STATISTIK INTERNET ABUSE INDONESIA 2011

LAPORAN DWI BULAN-IV TAHUN 2011

Bulan JULI dan AGUSTUS

Edisi: I

27 September 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.

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.

Yang menjadi perhatian kami pada Dwibulan-IV ini adalah komplain/pengaduan atas ***Network Incident*** yang terus meningkat sejak bulan Pebruari yang lalu 2011. Data ini belum bersifat final karena masih ada **5 (lima) Responden** yang belum menyerahkan datanya kepada kami.

Selain ***Network Incident***, peningkatan juga terjadi pada ***Malware*** dan ***Spoofing/Phishing.*** Dalam dua bulan terakhir ini, terjadi kasus ***Spoofing/Phishing*** yang terkontaminasi ***Malware***. Umumnya yang mengalami hal ini adalah sejumlah situs palsu perbankan di Indonesia dan Malaysia yang di “tempelkan” pada sejumlah situs web di Indonesia yang memiliki kelemahan sistem operasi/aplikasi. Situs web yang sering “ditempelkan” oleh masalah ini adalah: situs web Sekolah/Universitas (.sch.id, ac.id), Korporasi (.co.id, .com, .net) dan Pemerintahan (go.id) serta sejumlah situs web pribadi (blog).

Hingga laporan ini dibuat, komplain atas kasus ***Network Incident***, ***Spoofing/Phishing*** maupun ***Malware*** dan ***Spam*** juga terus meningkat.

Penelitian ini juga mendapatkan dukungan sponsor dari PANDI.

II. Metodologi penelitian

Metodologi yang digunakan dalam penelitian ini adalah:

A. Pengambilan data dari sejumlah responden.

B. Metode analisis berdasarkan:

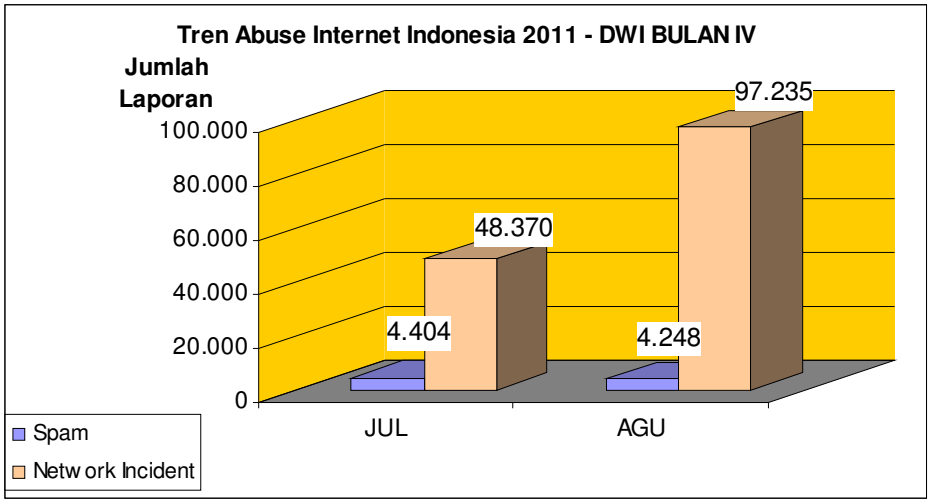
B.1. Tembusan laporan yang masuk via email akun abuse ISP/ Operator Telekomunikasi/lembaga non-ISP.

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

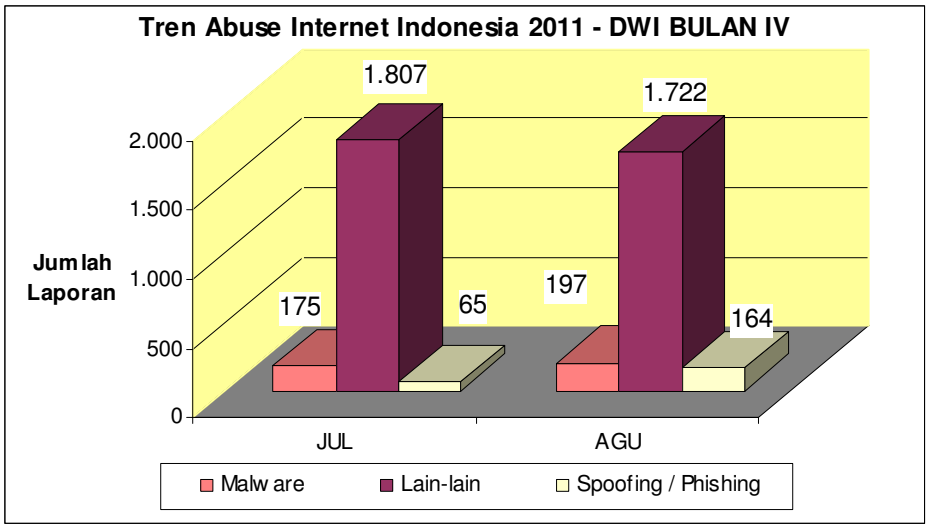
C. Dari laporan tersebut, kami melakukan pengkategorian laporan sebagai berikut:

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.

