STATISTIK INTERNET ABUSE INDONESIA 2011

LAPORAN DWI BULAN-II TAHUN 2011

Bulan MARET dan APRIL

Edisi: I

15 Mei 2011

Disusun oleh: AHMAD KHALIL ALKAZIMY, ST

DIDUKUNG OLEH:

DAFTAR ISI

I. PENGANTAR

Keamanan berinternet merupakan salah satu faktor terpenting dalam menjalankan usaha maupun bisnis.

Selain bertujuan memberikan deskripsi kejadian Abuse di Indonesia, laporan ini juga dapat dijadikan contoh agar Indonesia mempunyai data primer Abuse.

Setiap lembaga sangatlah penting menindaklanjuti berbagai keluhan/pengaduan yang diterimanya terkait internet *abuse*. Sebagai analogi: bila kita berkeinginan agar setiap keluhan/pengaduan dari negara kita direspon dengan baik oleh negara lain, tentunya kita juga harus memperlakukan hal yang sama terhadap laporan yang masuk.

Keluhan/pengaduan yang terjadi menunjukkan betapa lemahnya sistem yang dibangun sehingga membutuhkan perbaikan kedepannya. Kita tentu tidak ingin, situs web yang kita bangun ditumpangi oleh *Malware* ataupun *Phishing* yang terkait dengan *Fraud* akibat lemahnya sistem yang kita bangun.

Tidak hanya sebatas menindaklanjuti keluhan/pengaduan, tetapi kita juga harus bisa lebih pro-aktif melaporkannya bila menjadi korban dari prilaku jahat di internet.

Dalam penelitian ini, kami berhasil mengambil data dari tiga puluh sembilan (39) responden yang terdiri dari: **DITJEN AHU-KEMKUMHAM**, **KEMKOMINFO**, **ID-CERT**, **PANDI**, **DETIK.NET, 5 Operator** Telekomunikasi, **7 NAP** dan **22 ISP**.

Terhitung mulai 23 Pebruari 2011 ini juga, ID-CERT mulai mengaktifkan email cert@cert.or.id sebagai alternatif tambahan penerimaan pengaduan internet abuse selain abuse@cert.or.id.

Selain itu, yang menjadi perhatian kami pada Dwibulan-II ini adalah meningkat secara drastisnya ***Network Incident*** yang dalam dua bulan terakhir menduduki peringkat pertama untuk pertama kalinya sejak tahun 2010.

Data dalam laporan ini belum bersifat final, karena masih ada 3 responden lama yang belum menyerahkan data dan 3 responden baru yang juga belum menyerahkan datanya.

Penelitian ini juga mendapatkan dukungan sponsor dari PANDI dan KEMKOMINFO.

II. Metodologi penelitian

Metodologi yang digunakan dalam penelitian ini adalah:

