KEJAHATAN DIDUNIA MAYA

1. KEJAHATAN PHISING

Phishing Merupakan Suatu Bentuk Kegiatan Yang Bersifat Mengancam Atau Menjebak Seseorang Dengan Konsep Memancing Orang Tersebut. Yaitu Dengan Menipu Seseorang Sehingga Orang Tersebut Secara Tidak Langsung Memberikan Semua Informasi Yang Di Butuhkan Oleh Sang Penjebak. Phishing termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi hacker cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang hacker.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam phishing. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh fake link pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran online. Untuk pengantisipasian serangan phishing semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada link yang masuk melalui akun sosial media maupun email yang di gunakan untuk akun sosial media. Karena link yang tidak di kenal patut di curigai sebagai serangan phishing yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain

1. SUMBER-SUMBER ANCAMAN PHISHING

Untuk mengetahui sumber-sumber ancaman phishing kami telah melakukan survey literatur phishing dengan membaca beberapa jurnal. Berikut adalah garis besar dari beberapa sumber ancaman phishing berdasarkan survey yang telah kami lakukan:

* email

Berdasarkan survey yang telah dilakukan pada tahun 2014 ada lebih dari 120.000 serangan phishing yang berpuncak pada miliaran transmisi email[1]. 65% dari serangan phishing mulai dengan mengunjungi link yang diterima dalm sebuah email[2]. Pada Maret 2016, 229.265 laporan emailphishing diterima oleh Kelompok Kerja Anti-Phishing dari konsumen[8]. 18,3% penduduk Australia menjadi korban dari phishing melalui email[8].

* Website

Phishing pada website meliputi iklan dan sosial media (Facebook, Twitter, Instagram). Berdasarkan survey yang telah dilakukan Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 bukan milik pengguna yang sebenarnya dan perkiraan sekitar 1,5% (14.320.000) adalah akun yang secara tidak sengaja menyebarkan isi berbahaya tanpa diketahui oleh pengguna, seperti pesan spam dan link yang mencurigakan [3]. Sebagian besar serangan phishing dilakukan melalui web server yang sudah dihackdan 73% situs telah menjadi korban[11]. Pada Maret 2016 123.555 situs phishing terdeteksi oleh Kelompok Kerja Anti-Phishing[8]. 15,7% penduduk Australia menjadi korban phishing melalui situs belanja online dan 6,9% melalui sosial media[8].

* Malware

Phishing yang dilakukan melalui penyebaran malwaresalah satunya adalah malware Koobface yang telah membuat 81% pengguna menjadi korbannya [3]

1. CARA KERJA PHISHING

* email

Berikut merupakan cara kerja phishing berdasarkan sumber-sumber ancaman phishing yang telah kami survey dari beberapa jurnal:

Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti link URL yang terdapat dalam email tersebut [2]. Pada dasarnya, phishing menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima email [9]. Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut [13]. Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi [15].

* website

Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti password dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas [7].Phiser juga menggunakan tool untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu [6]. Selain itu, phiser menciptakan embedding link untuk mendapatkan informasi sensitif milik korban [3].

* malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu file yang di kirim oleh phiser sebagai penetralisir malware di komputer nantinya [8].

1. CARA MENCEGAH PHISHING

Berikut adalah hasil survey kami mengenai cara pencegahan atau antisipasi terhadap serangan phishing melalui website dari beberapaliteratur :

* Medeteksi dengan toolsdetect

Sekarang ini internet sudah dianggap sebagai makanan sehari-hari, bahkan ada beberapa orang yang beranggapan tanpa internet mereka tidak bisa hidup. Ada banyak hal yang bisa kita lakukan dengan internet, mulai dari mencari informasi, berbagi informasi, dsb. Namun, pasti kita pernah menjumpai situs-situs yang muncul tanpa kita inginkan dan mengandung informasi berhadiah yang menggiurkan. Tentu saja hal tersebut akan menarik kita untuk mengisinya dengan data penting tanpa tau bahwa itu hanyalah situs phishing. Untuk mencegah hal tersebut kita dapat menggunakan toolsdetect yang mana dapat membedakan mana situs yang asli dan palsu (phishing). Berikut toolsdetect yang dapat digunakan

* PhishShield

PhishShield merupakan aplikasi desktop yang berkonsentrasi pada URL dan konten situs web phishing [13]. Cara kerjanya dengan mengambil URL sebagai masukan dan outputnya berupa status yang mengkonfirmasi URL [13] termasuk phishing atau situs asli [13]. Tingkat akurasi yang diperoleh untuk PhishShield adalah 96,57% dan mencakup berbagai situs phishing yang dihasilkan tingkat kepalsuan negatif dan positif [13]

* LinkGuard Algoritma

LinkGuard Algoritma digunakan untuk menganalisis dua URL dan akhirnya tergantung pada hasil yang dihasilkan oleh algoritma [15]. URL tersebut adalah URL yang melibatkan ekstraksi URL yang sebenarnya dan URL visual (yang dilihat pengguna) [15].