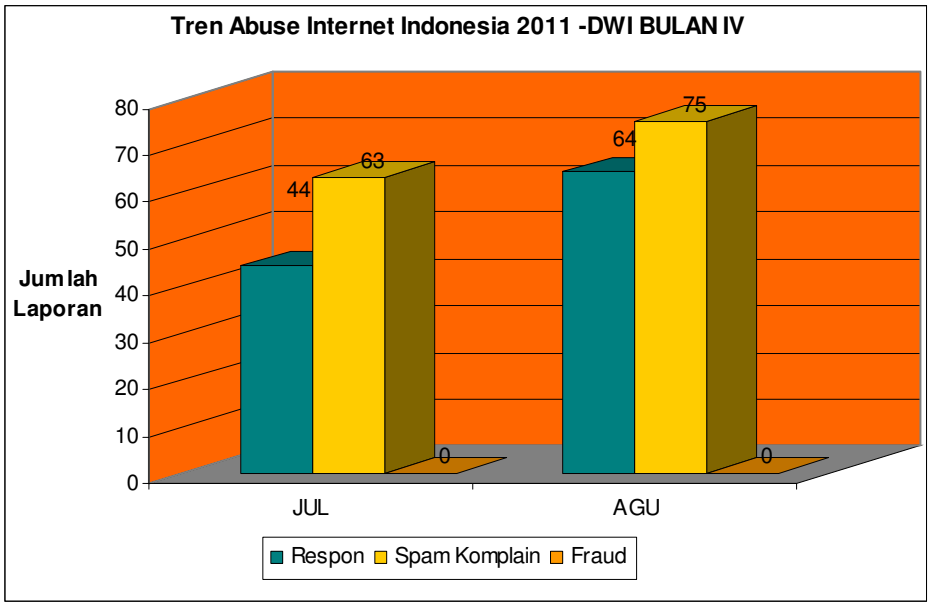
III. STATISTIK JULI – AGUSTUS



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

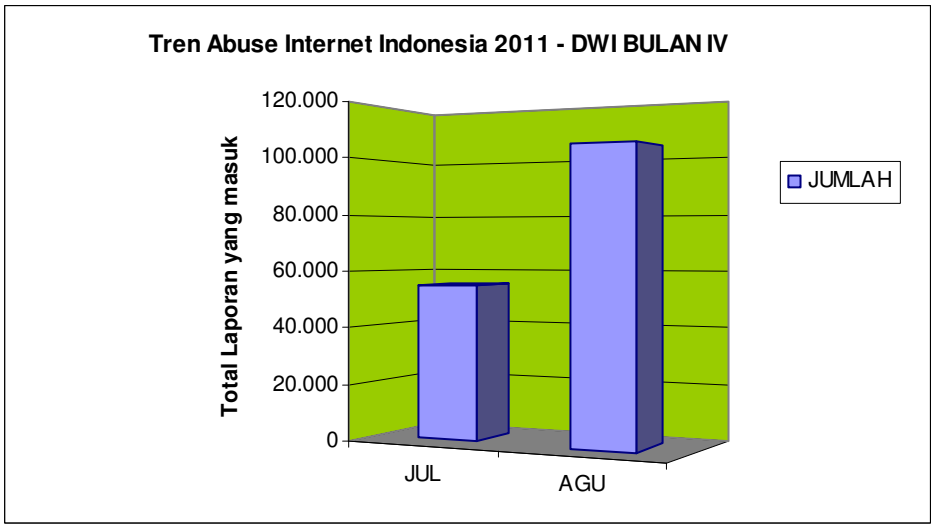


GRAFIK-II: Kategori MALWARE, Intellectual Propterty Rights/IPR (Lain-Lain) dan SPOOFING/PHISHING, Dwi Bulan - IV