A. Pengambilan data dari sejumlah responden.

B. Metode analisis berdasarkan:

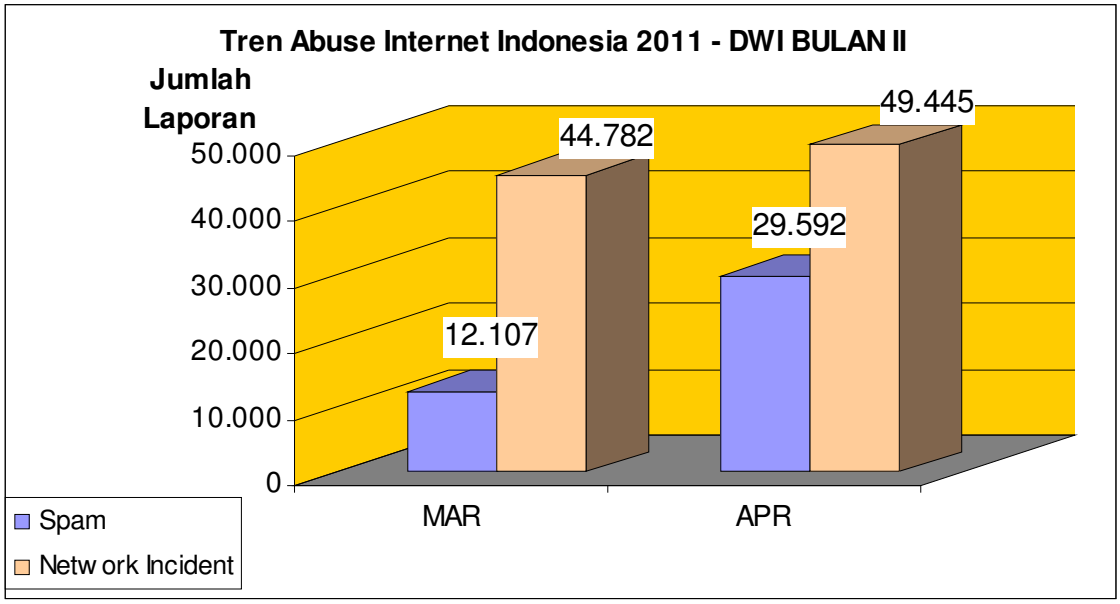
B.1. Tembusan laporan yang masuk via email akun abuse ISP/ Operator Telekomunikasi/lembaga non-ISP.

B.2. Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi yang dimaksud adalah: data-data yang telah dihitung dan dikategoriasi oleh responden tersebut.

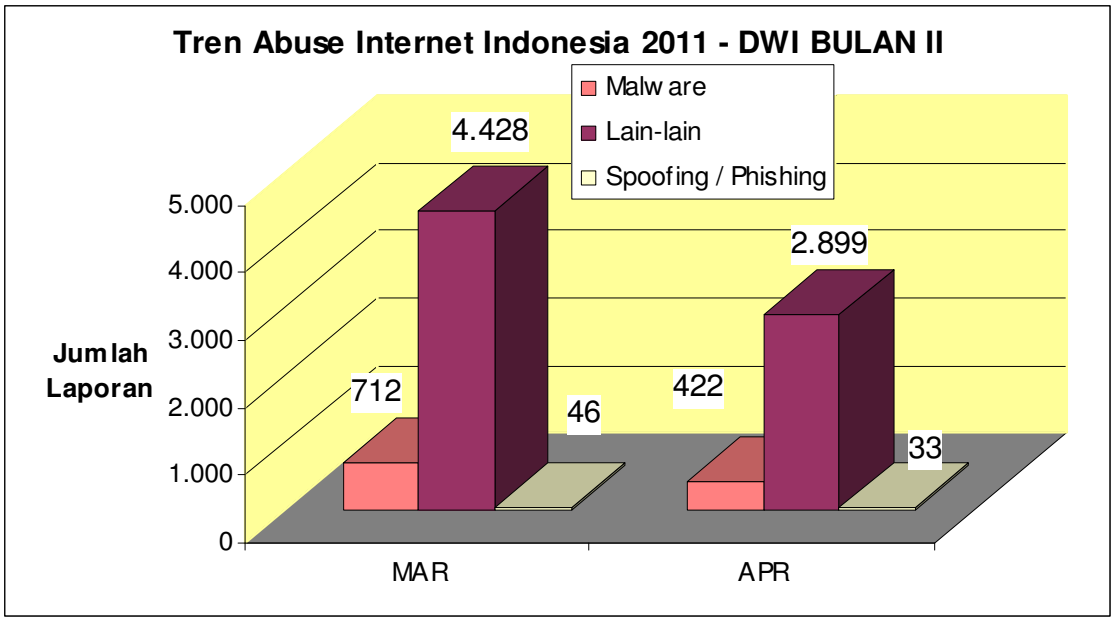
C. Dari laporan tersebut, kami melakukan pengkategorian laporan sebagai berikut:

