Penerbit : Jasakom

http://www.Jasakom.com/penerbi-

HACK ATTACK

Konsep, Penerapan dan Pencegahan

Penulis : Harianto Ruslim, CEH

Certified Ethical Hacker

HACK ATTACK : Konsep, Penerapan dan Pencegahan
Oleh : HR-Harianto Ruslim, CEH (Certified Ethical Hacker)

ISBN : 979-98545-5-5

Cetakan pertama : Oktober 2005

Kata Pengantar

Perkembangan Teknologi Informasi berkembang dengan sangat pesat sehingga bahkan orang yang bergelut di bidang IT pun kadang kala kesulitan untuk terus mengikuti perkembangannya. Terlebih sejak dengan adanya Internet yang secara tidak langsung menghubungkan jutaan jaringan computer (LAN) yang ada.

Hal ini membuat "information sharing" terjadi dengan sangat cepat dalam hitungan menit bahkan detik. Coba bandingkan dengan sebelum adanya Internet. Kita masih berkirim surat yang notabene akan sampai paling cepat dalam 1 hari, namun dengan teknologi Internet melalui pemanfaatan email, dalam waktu singkat sudah bisa sampai di tujuan.

Di satu sisi dengan adanya Internet terlihat sangat bermanfaat dalam hal komunikasi infomasi. Namun di sisi lain ternyata menyimpan ancaman / bahaya yang juga besar terutama terhadap integritas data personal maupun perusahaan. Karena banyak sistem komputer yang bisa di-exploit oleh para hacker yang memanfaatkan lubang security di berbagai sistem termasuk sistem operasi, aplikasi maupun database. Bahkan komputer yang sifatnya digunakan untuk personal di rumah juga tidak luput dari sasaran para hacker. Intinya di mana ada lubang yang bisa disusupi, akan mereka manfaatkan.

Hal ini disebabkan oleh karena para programmer yang membuat sistem operasi, aplikasi maupun database dulunya tidak berpatokan atau memperhatikan sisi keamanan / security. Bahkan satu vendor software yang besar yaitu Microsoft, baru memperhatikan security mulai pada awal tahun 2003 dengan pernyataan dari pimpinan mereka secara langsung, Bill Gates. Bahwa mulai tahun 2003 mereka akan fokus terhadap security. Faktanya memang sejak Windows NT 4.0 sampai saat ini, sistem operasi berbasis Windows ini yang paling banyak di-exploit oleh para hacker. Hal ini disebabkan awalnya Microsoft sendiri tidak terlalu *concern* dengan security. Faktor lainnya karena sistem operasi ini yang

paling banyak dikenal dan digunakan.

Insiden security sendiri dari tahun ke tahun juga semakin meningkat. Ada satu organisasi independen yang memantau insiden ini yaitu CERT (Computer Emergency Response Team) yang berdiri tahun 1988 di Amerika, dari tahun ke tahun sejak mereka berdiri insiden yang dilaporkan selalu meningkat dan mencapai angka yang sulit untuk dipercaya. Itu untuk insiden yang terlacak atau dilaporkan oleh perusahaan yang menjadi korban. Tidak termasuk mereka yang tidak melapor. Atau mereka (organisasi) yang mungkin tidak tahu kalau mereka sudah menjadi korban.

Bagaimana cara membantu untuk mengatasi masalah ini ? Salah satunya adalah melalui edukasi.

Industri IT berkembang jauh lebih cepat dibanding dengan usaha yang bisa kita lakukan untuk meng-training orang IT kita. Oleh sebab itulah, penulis ingin menulis buku ini yang bisa bermanfaat bagi dunia IT khususnya di Indonesia untuk mempelajari IT Security ini secara lebih mendalam. Penulis akan mencoba membahas berbagai sisi security berdasarkan pengalaman penulis selama ini sebagai konsultan security, pembahasan dititikberatkan pada sisi konsep sehingga dapat membantu mempermudah pemahaman.

Pembahasan akan dimulai dari data security sampai dengan physical security. Semuanya ditujukan untuk membantu melakukan proteksi terhadap berbagai ancaman (threat) pada sistem komputer yang terutama memproteksi data kita.

Selama dalam penulisan buku ini, penulis mengalami kerusakan pada sistem operasi yang digunakan, karena mencoba beberapa exploit dan Trojan serta bermain-main di situs underground yang berakibat harus menginstall ulang sistem operasi, namun masih beruntung karena tidak berakibat pada kerusakan data yang sebelumnya memang sudah dilakukan backup.

Oleh sebab itu, jangan pernah lupa backup data anda !. Sehingga apabila yang sesuatu terjadi pada komputer kita, data kita

tetap masih ada.

Penulis juga tak lupa sangat mengharapkan berbagai masukan berupa kritik maupun saran sehingga dapat menjadi masukan yang berharga dalam penulisan buku selanjutnya. Buku ini semoga dapat menjadi jawaban yang memberikan edukasi dan pemahaman seputar security atau keamanan komputer bagi pembaca atau pengguna komputer yang awam terhadap security. Segala masukan dan saran bisa di-email ke harry2009@gmail.com.

Dalam penulisan buku ini, penulis sengaja 'mempertahankan' istilah-istilah security tetap dalam bahasa Inggris dan tidak diterjemahkan, agar supaya tidak merubah inti atau isi yang dimaksud.

Semoga buku ini berguna dan menjadi panduan untuk mengenal IT security lebih mendalam terutama jenis dan tipe ancaman / threat yang ada.. Selamat Membaca.

Daftar Isi

“Buku ini didedikasikan kepada masyarakat Indonesia khususnya yang bergelut di dunia IT. “

Saya juga ingin berterima kasih kepada orang tua dan saudara-saudara yang mendukung segala usaha saya. Mantan pacar saya, Maria Yeny, yang setia memotivasi dan bahkan tak bosan mengingatkan untuk menyelesaikan buku ini di sela kesibukan dan aktivitas lainnya.

Special thank’s juga buat S’to yang banyak membantu dalam penulisan buku ini. Juga kepada teman-teman lain yang tidak bisa saya sebutkan satu-per-satu. Dan tak lupa juga kepada mereka yang telah dan sering mengirimkan email ke saya, sehingga memberikan ide, masukan and inspirasi baru dalam penulisan ini.

And most of all, Thank’s to God for making my wish comes true.

Introduction

Dua tahun ini, security awareness atau perhatian terhadap security di Indonesia meningkat dengan signifikan. Terbukti dengan perusahaan-perusahaan besar dan menengah umumnya sudah meng-implementasikan firewall, IDS maupun IPS serta tools dan teknologi security lainnya.

Membahas mengenai security tidak lepas dari resiko / risk yang ditimbulkan dari ancaman / threat yang ada. Threat bisa berupa orang atau proses yang melakukan eksploitasi lubang security (vulnerability) dari sistem komputer. Ancaman / threat yang dikenal antara lain virus, worm, spyware, serangan DoS (Denial of Service), pencurian informasi, power failure (mati listrik), banjir maupun api.

Vulnerability contohnya bug atau cacat pada software seperti sistem operasi, firewall, aplikasi dll. Atau sistem yang tidak dipasangi anti virus, sistem yang salah konfigurasinya atau dibiarkan default (tanpa dirubah sesudah instalasi). Vulnerability atau threat bagi masing-masing organisasi berbeda. Bagi perbankan atau institusi finansial, pencurian data / informasi menjadi prioritas utama. Bagi kalangan universitas, ketersediaan (availability) dari sistem komputer menjadi prioritas utama.

