SPAMGATE ATTACK
Penyerangan Besar

Oktober 2005, milist (Mailing List) NeoTek digemparkan dengan masuknya postingan yang aneh bin ajaib, kita kasih sebutan SpamGate I (penggunaan I karena ada II dan III). Aneh karena postingan tersebut berisi dengan teks yang sangat panjang dan tidak dapat dimengerti. Ajaib karena hampir seluruh postingan tersebut tidak hadir dengan jumlah 1 atau 2 atau 3, tetapi mencapai jumlah 100 bahkan ratusan.

UNTUK DAPAT MELAKUKAN POSTING PESAN DI MILIS NeoTek hanya dapat dilakukan oleh anggota yang terdaftar, dan benar postingan tersebut berasal dari email-email yang terdaftar sebagai anggota. Aneh bin Ajaib, pemilik email tidak pernah merasa mem-posting pesan tersebut.

Adapun potongan kecil isi postingan tersebut seperti yang diperlihatkan di bawah ini:

```
From:
"\"\\\"luPxCvKFRw70lP4bYGVZGLduDVnILEGnC6O4jsz4taPP7QqPHzl
a36gdQ2sjHVdCFUYhCqdoaZib7DWcqn\\\"\""
<melvin_ics@yahoo.com>
Date: Sat Oct 29, 2005  12:05 pm
Subject:
qpMmrChXwT7x4k6Uou8gqRDJoEac6XCZKkVwE9Ct7wJqPwkkeMF3
p9YMvWNOAzM1n8ONAFBpCbmwXwaxR

M3D%3EB%5D%2C%3DZ%3D%28%2A%29HP3E%22U%400Z%2A
%29CUU%2E%26G%29K%5C%5C%3BNH%27%5EU\
%2B%3F%5E%24Q%5D%22B%20WMR%283%3C2LGNR%2D%0A
MFZ%20RTG2%29G%5E%3BUM%3B%26K%3CERV0\
HR2%2B%3A%27%25G%2B%25%3DZ5D%230%3FNB%40F%3C%
2CK%20%3AA%20MS%3D486HJ%3CC%24%0AMF\

----------cut----------
```

Moderator milist NeoTek mengambil tindakan dengan melakukan moderasi posting, sehingga postingan yang masuk harus mendapat approve dari moderator. Namun, moderator milist NeoTek yang saat itu menangani kasus tersebut kecele (terkecoh). Terkecoh karena ada postingan dengan subject email yang tidak memiliki keanehan tetapi isi postingan-nya yang aneh, dan sempat beberapa postingan Aneh bin Ajaib telah di approve.

Masalah makin runyam karena dari ratusan postingan Aneh bin Ajaib juga terdapat postingan yang asli tidak ada keanehan a.k.a normal. Agar tidak membuat anggota menjadi bingung, moderator ekstra tenaga dan waktu untuk memeriksa satu persatu postingan yang masuk. Semoga Tuhan memberikan kesabaran dan berkah bagi moderator yang sabar ini.

Kesabaran lainnya (tindakan kedua) yang dilakukan oleh moderator adalah mengumpulkan informasi alamat email yang telah melakukan postingan aneh sekaligus merecord informasi header email.

Hujan Protes

Sejak kejadian postingan Aneh bin Ajaib, moderator menuai protes dan pertanyaan. Moderator yang sabar seperti kena sunat kembali (padahal udah disunat waktu kelas 4 SD), tetapi moderator yang sabar untungnya tetap sabar.

Moderator menyampaikan permintaan maaf (tindakan ketiga) kepada anggota milist atas kejadian tersebut dan moderator meminta kepada anggota yang emailnya terdaftar sebagai pengirim postingan untuk check and recheck terhadap kondisi komputer yang digunakan, menjaga kemungkinan malicious program yang menyusup ketika berselancar (apalagi berselancar di situs-situs porno) di dunia internet yang cukup kejam.