C.1. Spam	keluhan/pengaduan email spam dari luar negeri terhadap network di Indonesia.
C.2. Spam Komplain	Keluhan/pengaduan email spam dari dalam negeri terhadap network di Indonesia dan luar negri.
C.3. Respon	Respon yang diberikan semua pihak terhadap laporan yang masuk.
C.4. Network Incident	Aktifitas yang dilakukan terhadap network milik orang lain serta segala aktifitas terkait dengan penyalahgunaan network.
C.5. Fraud	**Laporan kepada penegak hukum/instansi terkait yang mengakibatkan kerugian finansial**.
C.6. Spoofing/Phishing	Pemalsuan e-mail dan situs untuk menipu pengguna.
C.7. Malware	Sebuah program komputer yang dibuat dengan maksud jahat.
C.8. Lain-lain	Laporan penyalahgunaan yang diterima selain dari kategori yang ada diatas.

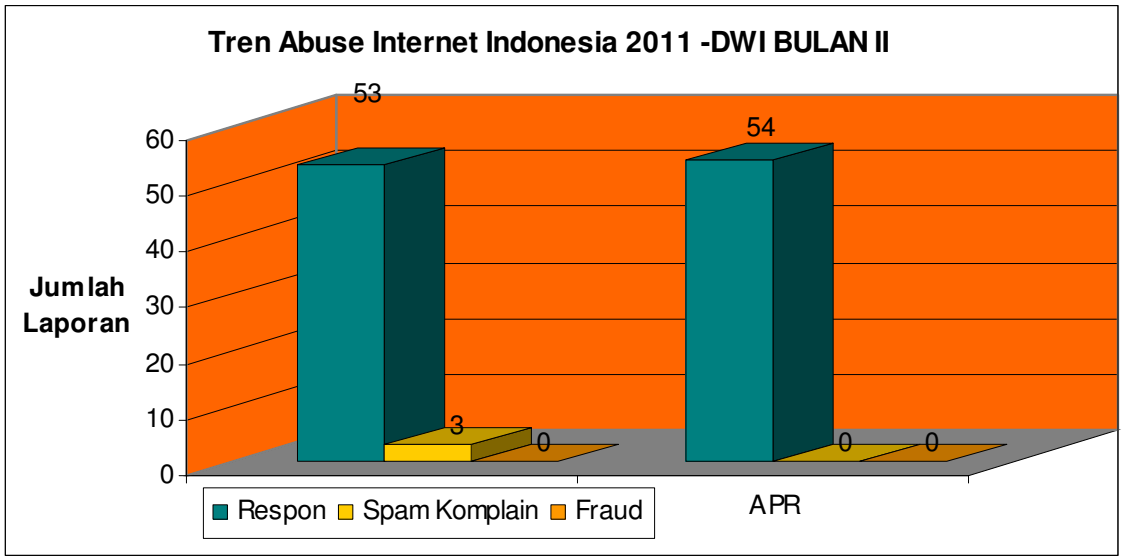
III. STATISTIK MARET – APRIL



GRAFIK-I: *SPAM* dan *NETWORK INCIDENT* – Dwi Bulan II

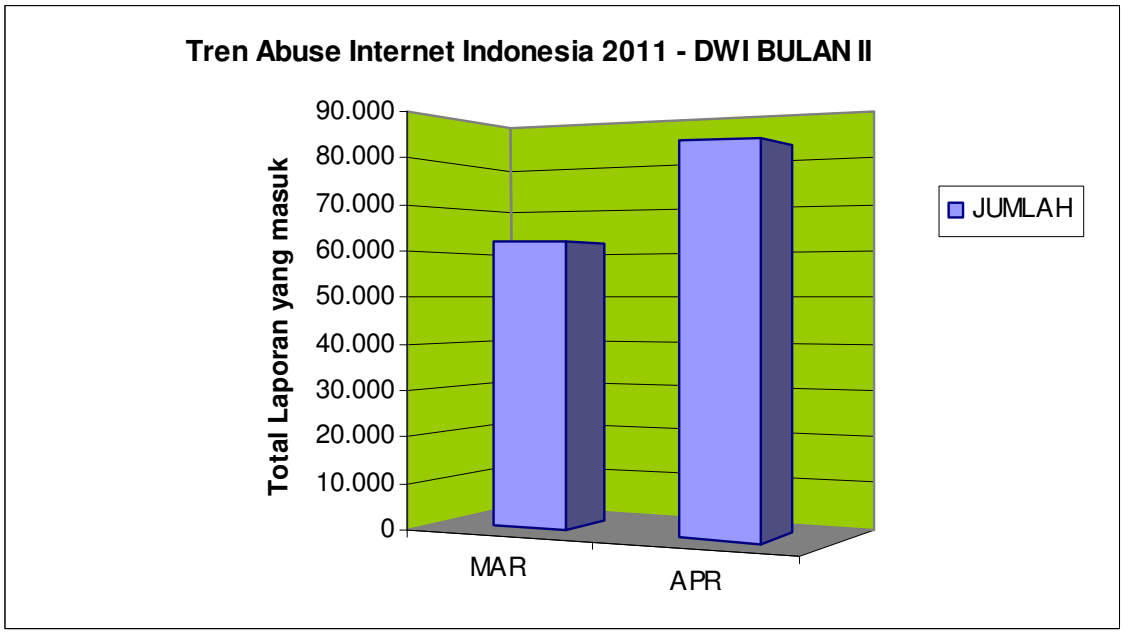


GRAFIK-II: Kategori MALWARE, Intellectual Propterty Rights/IPR (Lain-Lain) dan SPOOFING/PHISHING, Dwi Bulan - II



GRAFIK-III: Kategori RESPON, FRAUD dan SPAM KOMPLAIN, Dwi Bulan - II

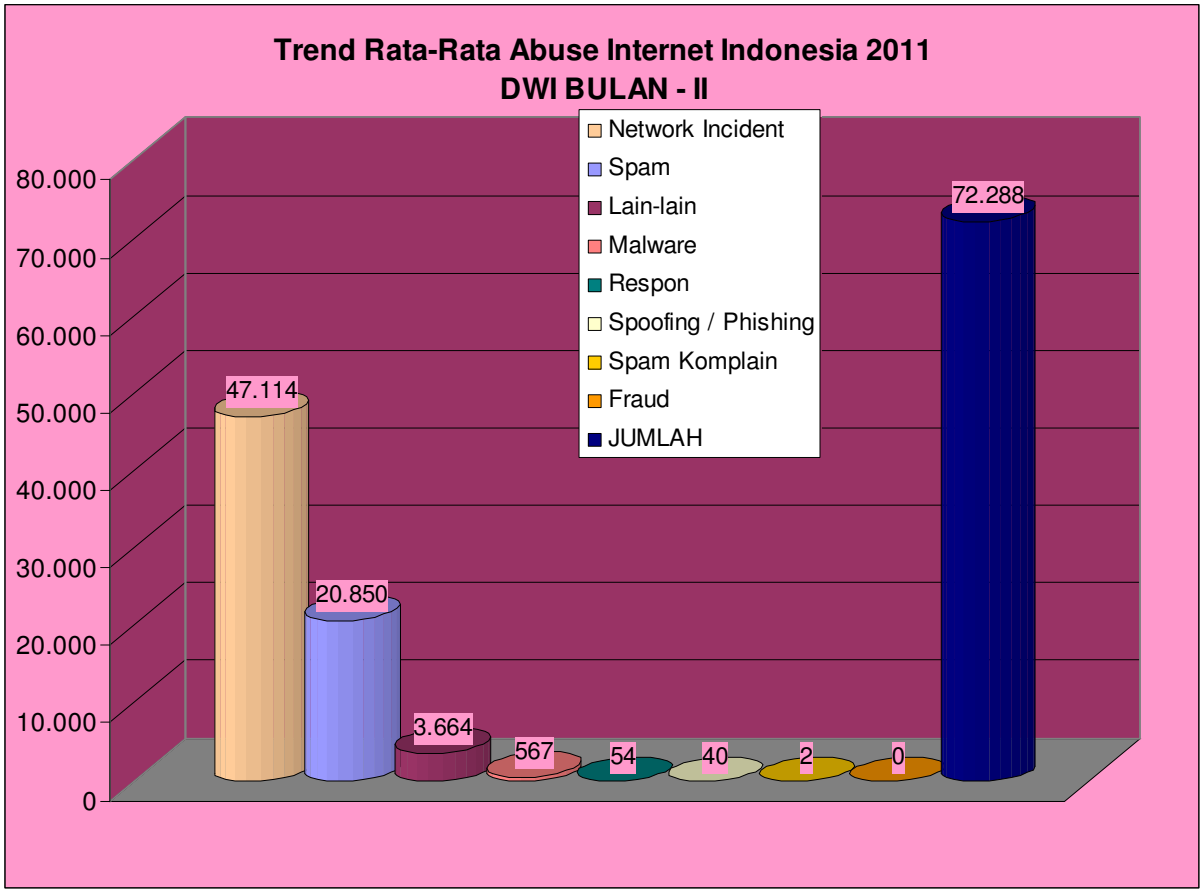
Tren rata-rata per bulannya secara total mencapai 72.288 laporan keluhan/pengaduan yang masuk.