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

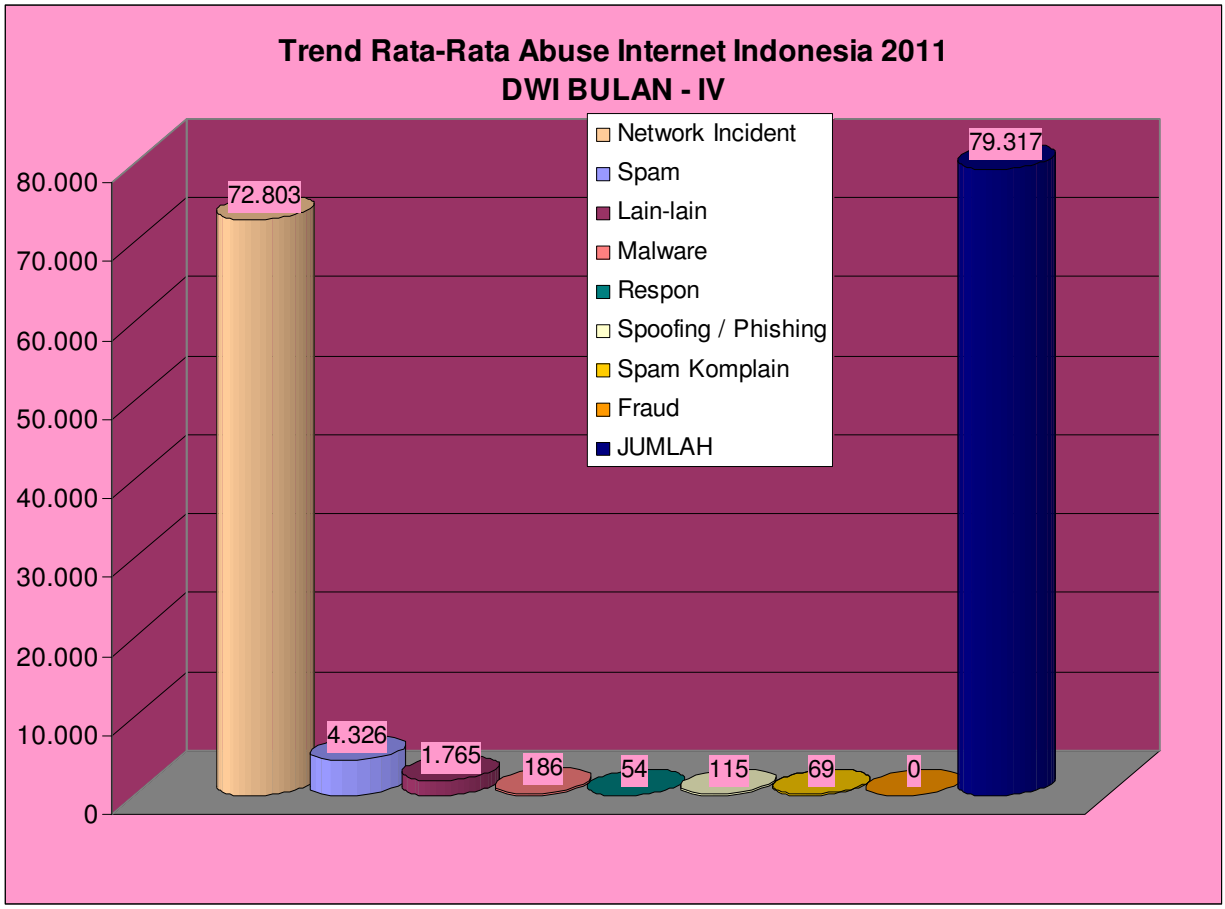
Tren rata-rata per bulannya secara total mencapai 79.317 laporan keluhan/pengaduan yang masuk.



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

IV. URAIAN

Secara umum pada Dwi Bulan – IV 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 - IV

A. NETWORK INCIDENT

Kini, *Network Incident* menduduki peringkat pertama sejak 9 bulan terakhir 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.*

Selain itu, terdapat pula laporan tentang IP Address pemerintah yang digunakan untuk melakukan *Network Incident* ke luar/dalam negeri, seperti melakukan *DDOS Attack, Probing* bahkan hingga *Flooding*. Laporan terbanyak untuk sektor pemerintah ini justru datang dari IP Address dan Situs web yang digunakan oleh kalangan pendidikan dibawah salah satu kementrian. Untuk Situs web, banyak laporan tentang adanya situs web .SCH.ID dan AC.ID yang mengalami serangan siber.

Bila dibandingkan pada bulan yang sama tahun 2010, tren saat itu adalah meningkat dari 124 laporan dibulan Juli 2010 menjadi 2.988 laporan dibulan Agustus 2010.

B. SPAM

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

SPAM sementara ini mengalami kenaikan pada bulan Juli dengan jumlah 4.404 laporan komplain.