Dari pengamatan moderator terhadap postingan Aneh bin Ajaib yang masuk, terdapat kesamaan yaitu sebagai berikut:

1. Pada header mail

```
Return-Path: <apache@ns2.altervista.org>
X-Sender: apache@ns2.altervista.org
Received: from unknown (HELO ns2.altervista.org) (207.44.184.37)
Received: from ns2.altervista.org (localhost.localdomain [127.0.0.1])
    by ns2.altervista.org (8.12.8/8.12.8) with ESMTP id
j9TG5mQd021332
Received: (from apache@localhost)
    by ns2.altervista.org (8.12.8/8.12.8/Submit) id
j9TG5mSB021329;
Message-Id: <200510291605.j9TG5mSB021329@ns2.altervista.org>
X-WEBSITE: hackerminds.altervista.org
X-Originating-IP: 207.44.184.37
```

Postingan dilakukan menggunakan script melalui hosting yang berada di luar negeri. Jadi pelaku postingan Aneh bin Ajaib dapat dipastikan 1 orang dan memanfaatkan informasi alamat email yang terdaftar di milist NeoTek untuk memasukkan postingan-nya. Lah..., apa bisa begitu? Yup..., sangat jelas sekali bisa karena identifikasi keanggotaan hanya berdasarkan alamat email. Tidak ada settingan khusus yang dimiliki oleh Yahoo!Groups mengenai identifikasi keanggotaan milist.

2. Salam Penutup Pesan

```
Servizio mail a cura di http://www.AlterVista.org
```

Salam yang manis bukan...

SpamGate II

Serangan postingan Aneh bin Ajaib sempat usai. Perkiraan moderator saat itu, "Mungkin pelaku capek ya" dan settingan milist dikembalikan ke sedia kala.

Tetapi suasana damai ternyata tidak berlangsung lama, February 2006, kembali aksi spam di milis NeoTek terjadi dengan bentuk yang masih sama. Sumber serangan juga masih sama. Moderator kembali kerja keras dan siap-siap dengan tagihan internet yang membengkak karena setiap hari berjaga-jaga.

SpamGate III

Maret 2006, kembali gempuran pelaku spam memenuhi

ruang milist NeoTek. Bagaimana dengan moderator? Alhamdulillah moderator masih sangat sabar. Tapi ada kabar gembira dari Serangan Maret (tidak pakai 1). Diserang kok gembira? Tentu saja gembira karena kebuntuan untuk melacak pelaku akhirnya terpecahkan. Memang Tuhan menyayangi umatnya yang sabar.

Dari header email spamgate yang menghampiri milist NeoTek, terjadi perubahan informasi. Informasinya adalah sebagai berikut:

```
Received: from unknown (HELO 5c47b8206f6e464)
(222.124.226.68)
Received: from localhost[127.0.0.1] (helo=5c47b8206f6e464) by
 localhost[127.0.0.1] with esmtp (QK SMTP Server 3);Tue, 11 Apr
2006 16:50:42
 -0700
Message-ID:
<1774120.1144799442096.JavaMail.SYSTEM@5c47b8206f6e464>
Mime-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-Mailer: ColdFusion MX Application Server
X-Originating-IP: 222.124.226.68
```

Moderator fokus kepada alamat IP dan melakukan whois terhadap alamat IP tersebut dengan memanfaatkan fasilitas yang diberikan oleh www.dnsstuff.com dan didapatkan informasi sebagai berikut:

```
inetnum:      222.124.224.0 - 222.124.239.255
netname:       TLKM_D5_BB_SPEEDY
country:      ID
descr:        PT Telkom Divisi Regional V Jawa Timur
descr:        TELECOMMUNICATIONS/COMMUNICATIONS
descr:        JL KAPUAS 51
descr:        SURABAYA
admin-c:       BP181-AP
tech-c:       SY737-AP

----------------------cut---------------------------------
```

Ternyata IP 222.124.226.68 merupakan IP SPEEDY Telkom yang dikelola oleh PT Telkom Divisi Regional V, Surabaya, Jawa Timur. Tingtong...

Bukan Hanya Milist NeoTek

Tadi ceritanya berkutat di milist NeoTek, ternyata ada cerita lain yang ternyata mengalami nasib yang sama seperti milist NeoTek. Pelaku spamgate tidak hanya menyerang milist NeoTek, ada beberapa milist besar lainnya yang mendapat serangan yang sama, antara lainnya yaitu milist Jasakom, milist IndoCrack, dan milist TpoTC. Apa hanya milist tersebut? Tentu saja tidak, masih ada milist lainnya.