GRAFIK-IV: JUMLAH LAPORAN YANG MASUK PADA Dwi Bulan-II

IV. URAIAN

Secara umum pada Dwi Bulan – II ini, terdapat informasi yang cukup beragam dari setiap responden, namun mayoritas hampir memiliki kesamaan dari segi tren yang terjadi.



GRAFIK-V: TREN RATA-RATA DWI BULAN - II

A. NETWORK INCIDENT

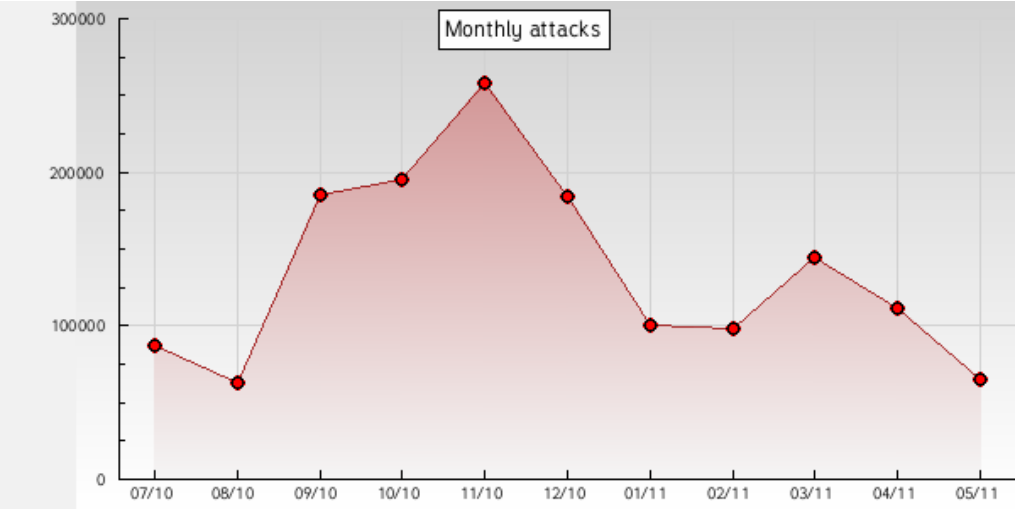
Terhitung mulai 23 Pebruari 2011 ini juga, ID-CERT mulai mengaktifkan email cert@cert.or.id sebagai alternatif tambahan penerimaan pengaduan internet abuse selain <abuse@cert.or.id> , namun diluar dugaan, ternyata email <cert@cert.or.id> menerima sekitar 10 pengaduan setiap menitnya tanpa henti. Pengaduan terbesar yang diterima melalui kedua akun email pengaduan yang ada melalui ID-CERT adalah *Network Incident*.

Kini, *Network Incident* menduduki peringkat pertama dari seluruh komplain yang diterima.