Kalau kita lihat, ancaman /threat serta vulnerability cukup luas. Namun salah satu cara untuk membatasi cakupan threat dan vulnerability sehingga penangulangannya bisa lebih terstruktur adalah dengan membagi security ke dalam domain-domain. Masing-masing domain dibatasi secara logikal maupun fisik antara lain :

- Physical Security Domain - domain ini membatasi akses secara fisik terhadap sistem atau peralatan IT, ruangan, gedung atau resource lainnya. Secara lebih mendetil, bisa dilihat di bab physical security
- Network Security Domain - domain ini membatasi dan mengontrol akses terhadap sumber daya (resources) dari jaringan / network. Contohnya hanya karyawan permanen

yang bisa akses ke informasi / data di server atau menggunakan printer jaringan.

- Application Security Domain - domain ini dibatasi secara logikal pada aplikasi. Contohnya pada aplikasi akunting, akses ke modul A/R (Account Receivable) dan modul A/P (Account Payable) dibedakan.
- Data Security Domain - sekilas domain ini terlihat overlap (tumpang tindih) dengan domain lainnya. Namun kalau kita gali lebih lanjut, domain ini merupakan inti dari domain - domain sebelumnya. Karena data / informasi merupakan obyek yang menjadi incaran dari hacker / ancaman lainnya. Contoh aplikasi dari domain ini adalah enkripsi data. Data yang ditranmisikan melalui jaringan perlu dienkripsi terutama melalui jaringan umum seperti Internet.

Kalau kita lihat, pembagian domain di atas hanya 4 security domain. Bagi penulis sebenarnya itu sudah cukup mewakili IT security, meskipun menurut International Information Systems Security Certifications Consortium $(ISC)^2$, bahwa IT security sendiri dibagi menjadi 10 domain yaitu Security Management Practices, Access Control, Security Models dan Arsitektur, Physical Security, Telekomunikasi dan Networking Security, Cryptography, Business Continuity Planning, Hukum - Investigasi dan Kode Etik, Aplikasi dan System Development serta Operations Security.

Di lain kesempatan, dalam buku selanjutnya, penulis akan menulis lebih lanjut mengenai 10 domain menurut $(ISC)^2$ ini.

Buku ini dititik beratkan pada ancaman/threat yang ada saat ini mencakup malware (virus, worm, trojan, backdoor, spyware dll), teknik dan metode hacker dalam menjalankan aksi mereka, phishing yang bisa merugikan konsumen perbankan, spam maupun teknik social engineering yang digunakan untuk mendapatkan informasi tanpa menggunakan IT tools apapun.

Ancaman / threat ini makin hari semakin nyata dengan banyaknya berita mengenai insiden security di situs-situs berita Internet yang terjadi hampir tiap hari. Situs web di-deface - diganti halaman index-, situs web tidak bisa diakses karena serangan

DoS (Denial of Service), penyebaran virus worm baru yang semakin ganas, spyware yang memata-matai korban dan mengambil datanya serta informasi kartu kredit dicuri orang,

Bahkan Indonesia pada tahun 2005 ini sudah menduduki peringkat pertama dunia dalam hal 'carding' - pencurian dan penyalahgunaan kartu kredit dalam belanja online-. Sehingga kartu kredit yang berasal dari Indonesia umumnya sudah tidak bisa digunakan untuk melakukan transaksi online di Internet. Bukan hanya itu, situs belanja online tertentu juga melakukan blocking terhadap alamat IP dari Indonesia .

Masing-masing threat juga ber-evolusi mengikuti perkembangan dan teknik yang digunkanan. Contohnya hacker berhasil mendapatkan cara untuk masuk ke satu sistem dengan mengeksploitasi lubang security yang berhasil ditemukan. Para security professional dan system administrator mencari cara baru untuk mengatasinya, dengan cara melakukan deteksi dini dengan tool IDS (Intrusion Detection System). Hacker pun mencari cara baru untuk mengakali tool deteksi ini. Dan seterusnya.

Kejar mengejar antara hacker dan security professional ini tidak ada habisnya. Sama dengan kejar-kejaran antara pembuat virus dan pembuat anti-virus. Lalu bagaimana kita menyikapinya ? Apakah kita diam saja, sebagai penonton dan menunggu menjadi korban selanjutnya ? Atau dengan implementasi tool yang seadanya ?.

Security management bukanlah satu proses yang statik. Perlu di-ingat, security itu mencakup tiga komponen utama yaitu People, Process dan Teknologi (PPT). Process di sini contohnya adalah pembuatan security policy, guideline atau prosedur security. Sedangkan teknologi yang merupakan tools-tools security itu sebagai implementasi dari security policy yang sudah dibuat (security policy enforcement). Dan kedua komponen ini tidak akan bisa jalan, tanpa adanya People atau orang yang membuat, mengawasi, memonitor, meng-evaluasi security tersebut.

Untuk lebih detil mengenai ancaman / threat, teknik-teknik hacker, berikut langkah pencegahannya, bisa dilihat di bab-bab selanjutnya.

Bab 10
Security Threat

Kebanyakan perusahaan masih bergantung dengan firewall, IDS dan security tools lainnya. Bahkan sekarang muncul solusi baru yang sedang trend yaitu IPS – Intrusion Prevention System. Ada paradigma yang salah di kalangan sebagian orang IT bahwa dengan implementasi tool seperti halnya firewall, IDS, IPS dsbnya, environment mereka sudah aman dari gangguan hacker maupun intruder.

Hal ini terlihat pada waktu kejadian, di mana divisi IT dari Komisi Pemilihan klaim tingkat keamanan yang diterapkan sangat tinggi bahkan sampai 7 lapis firewall dan klaim-klaim lainnya yang total jendral kabarnya menghabiskan dana milyaran rupiah.

Namun dengan mudahnya dijebol dengan menggunakan teknik hacking yang sudah cukup lama beredar di dunia bawah tanah (underground) yaitu SQL Injection. Untuk mempelajari trik dan prosesnya, anda bisa search di Internet ataupun membaca buku karangan teman saya, S'to – Seni Internet Hacking.

Sejalan dengan perkembangan security, orang mulai menyadari bahwa sebenarnya tool security saja tidak cukup. Firewall dan IDS itu saja tidak cukup. Perlu adanya satu mekanisme atau cycle yang mengatur perihal security ini antara lain adalah security policy atau semacam guideline / standar bagi perusahaan yang mengatur penggunaan segala sesuatu yang berkaitan dengan akses komputer.

Perimeter security atau security di level gateway (perbatasan antara jaringan internal dengan jaringan luar seperti Internet) tidaklah cukup meskipun itu jelas masih diperlukan. Oleh sebab itulah, penulis menambahkan bab ini dalam buku ini yaitu membahas mengenai system security. Computer system sendiri definisinya adalah semua komponen perangkat keras maupun lunak yang jalan di komputer.

Oleh sebab itu secara umum, bisa dikatakan bahwa system security adalah aspek keamanan atau security yang mencakup perangkat keras dan lunak di komputer.

Namun yang akan dibahas selanjutnya lebih ke arah perangkat lunak karena pada dasarnya untuk perangkat keras possibility untuk di-hack lebih kecil bukan tidak mungkin. Percobaan yang pernah dilakukan dalam merusak monitor dengan memainkan frekuensi refresh ratenya ternyata dapat membuat jebol monitor / layar komputer.

Saat ini yang ramai dibicarakan dari sisi security adalah mengenai vulnerability atau kelemahan atau mudah diserang terhadap server atau PC dalam hal ini aplikasi maupun sistem operasi. Bagaimana para vendor security berbondong-bondong untuk menawarkan solusi melakukan 'hardening' sistem operasi baik melalui yang namanya Patch management maupun dengan Host Based Intrusion Detection.

Namun sejalan dengan perkembangan dan perubahan ancaman, persepsi perimeter security itu sendiri, security sekarang lebih ditujukan ke sistem dan user / pengguna.

Terbukti bahwa pangsa pasar solusi security untuk solusi 'threat' masing menduduki persentase tertinggi yaitu di atas 50 %.

Software Security–Kesalahan Logika Programmer ?