* PhishDetector

PhishDetector adalah ekstensi browser yang digunakan untuk mendeteksi serangan phishing yang mana menggunakan algoritma pencocokan string perkiraan untuk menentukan hubungan antara konten dan URL dari suatu halaman web[11].

* Menggunakan add ons web browser anti tabnabbing

Setiap tahunnya para phisher melancarkan aksi-aksinya dengan membuat serangan-serangan baru. Dan salah satu serangan baru tersebut yaitu bernama tabnabbing. Serangan phishing tersebut dapat menyerang pada web. Dimana cara penyerangannya ketika pengguna membuka banyak tab, phishing tersebut akan terbuka di sela-sela tab yang lain. Saat pengguna lengah, maka tab tersebut akan di buka dan serangan di mulai. Tab palsu itu di samarkan menjadi salah satu tab yang di buka oleh pengguna dan tab asli yang sebelumnya lenyap. Untuk itulah serangan ini di anggap serangan yang pintar karena tidak lagi menggunakan link yang di klik dulu agar pengguna masuk perangkap phisher. Namun sepintar apapun suatu serangan, pasti ada jalan keluar. Beberapa cara pencegahan serangan tabnabbing: a) Ketika pengguna membuka firefox dan terjadi serangan, pengguna bisa mengatasi serangan dengan account manager. Account manager dapat mengamankan pengguna karena pengguna di sarankan menyimpan login dan saat itu juga pengguna di berikan password acak setiap kali login [14]. b) Tidak hanya pada firefox saja, pada crome juga di berikan pengamanan terhadap phishing tabnabbing. Yaitu menggunakan AgenTab. AgenTab melakukan tindakan ketika pengguna mulai membuka situs web [14]. AgenTab akan menyalakan peringatan ketika serangan terdeteksi. Peringatan tersebut akan muncul ketika tab tiba-tiba berubah tempat [14]. c) Dan yang terakhir dalam pencegahan tabnabbing dapat di lakukan dengan NoTabNab4. Add-on tersebut di usulkan oleh web browser Unlu dan Bicakci, dimana serangan phishing dapat diketahui saat suatu tab palsu meniru tab asli lalu add-on tersebut bekerja dengan cara memperingati dengan memberi tanda warna kuning atau merah sesuai tingkat serangan pada highlightned [14].

* Menggunakan mekanisme pre-filter

Pencegahan phishingjuga dapat di lakukan dengan penggunaan anti-phishing pre-filter ini. Di dalam pre-filter terdapat tiga bagian pencegahan yakni Site Identifier, Login Form Finder, dan Webpage Feature Generator. Ketiganya tersebut melakukan pencegahan secara berurutan. Site Identifier digunakan untuk mengurangi jumlah perhitungan situs yang tidak perlu dan hanya mendeteksi halaman yang sah [6]. Kemudian Login Form Finder di gunakan untuk menyaring halaman tanpa bentuk login lalu menghentikan mereka dari proses lebih lanjut karena form login merupakan satu-satunya cara untuk menyadarkan pengguna bila informasi pribadinya dicuri oleh phiser [6]. Sistem ini dapat mengurangi kesalahan positif dari sistem tanpa harus mencurigai jumlah kesalahan negatif [6]. Yang terakhir adalah Webpage Feature Generator, dimana fungsinya adalah mengidentifikasi halaman web phishing dengan melacak karakteristik phishing yang di pamerkan dalam halaman tersebut [6]. Seseorang dapat menggunakan cara ini ketika merasa bila halaman webnya sudah terserang phishing

* Pendeteksian dengan streaming analytics ‘PhishStrom’

Sekarang ini banyak sekali orang-orang yang berlomba-lomba melakukan penelitian untuk menciptakan suatu alat maupun aplikasi. Namun bukan hanya itu saja. Orang-orang juga mulai melakukan pendeteksian dengan berbagai cara. Dan anti phishing kali ini yaitu melakukan pendeteksian berupa streaming analisa menggunakan PhisStrom. PhisStrom sendiri di gunakan untuk mendeteksi URL yang terserang phishing. Dalam percobaannya, pendeteksian dengan cara ini dapat menghasilkan akurasi klasifikasi 94, 91% dengan tingkat positif palsu yakni 1,44% [10]. Untuk risiko pada pengujian dataset menunjukkan pengidentifikasian 99,22% pada web yang sah dan phishing 83,97% [10]. Untuk selanjutnya, PhisStrom dapat di gunakan sebagai alat add-on pada Mozila Firefox agar mempermudah dalam pendeteksian serangan phishing pada web