Dari seluruh laporan kategori ini yang masuk, umumnya disebabkan oleh banyaknya tindakan *probing* dan *Brute force* yang dilakukan dari IP Address Indonesia.

Yang termasuk dalam kategori ini diantaranya adalah: *DoS Attack, Open Relay, Open Proxy, Hacking, Port Scanning, Port Probe (HTTP/HTTPS, FTP, TELNET, TCP, SSH Brute, CGI, RPC, Netbios, VNC Portscan), TCP Sweep* dan *SQL Injection*.

Adapun komplain berikutnya dalam kategori ini adalah *Open Proxy* dan *DDoS.*



GRAFIK-VI: tren *Deface* bulanan ditingkat global (sumber: Zone-H)

Sebagai pembanding, ditingkat regional/global, Dari grafik VI diatas terlihat, bahwa tren yang terjadi tingkat global saat ini memiliki kecenderungan menurun pada dwibulan II tahun ini.Hal ini berbanding terbalik dengan yang terjadi di Indonesia.

Sejumlah peristiwa dunia yang terekam pada bulan Maret dan April ini diantaranya adalah: Kasus pembobolan sejumlah server milik *Wordpress*, yang berimbas pada masalah password user. (13 April 2011)

Bila dibandingkan pada bulan yang sama tahun 2010, tren saat itu adalah meningkat dari 1.566 laporan dibulan Maret 2010 menjadi 2.333 laporan dibulan April 2010.

B. SPAM

Dari total laporan yang masuk, *SPAM* menduduki peringkat kedua dari total laporan yang diterima.

SPAM sementara ini mengalami kenaikan pada bulan April dengan jumlah 29.592 laporan komplain.

Sedangkan bila dibandingkan dengan bulan yang sama tahun 2010 juga meningkat (bulan Maret 2010: 69.628 laporan, bulan April 2010: 100.631).Dan dari sisi volume laporan, tahun ini jauh lebih rendah dibandingkan pada bulan yang sama tahun 2010.

Sedangkan ditingkat global, berdasarkan data Messagelabs bulan April 2011, Negara-negara yang termasuk dalam negara paling banyak menerima spam adalah sebagai berikut:

APRIL 2011			
Rating	**Negara**	**% Spam**	**Keterangan**
1	Oman	81,9	Korban spam menurut penelitian *Messagelabs*
2	Belanda	74,1	
3	Australia	73,6	
4	Jerman	73	
5	USA	72,8	
6	Kanada	72,7	
7	Inggris	72,7	
8	Hong Kong	72,4	
9	Afrika Selatan	72,4	
10	Singapore	70,3	
11	Jepang	68,9	
…	**Indonesia**	**35,89**	**Riset Abuse ID-CERT 2011**

Tabel – 1: Rating Spam Dunia (Messagelabs dan ID-CERT)

C. INTELLECTUAL PROPERTY RIGHTS (LAIN-LAIN)

Posisi ketiga tertinggi pada tahun ini adalah dengan kategori LAIN-LAIN. Dimana yang masuk dalam kategori ini adalah semuanya terkait dengan pelanggaran HaKI (Hak Atas Kekayaan Intelektual) baik itu untuk Piranti Lunak maupun Film.

Umumnya pengirim keluhan/pengaduan ini berasal dari luar negeri.

Komplain ini juga mengalami penurunan dari 4.428 laporan pada bulan Maret menjadi 2.899 laporan pada bulan April.

Sedangkan bila dibandingkan dengan bulan yang sama tahun 2010, maka terjadi anomali dibanding tahun 2010. Sedangkan dari sisi volume laporan, mengalami penurunan (Maret 2010: 24.082 laporan, April 2010: 25.400 laporan).

D. MALWARE

Posisi keempat tertinggi adalah MALWARE.Posisi ini turun dibandingkan tahun sebelumnya.

Kecenderungan Malware pada bulan Maret dan April 2011 ini adalah menurun.