Dalam membangun sebuah system khususnya aplikasi perlu mempertimbangkan dari segi security. Dulunya hal ini tidak menjadi isu karena umumnya sebuah jaringan komputer sifatnya masih "tertutup" artinya tidak terhubung dengan dunia luar. Jadi hanya sebatas penggunaan internal, aliran dan komunikasi data hanya terbatas di dalam satu jaringan yang terhubung saja.

Namun isu security muncul seiring dengan perkembangan Internet yang notabene merupakan jaringan komputer terbesar di dunia yang menghubungkan jutaan jaringan komputer lainnya.

Software security erat hubungannya dengan patch yang sudah sering kita dengar. Bagian penjelasan ini sangat erat kaitannya dengan bagian 'vulnerability management'. Karena vulnerability management pada dasarnya solusi untuk mencari lubang security pada software baik berupa aplikasi, sistem operasi maupun firmware yang terdapat pada device (hardware) seperti router.

Intel sendiri pada tahun 2002 telah mengaplikasikan sebanyak 2,4 juta patches ke system jaringan mereka sendiri. *(Source: Intel White Paper)*

Ironisnya adalah para maintenance programmer sendiri menulis program patch dengan menggunakan metodologi pengembangan software yang sama dengan pada saat mereka membangun suatu aplikasi. Sehingga hal ini menyebabkan patch tersebut tetap tidak menyelesaikan masalah dan kode-kode yang dibuat tersebut tetap mengandung 'bug' atau celah security.

Isu lainnya adalah karena pertimbangan-pertimbangan bahwa programmer men-develop software atau aplikasi dengan fokus pada fungsionalnya atau kinerja dari software tersebut. Sehingga faktor security dikesampingkan. Hal ini juga di-aminin oleh sahabat saya yang menjabat sebagai architect developer DotNet di Silicon Valley.

Faktor lainnya yaitu penerapan security dapat mempengaruhi kinerja (performance). Sebagai contoh, coba bandingkan akses http dengan https (encrypt), jelas akses https jauh lebih lambat!.

Salah satu contoh sederhana lainnya yaitu penggunaan anti virus. Pada saat implementasi awal anti-virus, saya sangat yakin bahwa akan banyak respon dari pengguna (end-user) yang komplain bahwa PC atau komputer yang mereka gunakan menjadi lebih lambat dan mengganggu pekerjaan mereka. Tapi bagi orang security, itu merupakan bagian yang wajib di-implementasikan.

Software security merupakan bagian yang sulit dari security untuk di-solve. Karena di satu sisi, para programmer dikejar deadline atau waktu, di satu sisi fokus kepada fungsional software tersebut, di sisi lainnya adalah adanya 'perang' fitur dengan kompetitor lain yang mengeluarkan solusi yang sejenis sehingga tidak sempat untuk berpikir mengenai security.

Di luar daripada itu ada 3 hal pokok sumber dari permasalahan pada software security ini yaitu

- Konektivitas (Connectivity) – pengembangan software mengacu atau fokus pada Internet, di mana banyak kebutuhan supaya software tersebut bisa diakses dari mana saja dengan koneksi via Internet. Karena tuntutan pekerjaan maupun infrastruktur serta rekanan yang tersebar / distributed.
- Complexity (kompleksitas) – membangun software dengan memperhatikan aspek mobile ini tidak semudah yang dibayangkan
- Extensibility - tuntutan sistem yang berkembang secara cepat di mana software juga dituntut untuk mengikuti perkembangan sehingga terjadi perubahan kode software di tengah jalan.

Bagi para vendor software mungkin mereka akan beralasan bahwa mereka punya prosedur yang standar dalam pengembangan software, mereka punya tim QA (Quality Assurance) dalam pengecekan dan test software sebelum diluncurkan atau mungkin punya tim khusus untuk melakukan validasi atau pengecekan terhadap kode software tersebut.

Perlu diingat bahwa masing-masing pribadi mempunyai alur

logika (logic) yang unik sehingga tiap pribadi alur logikanya bisa berbeda antara yang satu dengan yang lain. Sehingga pengecekan terhadap kode software bisa menjadi tidak efektif. Ataupun software sendiri mempunyai 1001 sisi yang perlu dites, dengan kata lain bisa dipastikan ada bagian yang pasti luput dari pengetesan.

Salah satu vendor sistem operasi bahkan pernah mengerahkan sebagian besar developer-nya untuk mengecek kembali source-code buatan mereka untuk mencari vulnerability. Namun kenyataannya, hal ini tidak cukup membuat sistem mereka menjadi lebih aman atau 'bug'-nya berkurang.

Beberapa hal yang berkaitan dengan 'cacat' di software adalah:

- Buffer Overflow (dibahas di bagian fase hacking)
- Variabel yang digunakan (environment variables)
- System calls atau sering disebut system(). Bagian ini berkaitan dengan sistem operasi di mana software berjalan di atasnya
- Input yang tidak divalidasi –bagian ini juga ada relasi dengan buffer overflow.

Untuk mendapatkan atau mencapai aman 100% dalam hal security khususnya di software security adalah hal yang tidak mungkin. Namun yang bisa kita lakukan adalah meminimalisasi efek yang bisa ditimbulkan atau mencoba melakukan hal-hal seperti berikut ini:

- Developer Resources artinya sebelum membangun suatu software, kita perlu mengacu atau mencari resource "Best Practice" secara design dan arsitekturnya. Yang kemudian bisa kita kelompokkan bagian masing-masing (prosedural) berdasarkan tier misalnya business-logic tier, presentation tier maupun yang menjembatani keduanya atau sering disebut dengan middleware tier
- Awareness Training – bagian ini sangat penting untuk men-drive security awareness sehingga software yang dikembangkan selalu mengacu pada sisi security.

Training ini juga mencakup developer atau programmer, arsitek, tester dan management.

- Software Development LifeCycle – lifecycle dari software development adalah antara lain analisa kebutuhan (requirement analysis) termasuk memasukkan unsur security dan risk analysis, perancangan (design), test plan, coding, dan test hasilnya. Pada bagian test hasil bisa dimasukkan unsur dari security yaitu penetration testing untuk mencari 'flaw' atau cacat pada software yang mungkin bisa ditembus dengan berbagai teknik hacking. Selanjutnya melempar ke market atau pasar dalam bentuk beta testing dan memperbaiki software tersebut berdasarkan 'feedback' yang didapatkan.
- Menggunakan pendekatan berdasarkan resiko
- Perbaiki cacat yang ditemukan

Phishing – Merampok Nasabah Internet Banking

Istilah ini mungkin masih terdengar asing, namun sebenarnya bukanlah hal baru. Masih ingat dengan kasus web site BCA yang di-plesetkan ? dengan memanfaatkan salah ketik dari nasabahnya misalnya www.kilkbca.com atau www.klicbca.com dan berbagai variasi lainnya, di mana link sebenarnya adalah www.klikbca.com

Sehingga pengguna BCA Internet Banking yang tidak teliti dalam mengetikkan link asli tersebut akan masuk ke situs yang sengaja dibuat untuk mendapatkan account dan password internet banking. Aksi ini sendiri sebenarnya sudah bisa dikategorikan dengan tindakan 'hacking' dengan menggunakan cara 'social engineering'.

Phishing atau Password Harvesting Fishing arti sebenarnya adalah tindakan dengan menggunakan alamat email ataupun alamat situs yang dipalsukan dan dirancang untuk mengelabui sang penerima untuk mendapatkan data-data berupa nomor

kartu kredit, account transaksi dan password, beserta informasi penting lainnya.

Dengan meniru atau membajak nama bank terkenal, penjual online yang terkenal, dan perusahaan kartu kredit, para phisher (istilah pelaku phishing) dapat meyakinkan sejumlah 5% dari target korban mereka untuk merespon terhadap undangan mereka.

Misalnya asumsi phisher mengirimkan email ke 1000 calon korban berarti yang akan respon terhadap ajakan mereka misalnya melakukan update informasi atau data mereka akan ada sekitar 50 orang. Hasil ini merupakan penelitian yang pernah dilakukan terhadap perkiraan korban phishing.