Sedangkan bila dibandingkan dengan bulan yang sama tahun 2010 juga menurun (bulan Juli 2010: 703.465 laporan, bulan Agustus 2010: 686.537).Dan dari sisi volume laporan, tahun ini jauh lebih rendah dibandingkan pada periode yang sama tahun 2010.

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 sedikit penurunan dari 1.807 laporan pada bulan Juli menjadi 1.722 laporan pada bulan Agustus.

Sedangkan bila dibandingkan dengan bulan yang sama tahun 2010, maka terjadi anomali dibanding tahun 2010. Dari sisi volume laporan, mengalami kenaikan (Juli 2010: 1.294 laporan, Agustus 2010: 2.678 laporan).

D. MALWARE

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

Kecenderungan Malware pada bulan Juli dan Agustus 2011 ini adalah meningkat

Bila dibandingkan dengan bulan yang sama ditahun 2010, maka tren yang terjadi adalah anomali dibanding tahun lalu (Juli 2010: 4.790 laporan; Agustus 2010: 302 laporan).

Kasus yang menjadi sorotan dalam dua bulan terakhir ini adalah kasus Spoofing/Phishing yang berkombinasi dengan Malware: dimana situs web yang ditempeli dengan situs palsu ini berisi formulir bank palsu terdapat Malware yang akan menyerang disisi end-user yang membuka URL Phishing tersebut.

Untuk itu dihimbau kepada pemilik Server yang terkena kasus Spoofing/Phishing tersebut dan juga bagi yang belum terkena untuk memproteksi server mereka dengan cara mengupdate system mereka dengan update terbaru dan mengaktifkan opsi-opsi Pengamanan yang tersedia.Sistem yang diserang diantaranya yang berbasis Windows hingga Open Source seperti RedHat, Linux, dsb.

Adapula email Spoofing/Phishing yang beredar mengatasnamakan salah satu perbankan di Indonesia, agar melakukan instalasi program guna memproteksi transaksi online perbankan mereka, padahal software yang diberikan adalah Malware yang justru dapat membocorkan informasi transaksi online nasabah yang bersangkutan bila aplikasi tersebut di install.

E. SPOOFING / PHISHING

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

Laporan pada dwibulan ini mengalami peningkatan.

Dibandingkan dengan bulan yang sama tahun 2010, maka tren yang terjadi adalah anomali (Juli 2010: 3 laporan, Agustus 2010: 5 laporan).

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.

Sejumlah situs web perbankan di Indonesia yang dipalsukan serta dibuat mirip dengan aslinya. Umumnya situs yang dipalsukan adalah dengan nama domain generik (.COM, .NET, dsb). Sedangkan untuk bank dengan nama domain .CO.ID, hampir belum pernah ada laporan yang masuk.

Selain bank di Indonesia, hal yang sama juga menimpa situs perbankan di Malaysia dan Eropa yang justru dipalsukan dan ditempeli disitus web maupun IP Address organisasi di Indonesia.

Kesulitan ID-CERT adalah dalam hal menghubungi pihak Perbankan di Indonesia yang menjadi korban agar ada awareness dari pihak perbankan ybs untuk bisa memberikan himbauan antisipasi kepada nasabah mereka.

Sedangkan dari luar negeri, ID-CERT banyak menerima laporan dari CERT Perbankan Brazil dan HSBC Amerika Serikat selain juga tentunya dari CMC Malaysia dan Anti Fraud Comand Center (AFCC) yang banyak menginformasikan tentang adanya situs perbankan mereka yang dipalsukan menggunakan nama domain maupun IP Address Indonesia.

Phishing juga dilakukan melalui peredaran email atau yang disebut dengan *scam*. ID-CERT menerima laporan dari sebuah kelompok anti Fraud di Eropa yang menyampaikan keluhan tentang adanya dugaan email *Scam* yang beredar di Eropa mengatasnamakan institusi pemerintah Indonesia dan meminta bantuan ID-CERT melakukan investigasi lebih jauh tentang hal ini. Dalam kasus ini, ID-CERT telah meneruskan pengaduan tersebut kepada para pihak terkait.

F. SPAM KOMPLAIN

SPAM KOMPLAIN menempati peringkat ke enam.

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

Dibandingkan dengan bulan yang sama tahun 2010, Juli 2010: 20 laporan, Agustus 2010: 39 laporan.

G. RESPON dan FRAUD

Respon mengalami penurunan ke posisi ke lima pada Dwibulan-II menjadi posisi ke tujuh pada Dwibulan-IV ini.

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.

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 kami umumkan pada laporan Final tahun 2011 ini.