Bila dibandingkan dengan bulan yang sama ditahun 2010, maka tren yang terjadi adalah anomali dibanding tahun lalu (Maret 2010: 1.356 laporan; April 2010: 24.425 laporan).

Berdasarkan data Messagelabs, malware secara global memiliki kecenderungan menurun atau sama dengan tren di Indonesia pada bulan April 2011 ini.

Sejumlah peristiwa global yang terekam pada kurun waktu Maret-April ini adalah: Lebih dari satu juta Website diserang oleh *LizaMoon*. Motif penyerangan terkait dengan masalah uang.*(02 April 2011, selengkapnya pada lampiran).*

E. RESPON

Respon mengalami peningkatan dari posisi keenam pada Dwibulan-I menjadi posisi kelima pada Dwibulan-II ini.

Kecenderungan respon yang meningkat menunjukkan indikator yang cukup baik, karena pihak yang menerima komplain sudah mulai merespon laporan komplain yang masuk.

Sedangkan bila dibandingkan dengan jumlah komplain keseluruhan, respon masih terbilang rendah. Adapun penyebabnya: selain setiap keluhan/pengaduan yang masuk tidak/belum direspon, dimungkinkan pula bahwa respon dilakukan tanpa di tembuskan dalam proses riset ini.

F. SPOOFING / PHISHING

Posisi keenam tertinggi adalah *Spoofing/phishing*. yang mencakup pula *IP Spoofed, Web Spoofed* dan *Scam.*

Laporan pada dwibulan ini mengalami penurunan.

Dibandingkan dengan bulan yang sama tahun 2010, maka tren yang terjadi adalah anomali (Maret 2010: 58 laporan, April 2010: 264 laporan).

Dibulan Maret, hampir seluruh kasus Phishing menimpa sejumlah domain seperti .com, .edu, .go.id di Indonesia.

Sedangkan dibulan April, seluruh kasus Phishing menimpa sejumlah situs .com, .co.id, .or.id dan juga .go.id

Banyak sekali kasus spoofing/phising yang menimpa situs pemerintah (.go.id) yang sulit sekali dicari kontak penanggungjawabnya. Sehingga tidak jarang situs yang terdapat phishing tersebut baru diturunkan dalam jangka waktu 1-2 minggu. Padahal, semestinya situs yang terdapat Phishing harus diturunkan dalam waktu yang secepatnya agar korban yang mengakses situs yang terdapat Phishing tadi tidak terus berjatuhan dan kerugian bisa ditekan.

G. SPAM KOMPLAIN dan FRAUD

SPAM KOMPLAIN menempati peringkat terakhir.

Yang masuk pada kategori ini adalah laporan korban spam dari network di Indonesia maupun luar negeri.

Dibandingkan dengan bulan yang sama tahun 2010, saat itu belum ada laporan yang masuk dengan kategori ini.

Untuk *Fraud*, kami belum berhasil mendapatkan data dari pihak penegak hukum tentang berapa besar kasus Fraud yang terjadi di Indonesia. Kami sedang mengupayakan data dari sejumlah pihak terkait, yang insya Allah akan mulai kami umumkan pada laporan Semester – I tahun 2011 ini.

V. RANGKUMAN

Intellectual Property Rights/IPR (lain-lain), Spoofing/Phishing memiliki kecenderungan anomali (berbanding terbalik) dibandingkan bulan yang sama tahun sebelumnya. Ini artinya, kita tidak bisa selalu berpatokan pada bulan yang sama ditahun sebelumnya.

Yang perlu menjadi perhatian dari sisi volume laporan adalah *Network Incident* (*deface*, *hacking*, *Ddos*, *probing*, dsb) serta *spam* memiliki kecenderungan meningkat dalam dua bulan terakhir.