Umumnya yang terjadi pada tindakan phishing adalah seseorang menerima email yang mengiring si penerima untuk melakukan update informasi yang sifatnya personal seperti password, user account, nomor kartu kredit, tanggal lahir, nomor account di bank dan sebagainya.

Situs ini sendiri sebenarnya adalah situs palsu atau gadungan, dan dibuat dengan tujuan untuk mengelabui pengunjungnya. Sebagai contoh pada tahun 2003 lalu, para pengguna ebay ada yang menerima email seakan-akan dikirim oleh ebay. Email tersebut menyuruh user untuk melakukan update informasi personal seperti nomor kartu kredit dsbnya, yang apabila tidak dilakukan maka account mereka akan dibekukan. Dan cukup banyak yang tertipu pada saat itu. Bahkan saya juga menerima email eBay palsu beberapa kali. Bahkan trik ini pada tahun 2005 ini masih muncul dan mencari korban pengguna eBay.

Untuk membuat situs yang persis sama dengan aslinya merupakan hal yang sangat gampang dilakukan seperti halnya yang pernah dilakukan oleh Steven yang mem-plesetkan alamat situs internet banking BCA dengan memanfaatkan 'human error' dalam kesalahan mengetik alamat situs.

Kita langsung pelajari case-by-case phishing ini sehingga ada gambaran, bagaimana untuk trace sumber dari satu situs yang dikirim via email. Apakah dari sumber yang benar ?

Di bawah ada beberapa case yang akan saya bahas termasuk case untuk citibank dan washington mutual.

Case 1 - Citibank (www.citi.com / www.citibankonline.com)

Berikut adalah contoh email dari Citibank yang palsu

-----Original Message-----

```
From:   CITI [mailto:identdep_op26461529008752@citibank.com]
Sent:   Wednesday, September 08, 2004 3:26 PM
To:     harrylim@cbn.net.id
Subject:        Citibank Reminder: Please Update Your Data
[Wed, 08 Sep 2004 01:25:12 -0700]
```

<https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp>

Bagaimana kita trace alamat ini apakah valid atau tidak ? Apakah benar dari citibank ?

Di bab 2, telah dibahas langkah-langkah untuk mencari atau mengali informasi mulai dengan kita hanya tahu alamat atau URL situs.

Untuk case ini, kalau kita trace dengan view source email ini. Maka didapatkan:

```
href="http://
%31%34%38%2E%32%34%34%2E%32%31%33%2E%31%33%31:%38%38/
%63%69%74/%69%6E%64%65%78%2E%68%74%6D">https://web.da-
us.citibank.com/Iogin.ref.999685633/scripts/client_conf.
jsp</a>
```

Di mana mereka melakukan spoofing, tertulis https://web.da-us.citibank.com seakan-akan benar-benar dari citibank dan dibuat memberi kesan 'secure' karena menggunakan protokol https. Yang memang biasanya digunakan oleh bank pada um-

umnya, padahal situs ini mengarah ke

```
http://%31%34%38%2E%32%34%34%2E%32%31%33%2E%31%33%31:%38%38
```

Terlihat dari alamatnya di-spoof dengan menggunakan hex dan tidak menggunakan https. Yang setelah saya lakukan decode, saya dapatkan alamat IP nya 148.244.213.131:88.

Angka 88 di belakang merupakan nomor port yang digunakan.**Lalu sebenarnya hostnya apa dan sumbernya dari negara mana?**

Coba kita trace dengan menggunakan command traceroute

```
C:\>tracert 148.244.213.131
Tracing route to host-148-244-213-131.block.alestra.net.mx
[148.244.213.131]
over a maximum of 30 hops:

1  200ms 191ms  190ms  nas2-3.cbn.net.id [202.158.2.236]
2  191ms 180ms  190ms  nas2-rtif.cbn.net.id [202.158.2.233]
3  190ms 180ms  180ms  202.158.31.33
4  180ms 190ms  191ms  202.158.31.241
5  180ms 181ms  180ms  202.158.31.226
6  190ms 190ms  190ms  202.93.46.137
7  190ms 190ms  190ms  gw-en-kppti.palapanet.com
[202.93.46.134]
8  360ms 371ms  360ms  500.POS2-1.IG2.SAC1.ALTER.NET
[157.130.210.217]
9  361ms 370ms  371ms  0.so-0-0-0.XR1.SAC1.ALTER.NET
[152.63.54.114]
10 961ms 451ms  380ms  0.so-0-1-0.XL1.SAC1.ALTER.NET
[152.63.53.241]
11 361ms 370ms  361ms  POS6-0.BR5.SAC1.ALTER.NET
[152.63.52.225]
12 360ms 361ms  421ms  204.255.174.174
13 541ms 1502ms 370ms  tbr2-p013202.sffca.ip.att.net
[12.123.13.70]
14 2323ms721ms  511ms  tbr1-cl3.la2ca.ip.att.net
[12.122.10.26]
15 441ms 1042ms 691ms  tbr1-cl2.dlstx.ip.att.net
[12.122.10.49]
16 1492ms2594ms 1882ms gbr2-p10.dlstx.ip.att.net
```

```
[12.122.12.62]
17 1222ms1372ms 430ms  gar1-p370.dlstx.ip.att.net
[12.123.16.237]
18 3425ms1092ms 1251ms 12.119.124.90
19 451ms 451ms  440ms  rcmex1.att.net.mx [200.94.59.33]
20 460ms 471ms  461ms  rcgdl1.att.net.mx [148.244.145.190]
21 451ms 440ms  451ms  ragdl2.att.net.mx [200.76.5.3]
22 460ms 471ms  461ms  host-200-56-123-238.block.alestra.net.
mx [200.56.123.238]
23 471ms 460ms  471ms  host-148-244-213-131.block.alestra.net.
mx [148.244.213.131]

Trace complete.
```

Hmmm, ternyata sumbernya dari negara mx atau Mexico. Dan di-hosting di jaringan att.net.

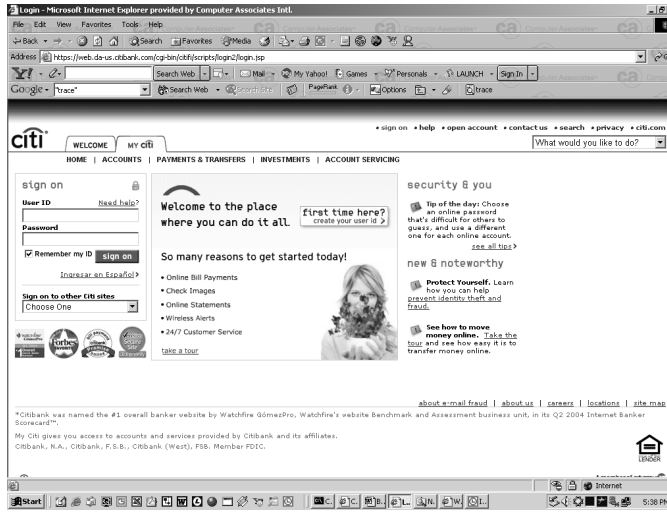
Sedangkan kalau kita ping alamat aslinya

```
C:\>ping web.da-us.citibank.com
Pinging web.da-us.citibank.com [192.193.187.86] with 32 bytes
of data:

Request timed out.
Request timed out.
```

Terlihat bahwa alamat IP dari situs sebenarnya adalah 192.193.187.86, dan kalau kita masukkan IP ini ke URL, maka akan dibawa ke situs aslinya

Citibank. Dan di sebelah kanan bawah dari situs Citibank yang asli ini terdapat gambar gembok. Yang merupakan tanda / lambang dari digital certificate. Certificate ini dikeluarkan oleh Verisign untuk Citibank. Namun apakah ini menjamin bahwa situs Citibank asli atau tidak ?