Mengindikasikan Pelaku

Dari hasil diskusi sesama moderator dimana milist yang dikelola mendapat serangan spamgate, muncul 1 nama. Pemunculan 1 nama tersebut tidak asal pilih, mulai dari pencocokan sana-sini, pencocokan silang, dan lain sebagainya. Tetapi tetap saja belum bisa dipastikan, untunglah saudara Aris Wendy (moderator milist TPoTC) memiliki kenalan dengan pihak Telkom Divre V Surabaya, melakukan investigasi dan mendapat informasi penting.

Berikut cuplikan informasi yang didapat dari saudara Aris Wendy (dapat juga anda temukan cuplikan tersebut di situs www.bukuweb.com)

Walah.....masih surabaya toh. Alhamdulillah masih mempunyai hubungan baik dengan TELKOM disini. Jadi ane tinggal minta tolong ke beberapa rekan di DIVRE V untuk mengetahui identitas Mr X. Sambil menunggu hasil investigasi pihak TELKOM saya berusaha memprovokasi Mr X yang sudah dicurigai beberapa temen dengan jalan memasang status pada YM saya "Don't worry ane kejar terus pelakunya". Setelah beberapa jam hasil investigasi terjawab sudah, bahwa Mr X berdomisili di daerah Ketintang Surabaya dengan nomer telpon (031) 829xxxx. Selain itu pihak telkom juga memberikan statement koneksi dengan menggunakan telpon tersebut telah berganti IP pada tanggal 12 April 2006 jam 10 pagi. Sekali lagi, jebakan sudah berjalan. Rupanya Mr X sudah mereboot Speedy nya agar IP nya bisa berubah.Tetapi too late.....

Informasi penting yang dimaksudkan adalah IP 222.124.226.68 digunakan oleh nomer telpon (031)829xxx yang beralamat di jalan Ketintang.

Informasi tersebut klop dan praduga hasil diskusi melahirkan tersangka pelaku SpamGate yang telah membuat gusar saudara S'TO (moderator milis Jasakom).

Tindakan untuk Pelaku

Tindakan pertama yang dilakukan adalah melakukan teguran kepada pelaku dan melaporkan kepada pihak Telkom yang terkait untuk menindak lanjuti kasus ini. Semoga pihak Telkom cepat menyelesaikannya, itu harapannya karena jika pihak Telkom tidak menindak lanjuti dengan tegas atas pengaduan tersebut, kemungkinan terburuk lah yang mungkin akan hadir. Tetapi segenap pihak percaya Telkom akan serius menidak lanjuti masalah ini karena yang menjadi korban SpamGate tidak sedikit terdapat nama-nama besar di dunia IT Indonesia yang dihantam oleh pelaku SpamGate ini, salah satunya Onno W Purbo (Pakar Telematika Indonesia) yang informasi alamat email digunakan untuk memasukkan postingan Aneh bin Ajaib. Dan yang Aneh bin Ajaib lagi, setelah kasus sedikit diangkat ke permukaan, kontan abisss... SpamGate ikut hilang menelan sendok.

Pelanggaran Serius

Apa yang dilakukan oleh pelaku SpamGate ini sudah termasuk pelanggaran hukum yang sangat serius. Mengapa begitu? Penggunaan identitas orang lain untuk melancarkan SpamGate yang mana tujuannya adalah jelas-jelas menyerang orang lain.

Bagaimana ya rasanya kalo alamat surat (bukan email) anda dipakai orang lain untuk mengirim surat yang isinya aneh-aneh (apalagi kalau isinya berupa surat ancaman, penghinaan, tuduhan, dan lain-lain) ke orang lain? Fitnah telah terjadi, dan agama mengatakan "Fitnah itu lebih kejam dari pembunuhan".

Dampak negatif yang paling dekat diakibatkan serangan SpamGate adalah pencemaran nama baik seseorang (inilah yang jelas-jelas telah terjadi) dan juga seperti narasi singkat di atas.

Dampak negatif lainnya adalah kerugian waktu dan bandwith yang harus ditanggung oleh anggota milist yang mendapat serangan SpamGate ini harus ekstra untuk membersihkan inbox email mereka.

Siapakah Pelaku dari SpamGate

Pelaku dikenal dengan si010010 a.k.a Udin, yang mengusung komunitas Sarang Tikus (www.sarangtikus.or.id). Dari informasi yang beredar, pelaku dikenal memiliki perilaku yang tidak baik, aneh seaneh bin ajaibnya SpamGate yang telah dilakukannya. Dan yang lebih aneh lagi, pelaku tetap menolak atas apa yang telah lakukannya. Terlepas dari anehnya tersebut, kemampuan social engineering si010010 lumayan. Memainkan peran sebagai wanita un-

tuk memikat korbannya. Hanya saja masih sering ditemui ceceran jejak-jejaknya.