Berikut ini sejumlah rekomendasi :

A. Gunakan piranti lunak anti virus dan piranti lunak tambahan untuk mengurangi resiko *spam* ;
B. Hindari pencantuman alamat email ditempat umum seperti disitus web, forum, dsb. Gantikan dengan formulir isian;
C. Laporkan kepada ID-CERT bila menjadi korban dari tindakan *abuse* internet;
D. ISP dan Operator Telekomunikasi disarankan menyediakan tombol pelaporan khusus untuk *abuse* internet yang memudahkan user untuk melapor;
E. Cantumkan formulir pengaduan *Internet Abuse* disetiap website.
F. Terkait dengan HaKI, sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai konten yang melanggar HaKI, karena ISP maupun penyelenggara konten memerlukan landasan hukum yang jelas untuk menurunkan suatu konten yang bermasalah;
G. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada pihak penegak hukum;

VI. UCAPAN TERIMA KASIH

Dalam kesempatan ini, saya ingin mengucapkan terima kasih kepada berbagai pihak atas dukungan yang diberikan sehingga riset ini dapat terlaksana dengan baik dan lancar.

Ucapan terima kasih kami sampaikan kepada seluruh responden yang telah berpartisipasi dalam riset ini, yang terdiri dari:

[A] – Kementrian Komunikasi dan Informatika [KEMKOMINFO]

[B] – Direktorat Jendral Administrasi Hukum Umum (AHU), Kementrian Hukum dan HAM (KEMKUMHAM)

[C] – Pengelola Nama Domain Internet Indonesia [PANDI]

[D] – DETIK.NET

[E] – 5 Operator Telekomunikasi, 7 NAP dan 22 ISP.

VII. DAFTAR PUSTAKA

[1] – Statistik Internet Abuse 2010:
http://ahmadkaz.wordpress.com/riset-abuse/

[2] – Statistik MyCERT
http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html

[3] – APCERT Annual Reports 2009
http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2009.pdf

[4] – CERT Vulnerability Reporting forms; https://forms.cert.org/VulReport/

[5] – Messagelabs http://www.messagelabs.com/resources/mlireports.aspx

[6] – Tips menghindari spam di Yahoo :
http://answers.yahoo.com/question/index?qid=20100121090957AAHWAMm

[7] – Tren Deface bulanan secara global: http://www.zone-h.org/stats/ymd

[8] – Serangan LizaMoon: 1 JUTA HALAMAN WEBSITE DISERANG
http://www.detikinet.com/read/2011/04/02/101140/1607063/323/1-juta-halaman-website-diserang?i991101105

[9] – Security Incident pada Wordpress: http://en.blog.wordpress.com/2011/04/13/security/

VIII. LAMPIRAN

Sabtu, 02/04/2011 10:11 WIB
1 Juta Halaman Website Diserang
Ardhi Suryadhi - detikinet


Ilustrasi (Ist.)

Jakarta - Lebih dari satu juta halaman website dilaporkan telah menjadi korban serangan dedemit maya. Pelaku menyuntikkan kode-kode pemrograman dan mengarahkan pengunjung situs tersebut ke situs penjualan software palsu.

Pakar keamanan yang dikutip **detikINET** dari Reuters, Sabtu (2/4/2011), menyebut serangan ini sebagai '*mass injection*', dan tercatat sebagai serangan terbesar yang pernah ada untuk versi ini.

Websense, pihak yang mendeteksi serangan massal tersebut di awal minggu lalu menyebut aksi ini sebagai 'LizaMoon'.

Senior Manager lembaga riset keamanan Websense, Patrik Runald, mengatakan pengguna akan melihat bahwa telah di-*redirect* ketika mereka coba mengakses situs yang telah terinfeksi tersebut.

Namun sejauh ini, mereka yang menjadi target serangan dilaporkan masih sebatas situs-situs kecil. Belum ditemukan situs populer milik perusahaan atau pemerintah yang jadi korban.

Tidak dijelaskan dengan jelas siapa pelaku atau dari mana asal serangan ini, yang pasti ujung-ujungnya motif pelaku diduga terkait uang.
"Serangan seperti ini akan bertahan dalam jangka waktu lama. Sekali mereka masuk, maka akan tetap bertahan dengan kita. Serangan LizaMoon ini tidak akan hilang dalam satu hari," pungkas Runald.

(ash / ash)