Belum tentu ! Karena certificate ini bisa dipalsukan dengan cara di-copy.

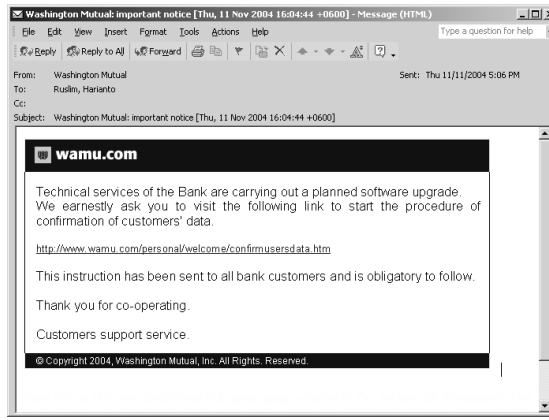


Situs Asli Citibank

Digital Certificate Situs Citibank

Case 2 – Washington Mutual (www.wamu.com)

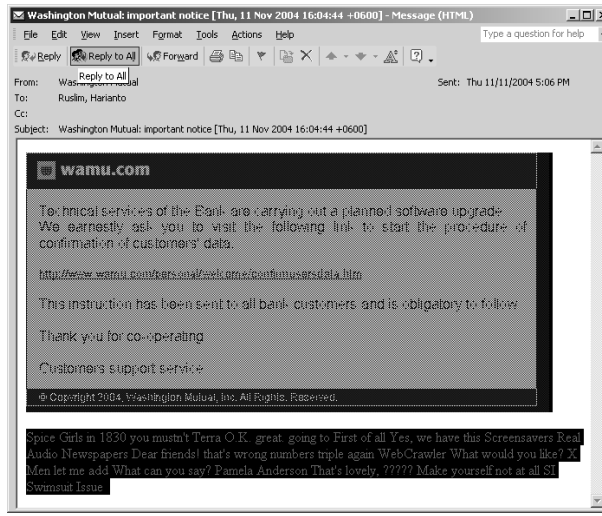
Case kedua ini saya ambil contoh dari email yang juga saya terima. Mutual Washington merupakan perusahaan keuangan yang berbasis di Amerika.



Email Dari Mutual Washington Palsu

Dan tanpa sengaja sewaktu saya ingin meng-highlight tulisannya, saya dapatkan signature dari si penulisnya. Mungkin dia juga lupa. Signature di bagian bawah emailnya adalah:

Spice Girls in 1830 you mustn't Terra O.K. great. going to First of all Yes, we have this Screensavers Real Audio Newspapers Dear friends! that's wrong numbers triple again WebCrawler What would you like? X Men let me add What can you say? Pamela Anderson That's lovely, ????? Make yourself not at all Sl Swimsuit Issue



Email Dari Mutual Washington Palsu - DiHighLight

Kalau kita membaca message seperti di atas, bisa kita confirm bahwa emailnya pasti palsu. Kemungkinan email ini merupakan automated message yang di-generate oleh server. Dan kalau kita lihat source dari email tersebut :

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>Message</TITLE>
<META http-equiv=Content-Type content="text/html; charset=us-
ascii"><MAP
name=FPMap0><AREA shape=RECT coords=0,0,590,292
  href="http://%32%30%30%2E%39%34%2E%39%36%2E%34:%38%37/
%77%61/%69%6E%64%65%78%2E%68%74%6D"></MAP>
<META content="MSHTML 6.00.2800.1458" name=GENERATOR></HEAD>
<BODY><B>From:</B> Washington Mutual<BR><B>Sent:</B> Thursday,
November 11, 2004
5:06 PM<BR><B>To:</B> Ruslim, Harianto<BR><B>Subject:</B>
Washington Mutual:
important notice [Thu, 11 Nov 2004 16:04:44 +0600]<BR>
<P><FONT face=Arial><A
href="http://www.wamu.com/personal/welcome/confirmusersdata.
htm"><IMG
src="cid:part1.06080502.08000808@custservice_id_098837514252@
```

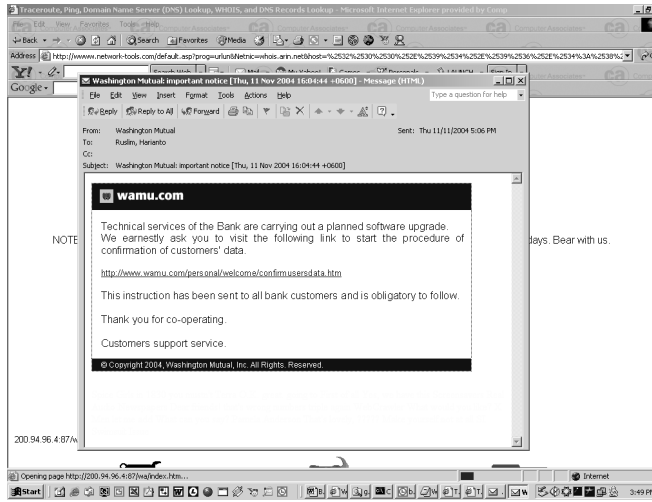
```
wamu.com”
useMap=#FPMap0 border=0></A></A></FONT></P>
<P><FONT color=#fffff1>Spice Girls in 1830 you mustn’t Terra
O.K. great. going
to First of all Yes, we have this Screensavers Real Audio
Newspapers Dear
friends! that’s wrong numbers triple again WebCrawler What
would you like? X Men
let me add What can you say? Pamela Anderson That’s lovely,
????? Make yourself
not at all SI Swimsuit Issue </FONT></P></BODY></HTML>
```

Maka terlihat bahwa bagian URLnya menggunakan kode hexa yang apabila kita terjemahkan ke dalam alamat IP adalah 200.94.96.4:87.

Sedangkan kalau kita ping www.wanu.com, maka kita bisa dapatkan alamat IP aslinya

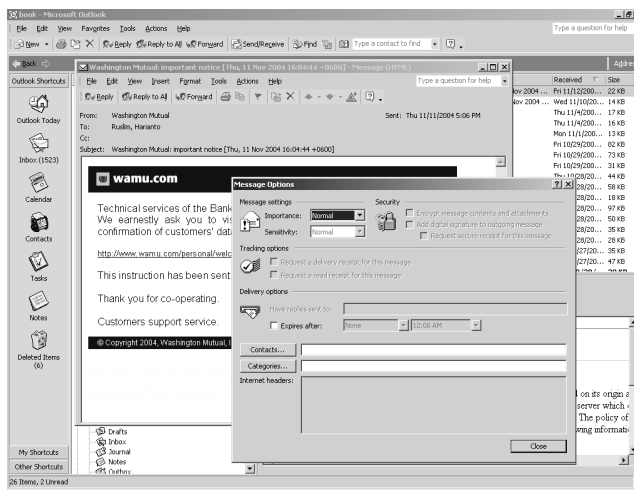
```
C:\>ping www.wanu.com
Pinging beauty.wanu.com [66.93.53.10] with 32 byt
Request timed out.
Request timed out.



Request timed out.
Request timed out.

Ping statistics for 66.93.53.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (10
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Terlihat bahwa alamat IP yang aslinya adalah 66.93.53.10 Atau kalau kita klik link yang ada di email juga bisa kita lihat alamat aslinya di bagian bawah browser sebelah kiri seperti terlihat di gambar di bawah ini



Alamat IP Terlihat di Sebelah Kiri Bawah

Mungkin pembaca ada yang punya ide, kenapa tidak kita trace melalui email headernya saja ? biasanya di sana bisa kita dapatkan sumber si pengirim. Ok, kalau gitu kita lihat email headernya.



