dalih mempermudah akses agar tidak perlu mengetik sendiri alamat yang harus dituju. User yang ceroboh tentunya akan langsung klik saja link yang disediakan, padahal secara tidak sadar link itu tidaklah menuju situs yang dibicarakan, melainkan ke situs jebakan milik penjebak, hanya saja tampilannya situs palsu itu sangat mirip dengan yang asli.

Tidak hanya di internet, phishing juga bisa berlaku dalam dunia jaringan komunikasi seluler, modusnya kebanyakan adalah mengenai pembelian voucher prabayar, tapi ada juga yang menggunakan kebohongan bahwa calon korban mendapatkan hadiah undian melalui SMS.

G. Mencegah dan Melawan Phising

Berikut adalah beberapa tips yang bisa dijadikan sebagai pedoman untuk menghindari atau mencegah ‘phishing’ ini :

1. Ceklah dengan teliti URL atau address yang sedang Anda tuju, pastikan bahwa alamat yang tertera di Address bar adalah benar bahwa alamat tersebut adalah alamat yang Anda tuju.

2. Biasakan mengetik URL atau alamat situs yang Anda tuju, hindari link dari Web yang Anda rasa mencurigakan.

3. Gantilah password Anda secara berkala, baik 1 minggu, 2 minggu, 1 bulan atau pada periode tertentu, hal ini bermanfaat agar password Anda sulit dilacak.

4. Jangan pernah membalas **email** yang mencurigakan apalagi memasukkan sandi pada situs yang mencurigakan atau tidak anda percayai serta mengirimkan password dan data pribadi penting anda melalui email. Situs atau bisnis yang sah umumnya tidak akan meminta informasi melalui email.

5. Jika anda menerima permintaan informasi sensitif, buka jendela browser baru dan pergi kesitus organisasi dengan mengetik alamat website organisasi untuk meyakinkan bahwa anda sedang berhadapan dengan situs organisasi real dan

bukan dengan website phiser. Jika ada sesuatu yang diperlukan dari anda, biasanya ada pemberitahuan disitus organisasi ini atau jika anda tidak yakin dengan permintaan ini sebaiknya menghubungi situs organisasi tersebut untuk bertanya.

6. Jangan pernah membuka situs yang mencurigakan atau tidak anda percayai. Periksa URL untuk memastikan halaman sebenarnya adalah bagian dari situs organisasi dan bukan halaman penipuan pada domain yang berbeda seperti **mybankk.com** atau **g00gle.com**

7. Berhati-hati terhadap tawaran yang fantastis yang tampaknya terlalu mudah untuk menjadi kenyataan, ini mungkin PHISER.

8. Gunakan browser yang memiliki filter phising yang akan membantu anda mengetahui serangan phising potensial. Alamat situs yang aman dimulai dengan “https://” dan menampilkan icon Gembok terkunci diperamban anda.