V. RANGKUMAN

Sejumlah masalah yang menjadi perhatian dalam penelitian kami kali ini adalah sebagai berikut:

A. Kasus *Spoofing/Phishing* yang berkombinasi dengan *Malware*: Saran kepada pemilik Server yang terkena kasus Spoofing/Phishing tersebut dan juga bagi yang belum terkena untuk memproteksi server mereka dengan cara mengupdate system mereka dengan update terbaru dan mengaktifkan opsi-opsi Pengamanan yang tersedia.Sistem yang diserang diantaranya yang berbasis Windows hingga Open Source seperti RedHat, Linux, dsb;

B. Kasus *Scam* (Penipuan) mengatasnamakan Institusi pemerintah Indonesia: Merespon hal ini, ID-CERT menyatakan bahwa untuk masalah teknis dihimbau kepada ISP, NAP dan Operator Telekomunikasi untuk membantu menginformasikan kepada pelanggan mereka tentang adanya kemungkinan kelemahan pada sistem mereka yang mungkin saja dimanfaatkan oleh pihak lainnya. Sedangkan untuk masalah investigasinya, ID-CERT menyerahkan masalah ini kepada sejumlah pihak terkait untuk menelusurinya lebih jauh karena ID-CERT tidak memiliki kewenangan apapun untuk melakukan hal ini;

C. Sejumlah situs web pemerintah, disusupi oleh Phishing yang berulang: Terdapat sejumlah kasus Spoofing/Phishing berkombinasi dengan Malware: yang menimpa sejumlah situs web Pemerintah (.go.id) dan peristiwa kerap berulang dalam beberapa minggu setelah diperbaiki. Adapula yang kontaknya tidak merespon dan setelah ditelusuri, ternyata kontak admin dari institusi pemerintah tersebut diberikan kepada vendor/pihak ketiga/non-Pegawai institusi ybs;

D. IP Address pemerintah yang digunakan untuk melakukan Network Incident ke luar/dalam negeri, seperti *melakukan DDOS Attack, Probing bahkan hingga Flooding*: Laporan terbanyak untuk sektor pemerintah ini justru datang dari IP Address dan Situs web yang digunakan oleh kalangan pendidikan dibawah salah satu Kementrian. Untuk Situs web, banyak laporan tentang adanya situs web .SCH.ID dan AC.ID yang mengalami serangan siber;

E. Kasus *Spoofing/Phishing* yang menimpa sejumlah bank di Indonesia dan Malaysia serta sejumlah negara Eropa: Kasus terbanyak yang dilaporkan ke ID-CERT dalam masalah *Spoofing/Phishing* ini adalah situs web perbankan di Indonesia yang dipalsukan serta dibuat mirip dengan aslinya. Umumnya situs yang dipalsukan adalah dengan nama domain generik (.COM, .NET, dsb). Sedangkan untuk bank dengan nama domain .CO.ID, hampir belum pernah ada laporan yang masuk. Selain bank di Indonesia, hal yang sama juga menimpa situs perbankan di Malaysia dan Eropa yang justru dipalsukan dan ditempeli disitus web maupun IP Address organisasi di Indonesia;

F. Kesulitan ID-CERT adalah dalam hal menghubungi pihak Perbankan di Indonesia yang menjadi korban agar ada awareness dari pihak perbankan ybs untuk bisa memberikan himbauan antisipasi kepada nasabah mereka. Sedangkan dari luar negeri, justru ID-CERT banyak menerima laporan dari CERT Perbankan Brazil dan HSBC Amerika Serikat selain juga tentunya dari CMC Malaysia dan Anti Fraud Comand Center (AFCC) yang banyak menginformasikan tentang adanya situs perbankan mereka yang dipalsukan menggunakan nama domain maupun IP Address Indonesia;

G. Berikut ini sejumlah rekomendasi :

- ✓ Gunakan piranti lunak anti virus dan piranti lunak tambahan untuk mengurangi resiko *spam* ;
- ✓ Hindari pencantuman alamat email ditempat umum seperti disitus web, forum, dsb. Gantikan dengan formulir isian;
- ✓ Laporkan kepada ID-CERT <abuse@cert.or.id> bila menjadi korban dari tindakan *abuse* internet;
- ✓ ISP dan Operator Telekomunikasi disarankan menyediakan tombol pelaporan khusus untuk *abuse* internet yang memudahkan user untuk melapor;
- ✓ Cantumkan formulir pengaduan *Internet Abuse* disetiap website.
- ✓ 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;
- ✓ 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 Perdagangan [KEMDAG]

[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/