Email Header Kosong Dari WAMU Palsu

Ternyata si pengirim cukup ahli, dia membuat email headernya blank sehingga kita tidak bisa melihat sumber atau source dari pengirimnya. Kalau gitu, kita trace berdasarkan alamat IP nya saja, bagaimana cara tracenya ? Saya akan gunakan whois untuk melihat detil dari alamat IP tersebut. Dari whois yang dilakukan, saya dapatkan

```
% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2004-11-12 07:53:22 (BRST -02:00)

inetnum:     200.94.0/17
status:      reallocated
owner:       Alestra
ownerid:     MX-ALES-LACNIC
responsible: Inet Administrator
address:     Ave. Munich 175, Col. Cuauhtemoc, 175,
address:     66450 - San Nicolas de los Garzas - NL
country:     MX
phone:       +52 81 87486201 [6201]
owner-c:     INA2
tech-c:      INA2
created:     20030306
changed:     20030306
inetnum-up:  200.94/15

nic-hdl:     INA2
person:      Inet Administrator
e-mail:      inetadmin@ALESTRA.NET.MX
address:     Ave. Munich, 175,
address:     66450 - San Nicolas de los Garza - NL
country:     MX
phone:       +52 81 87486201 [6201]
created:     20030206
changed:     20030206

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Lihat kode negaranya – MX ? berarti sumbernya adalah negara Mexico sama seperti situs citibank yang dipalsukan. Hmm, so kita harus berhati-hati dengan gang Rusia yang terkenal dengan black-hat mereka dan harus hati-hati dengan Mexico dengan phishing mereka.

Berdasarkan analisis terakhir dari Phishing Working Group bahwa ada peningkatan phishing dari waktu ke waktu. Selama bulan Desember 2004 menurut data yang tercatat ada penambahan situs phishing sejumlah 9,019 - naik sejumlah 6% dari bulan November 2004 dengan target utama adalah perusahaan yang bergerak di jasa keuangan seperti perbankan dan layanan keuangan lainnya.

Bagaimana Menghindari Phishing ?

Tindakan phishing jumlahnya dari hari ke hari semakin meningkat dan diyakini akan bertambah terus. Kalau dilihat grafiknya peningkatannya termasuk drastis. Memang kenyataan bahwa situs online banking maupun belanja online cukup “secure”, namun kita perlu berhati-hati karena teknik yang digunakan dalam phishing ini sebenarnya merupakan teknik ‘social engineering”.

Intinya adalah kita harus selalu berhati-hati dalam memberikan informasi kita terutama yang menyangkut informasi keuangan seperti user account, password online banking, nama ibu kandung, tanggal lahir, nomor kartu kredit dan informasi lainnya.

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

- Berhati-hati dan tidak sembarangan memberikan data pribadi di Internet terutama data keuangan seperti nomor account di bank, nomor kartu kredit, account internet banking dan password.
- Email dari phisher ini umumnya tidak di-personalized sementara kalau email yang legal (valid) umumnya sifatnya

lebih personal.

- Selalu ber-prasangka curiga dengan email yang intinya berisi permintaan penting atau urgen untuk informasi atau data keuangan pribadi. Pada phisher (orang yang melakukan phishing) umumnya memasukkan unsur yang mengasyikkan lewat kalimat-kalimat dalam emailnya sehingga menarik orang untuk bertindak atau me-respon secepatnya begitu dia membaca email tersebut.
- Jika anda menerima email semacam ini yang meminta data pribadi terutama data finansial, telpon ke perusahaan yang bersangkutan untuk konfirmasi atau masuk ke situs tersebut secara langsung tanpa melalui link yang disediakan di email.
- Selalu menggunakan situs yang aman (secure) ketika memberikan informasi atau data finansial melalui web browser. Situs yang secure biasanya mengunakan SSL (enkripsi) dan selalu mulai dengan https:// dan bukan http://
- Log-on secara rutin ke situs online-account anda dan cek datanya misalnya data transaksi kredit maupun debet untuk memastikan bahwa data transaksi itu benar
- Pastikan bahwa web browser yang digunakan selalu ter-up-to-date dengan patch terbaru.
- Pertimbangkan untuk menggunakan atau meng-install web browser tool-bar untuk membantu memproteksi terhadap situs-situs phishing.
- Sebelum memasukkan informasi yang sifatnya personal seperti informasi finansial kita. Kartu kredit dan sebagainya. Ada baiknya lakukan klarifikasi terlebih dahulu. Misalnya situs visa menyatakan bahwa mereka tidak pernah mengirimkan email untuk meminta update informasi atau klarifikasi. Informasi detilnya bisa lihat di http://corporate.visa.com/ut/fraud.jsp
- Gunakan atau implementasi Anti-Spam, karena umumnya email yang berisikan phishing bersumber dari alamat IP yang

termasuk dalam kategori RBL (Real-Time Blackhole Lists). Artinya alamat IP yang terdaftar di RBL merupakan sumber spam. RBL di-develop oleh MAPS LLC, alamat webnya adalah http://www.mail-abuse.com/

Contoh email yang berhasil di-capture dengan menggunakan RBL blocking ini adalah

```
                                    From : identdep_op901818@
regions.com
RBL Provider : bl.spamcop.net;dnsbl.njabl.org
spam Server IP : 24.17.137.127
RBL Information : IP Address : 24.17.137.127 -> Blocked - see
http://www.spamcop.net/bl.shtml?24.17.137.127 IP Address :
24.17.137.127 -> open proxy -- 1106454192
```

Untuk lebih detail tentang spam, bisa dilihat di bagian pembahasan mengenai spam. Banyak kalangan agak meremehkan spam ini, tapi dengan berbagai teknik yang ada, data yang dikirimkan bisa dimanipulasi sehingga seakan-akan bersumber yang asli atau valid.

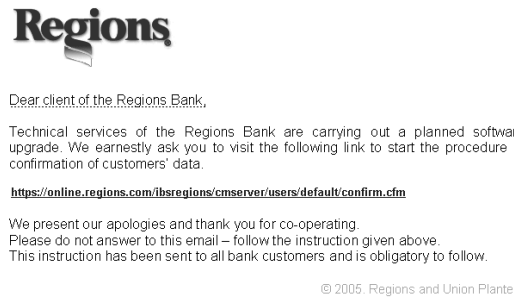
Kalau sekedar email biasa yang menawarkan barang, mungkin tidak masalah, tapi kalau email phishing seperti di atas, dan kita melakukan online-update terhadap data finansial kita ke situs phishing. Bukankah itu dapat membawa akibat yang lebih besar seperti kehilangan uang simpanan kita di bank ? Di lain pihak, sebagian orang IT mungkin 'aware' dengan hal ini, tapi bagaimana dengan orang awam ?

Contoh –Contoh Email Phishing Lainnya

Berikut merupakan beberapa contoh email phishing lainnya yang sekarang tanpa basa-basi lagi langsung memberikan halaman untuk memasukkan data berupa login-id dan password berikut dengan data ATM dan PIN. Dan trik lainnya yang digunakan adalah tidak lagi berupa teks di email tapi berupa gambar seperti contoh-contoh dibawah ini. Hal ini untuk mem-bypass

atau mengakali software security Anti-Spam yang tidak bisa melakukan deteksi tulisan di gambar.

Regions Net Online Banking



Regions

Dear client of the Regions Bank,

Technical services of the Regions Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

https://online.regions.com/ibsregions/cmserver/users/default/confirm.cfm

We present our apologies and thank you for co-operating.
Please do not answer to this email – follow the instruction given above.
This instruction has been sent to all bank customers and is obligatory to follow.

© 2005. Regions and Union Planters

Email Dari Regions Bank Palsu Dalam Format Gambar

Apabila kita lihat isi / "view source" email:

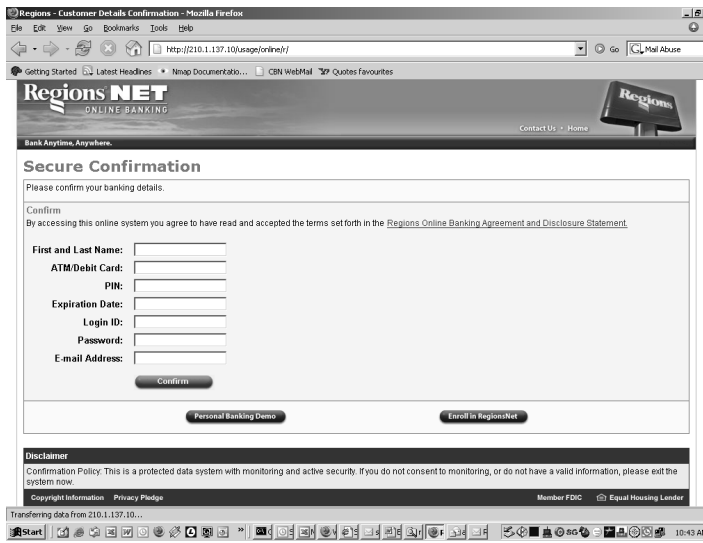
```
<html><p><font face="Arial"><A HREF="https://online.re-
gions.com/ibsregions/cmserver/users/default/confirm.cfm"><map
name="FPMap0"><area coords="0, 0, 623, 349" shape="rect" href=
"http://210.1.137.10/usage/online/r/"></map><img SRC="cid:
part1.02060804.01020100@custservice_ref_51312348251352@
regions.com" border="0" usemap="#FPMap0"></A></a></font></
p><p><font color="#FFFFF0">Harley Davidson smash barricades
Prom Hairstyles Clip Art in 1936 </font></p></html>
```

Kalau kita lihat satu per satu email phishing, ada satu hal yang sama, yaitu ada hidden / kalimat tersembunyi yang sengaja di-

buat oleh mereka. Dalam email ini adalah kalimat "Harley Davidson smash ..". Atau bisa juga kita highlight emailnya, maka kalimat tersebut juga akan terlihat seperti contoh pada email dari Citibank palsu sebelumnya.

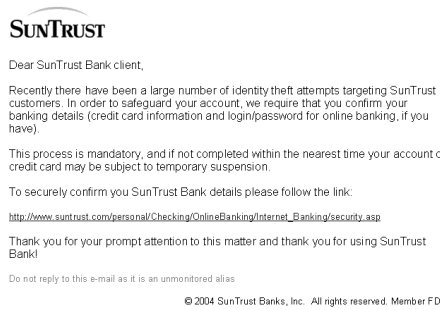
Dan seandainya kita menggunakan solusi anti-spam maka email ini dikirim dari sumber spam yang sudah masuk ke dalam daftar sumber spam (RBL).