Hati-hati!!!

Pelaku sampai saat ini masih terhitung anggota milist NeoTek, baru-baru ini pelaku menawarkan "Buku Gratis" yang berjudul "Seni Internet Hacking Recoded" terbitan Jasakom. Bagi yang berminat dipersilakan untuk mengunjungi situsnya.

Mengapa sub ini diberi title hati-hati? Jawabnya "Kemarin nyepam sekarang bagi-bagi buku". Selain itu ditemui beberapa kejanggalan yang harus dperhatikan.

Aktifitas Scammer

Pada saat menawarkan buku gratis, pelaku menggunakan nama MrKey a.k.a Hamdanah.

Berikut cuplikan emailnya:

From: "MrKey" <banjarmasin@gmail.com>
Date: Thu Apr 27, 2006 11:09am
Subject: OOT - FREE ORIGINAL BOOK: Seni Internet Hacking Recoded si010010

Salam,

Maaf pak moderator, sekedar memberi tahu, mudah-mudahan bermanfaat=20 untuk anggota milist yang ada.

FREE ORIGINAL BOOK: Seni Internet Hacking Recoded
http://www.sarangtikus.or.id

<:3)~

MrKey
(Hamdanah)

SARANGTIKUS.COM
Komunitas Teknologi Informasi Bawah Tanah Indonesia

Jika merujuk pada url yang diberikan, ditemui MrKey a.k.a A. Yuliani. Aneh bukan?

Selain itu, penawaran buku gratis harus mengikuti langkah pertama, otomatis akan ada langkah kedua, ketiga, atau bahkan keseratus, atau sudah tidak ada langkah lain (skak mat).

Dari shoutbox yang terdapat halaman situs itu juga, ternyata telah ada yang melakukan pedaftaran:

Asrofi: mau terima buku itu..... bagaimana langkah selanjutnya bang??? ditunggu... aku dah bikin email tuh

Berapa banyak buku yang mereka miliki? Penulis mencoba memberitahukan seseorang mengenai pembagian buku gratis, tetapi apa jawabannya:

rr** **r**: boleh gw bilang website ini scammer?
rr** **r**: Free email yang mereka miliki itu bukan dr server mereka
rr** **r**: gw rasa ada award or something yang mereka dapatkan dr banyaknya user yang ter-register
rr** **r**: dan mereka sekarang menuliskan
rr** **r**: Free Original Books milik S`to
rr** **r**: dan bukan copy melainkan original
rr** **r**: tapi dengan syarat 1
rr** **r**: daftar ke email mereka
rr** **r**: lalu nothing happened and..
rr** **r**: mereka suruh kita tunggu langkah berikutnya
rr** **r**: hmm
rr** **r**: buku itu fake and gak pernah ada eksistensinya gw bilang
rr** **r**: gak
rr** **r**: kalau gw lihat lg
rr** **r**: buku itu gak akan pernah ada
rr** **r**: memberikan 1 langkah dan disuruh nunggu langkah berikutnya itu udah 1 bentuk deception
rr** **r**: penipuan
rr** **r**: dimana bisa saja nanti dia akan memberikan langkah ke 2
rr** **r**: register ke forum mereka
rr** **r**: langkah ke 3
rr** **r**: register ke mailing list mereka
rr** **r**: hasilnya?
rr** **r**: mereka memenangkan users
rr** **r**: tanpa mengeluarkan buku

Aktifitas Phising

Mengumpulkan informasi pendaftaran yang dilakukan oleh orang-orang yang mendaftar di media yang telah dirancang sebelumnya, bukanlah tindakan baru. Seperti melakukan tindakan phising.

Kesalahan yang dimanfaatkan adalah kecendrungan orang yang menggunakan 1 password untuk berbagai account yang dimiliki.

Indikasi tidak hanya pada pendaftaran email tetapi juga pada forum. Jika kita menelusuri situs tersebut lebih dalam, makin banyak ditemui kejanggalan, terutama dengan forum. Terdapat pendaftaran anggota forum tetapi yang bukan anggota forum selain dapat membaca isi forum, juga dapat melakukan posting pesan ke dalam forum.

Jadi point dari pendaftaran dapat saja merupakan phising.