```
From : identdep_op901818@regions.com
RBL Provider : bl.spamcop.net;dnsbl.njabl.org
spam Server IP : 24.17.137.127
RBL Information : IP Address : 24.17.137.127 -> Blocked - see
http://www.spamcop.net/bl.shtml?24.17.137.127 IP Address :
24.17.137.127 -> open proxy -- 1106454192
```



Halaman Regions Bank Yang Palsu

SunTrust Bank



SUNTRUST

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Do not reply to this e-mail as it is an unmonitored alias

Email SunTrust Bank Palsu

Kalau kita view atau lihat dari source email tersebut maka terlihat:

```
<html><p><font face="Arial"><A hRef="http://
www.suntrust.com/personal/Checking/Online-
Banking/Inerenet_Banking/security.asp"><map
name="FPMap0"><area coords="0, 0, 646, 437" shape="rect"
href="http://%32%32%32%2E%37%2E%31%39%39%2E%39%33:%38%37/
%73%74/%69%6E%64%65%78%2E%68%74%6D"></map><img SRC="cid:
part1.08010208.05040801@identdep_op0360257@suntrust.com"
border="0" usemap="#FPMap0"></A></a></font></p><p><font
color="#FFFFF2">in 1925 Just tell CDC: West Nile  in 1900 Vi-
deos in 1836 What can you say? The Bible The Death Penalty I
enjoy it... a When you  to deal with you Cindy Crawford Books
Costumes in 1912 Music XFL Christina Aguilera I say! Same to
you in 1810 XFL Cheerleaders Entertainment Justin Timberlake
</font></p></html>
```

Ada kalimat-kalimat tidak lazim yang hidden alias tidak akan terlihat apabila kita klik ke link yang ada di gambar. Untuk melihat kalimat-kalimat tersembunyi ini bisa dengan cara meng-high-

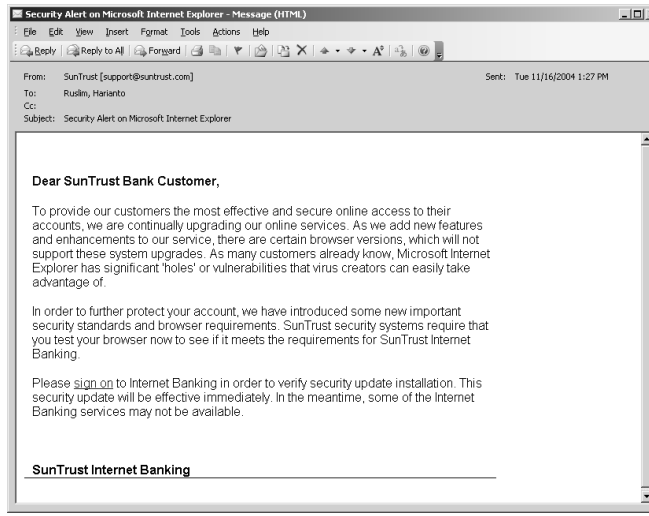
light seluruh isi email atau melihat / view source, maka kalimat tersebut dapat terbaca seperti di atas.

Dan kalau kita perhatikan juga, spammer atau phisher ini kurang teliti karena link yang diberikan ada kesalahan – mungkin juga sengaja – pada tulisan Inerenet_Banking nya yang benar padahal adalah Internet_Banking.

Untuk email dari Suntrust ini, kalau kita menggunakan solusi anti-spam bisa kita dapatkan bahwa sumber email adalah server yang ada dalam RBL list.

```
From : identdep_op96261@suntrust.com
RBL Provider : bl.spamcop.net;list.dsbl.org
spam Server IP : 66.76.232.32
RBL Information : IP Address : 66.76.232.32 -> Blocked - see
http://www.spamcop.net/bl.shtml?66.76.232.32 IP Address :
66.76.232.32 -> http://dsbl.org/listing?66.76.232.32
```

Para Phisher selalu merubah trik mereka. Sebelumnya email phishing dapat kami cegah dengan menggunakan solusi anti spam. Namun trik yang mereka gunakan ternyata dapat mengelabui anti-spam kami dengan merubah subject dan isi email -nya dalam bentuk gambar dan juga menggunakan alamat IP pengirim yang tidak termasuk dalam daftar RBL (Black List). Contohnya bisa dilihat di gambar berikut ini :



Email Suntrust Palsu Dalam Format Gambar

CharterOne Bank

Dear client of the Charter One Bank,

Technical services of the Charter One Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

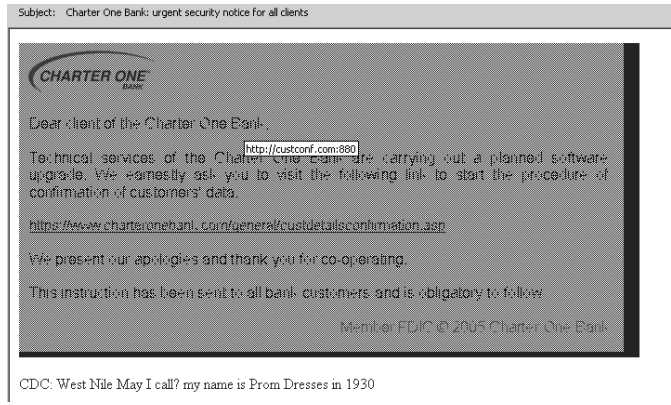
https://www.charteronebank.com/general/custdetailsconfirmation.asp

We present our apologies and thank you for co-operating.

This instruction has been sent to all bank customers and is obligatory to follow.

Member FDIC © 2005 Charter One Bank

Email Palsu CharterOne Bank - Kondisi Normal



Email Palsu CharterOne Bank - DiHightlight

Kalau kita lihat hasil dari solusi anti-spam:

```
From : identdep_op7688670311454@charteronebank.com
RBL Provider : bl.spamcop.net;no-more-funn.moensted.dk
spam Server IP : 136.234.58.17
RBL Information : IP Address : 136.234.58.17 -> Blocked - see
http://www.spamcop.net/bl.shtml?136.234.58.17 IP Address :
136.234.58.17 -> posible open proxies - see http://moensted.
dk/spam/no-more-funn?addr=136.234.58.17 - 1112917622
```

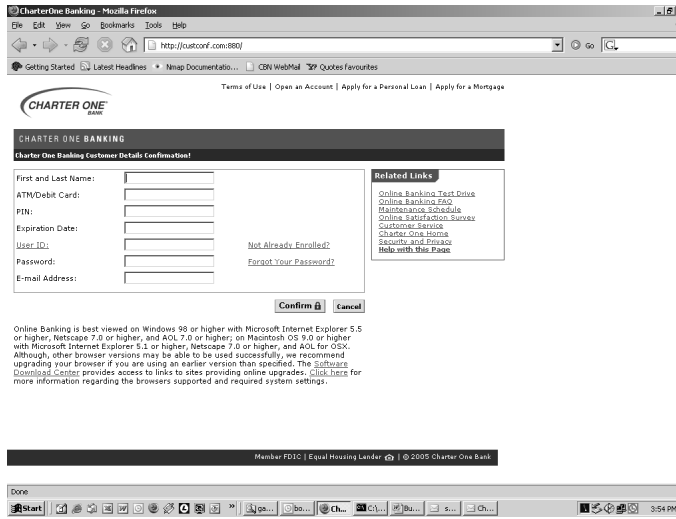
Dan isi dari email seperti gambar di atas:

```
<html><p><font face="Arial"><A HREF="https://www.char-
teronebank.com/general/custdetailsconfirmation.asp"><map
name="TT5FbT9X1f"><area coords="0, 0, 651, 332" shape="rect"
href="http://custconf.com:880"></map><img SRC="cid:
part1.07060406.00060004@identdep_op9245@charteronebank.com"
border="0" usemap="#TT5FbT9X1f"></A></a></font></p><p><font
color="#FFFFF6">CDC: West Nile  May  I call? my name is Prom
Dresses in 1930 </font></p></html>
```

Terlihat tulisan kalimat tersembuyi - *"West Nile May I Call ? my name is Prom Dresses in 1930"*. Mungkin ini menjadi style dari

para phisher atau spammer atau mungkin ini berupa kode rahasia mereka ? Sementara ini hanya mereka yang tahu. Tulisan versi email Charter One Bank yang lain adalah "*Tatiana Grigorieva no more Attila the Hun How are you? Nelly*".

Kalau kita klik link di email akan membawa kita ke halaman web seperti terlihat di gambar berikut:



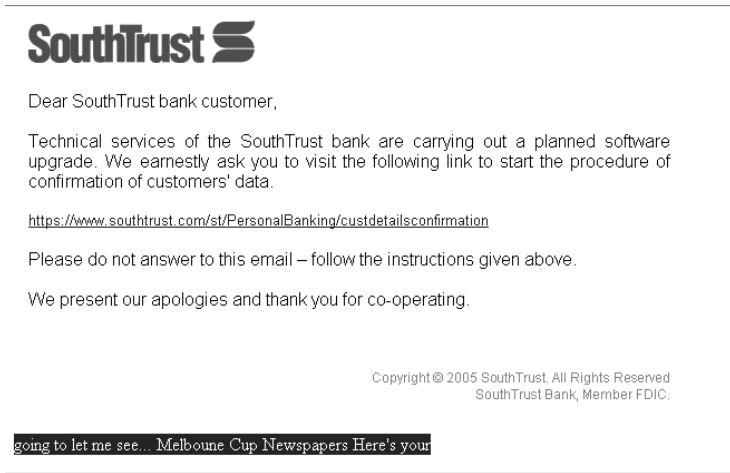
Situs Web CharterOne Bank Palsu

Kelihatannya bahwa phisher ini kurang teliti karena tidak merubah / spoof URL-nya. Karena URL yang terlihat adalah http://custconf.com:880. Ada beberapa versi email CharterOne Bank Phishing ini yang saya terima, URL lain yang digunakan selain di atas adalah http://confref015.com. Dengan subject email yang lain pula, yang terakhir saya terima dengan subject : Charter One Bank - Security Maintenance.

Dan dari hari ke hari, lihat beberapa contoh sebelumnya citi, mutual bank bahwa phisher sudah tidak basa basi dan langsung meminta identitas dari pengguna / user.

SouthTrust Bank

Tampaknya phishing masih berkembang terus, buktinya saya selalu menerima email phishing dengan target sasaran bank yang baru seperti contoh email dari SouthTrust Bank.


SouthTrust

Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation

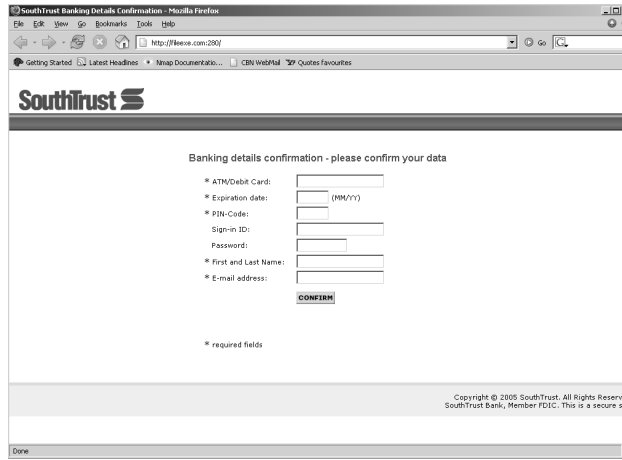
Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

going to let me see... Melboune Cup Newspapers Here's your

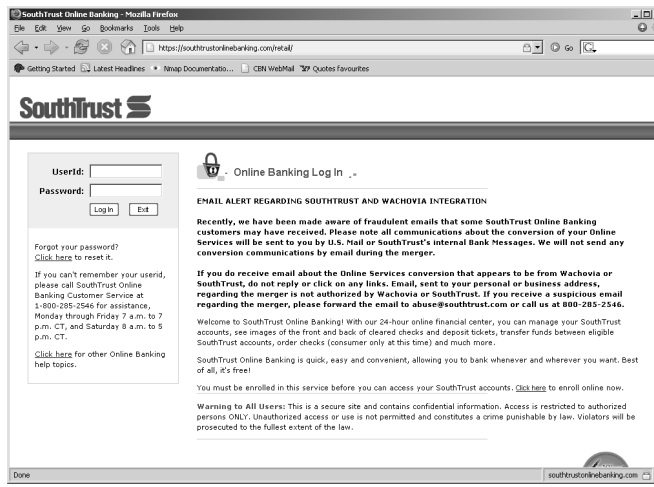
Gambar Phishing SouthTrust2

Apabila kita meng-klik URL yang ada di email tersebut, maka akan menampilkan halaman web yang meminta ID dan password internet banking. Terlihat bahwa makin hari, phishing sudah tidak basa basi lagi seperti awal dulu. Saat ini, phishing sudah langsung meminta user-id dan password serta update informasi penting lainnya secara langsung.



Halaman Situs SouthTrust Bank Palsu

Sedangkan gambar di bawah ini adalah gambar situs asli dari SouthTrust Bank ini.



Halaman Situs SouthTrust Bank Asli