Laporan Dwi Bulan IV 2013

ID-CERT[1]

Ringkasan
Di laporan Dwi Bulan IV 2013 ini disajikan hasil pengumpulan pengaduan selama dua bulan, Juli dan Agustus 2013. Pengaduan tsb. diterima dalam bentuk email dan dikumpulkan sesuai kategori, sebagai bahan penyusunan statistik, dalam bentuk angka dan grafik. Spam, komplain spam, respon, network incident, Hak atas Kekayaan Intelektual, fraud, spoofing/phising, dan malware merupakan kategori yang dipilih untuk pengelompokan pengaduan yang masuk.

Kata kunci
Security – Pelaporan – Laporan Dwi Bulan

[1] Diterbitkan 21 Oktober 2013

Daftar Isi

1. Pendahuluan

Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian lebih penting – dari komunikasi antarwarga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lansia, para pekerja di lapangan hingga bot otomatis. Batas-batas yang telah ada sebelumnya juga mengalami pergeseran dengan adanya Internet, menciptakan kemungkinan baru yang perlu dicermati. Tidak terkecuali aspek keamanan Internet (Internet security) yang menjadi perhatian secara khusus dan kerja sama banyak kalangan.

Sebagai bagian dari pemantauan keamanan Internet, ID-CERT[1] menerima pengaduan lewat email yang diterima dari beberapa responden. Pengaduan tsb. dikelompokkan dalam sejumlah kategori dan disajikan dalam bentuk laporan Dwi Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (security incident) yang terjadi selama dua bulan, Juli dan Agustus 2013. Selain gambaran tsb., penyediaan laporan ini juga dimaksudkan sebagai contoh data primer keamanan teknologi informasi (TI) di Indonesia.

Penting ditekankan dalam hal ini adalah tindak lanjut terhadap laporan tentang penyalahgunaan Internet (Internet abuse) sebagai respon positif dan langkah untuk memperbaiki keadaan. Hal ini juga bagian interaksi positif antara kita, pengguna Internet di Indonesia, dengan

[1] Indonesia Computer Emergency Response Team.

pihak-pihak di mancanegara terkait penanganan laporan. Pengaduan yang diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antarlembaga, dan untuk membantu penyusunan rencana ke depan.

Pada laporan Dwi Bulanan IV 2013 ini, spam menempati jumlah pengaduan terbanyak. Dari jumlah pelaporan per kategori, di laporan kali ini tidak terdapat perbedaan yang mencolok dari satu kategori ke kategori lain, hanya terdapat lonjakan yang sangat tinggi untuk komplain spam sampai dua puluh kali lipat. Pengaduan dikumpulkan dalam bentuk email yang diterima ID-CERT dari para responden ditambah informasi sudah dalam bentuk cacah hasil penghitungan dari APJII.

Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: spam sendiri pada kelompok pertama, selanjutnya kelompok kedua memiliki jumlah pelaporan sedang, dan kelompok terakhir berjumlah pengaduan rendah. Penjelasan lengkap tentang ketiga kelompok tsb. dipaparkan di bagian Uraian.

Pada penelitian ini, data diambil dari tiga puluh tujuh (37) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), tiga operator telekomunikasi, tujuh NAP, dan 22 Penyedia Jasa Interenet (PJI/ISP).

2. Metoda

Penyusunan dokumen Dwi Bulan ini dari beberapa sumber dalam bentuk laporan dengan langkah-langkah berikut:

1. Pengambilan data dari sejumlah responden.
2. Penyusunan analisis berdasarkan:
   (a) Tembusan laporan yang masuk lewat alamat email pengaduan penyalahgunaan (abuse) yang disediakan PJI/operator telekomunikasi/lembaga non-ISP.
   (b) Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi ini berupa kumpulan data yang telah dihitung dan dikelompokkan oleh responden.

Dari laporan yang sudah terkumpul, dilakukan pengelompokan sbb.:

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain[2] berdasarkan data yang sudah masuk ke penegak hukum.

Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau Intellectual Property Rights (IPR).

Komplain Spam Keluhan/pengaduan email spam dari dalam negeri terhadap pengirim di Indonesia dan luar negeri.

Malware Program komputer yang dibuat untuk maksud jahat[3].

Network incident Aktivitas yang dilakukan terhadap jaringan pihak lain dan semua aktivitas terkait dengan penyalahgunaan jaringan.

Respon Respon terhadap laporan yang masuk.

Spam Penggunaan sistem pengelolaan pesan elektronik untuk mengirim pesan-pesan tidak-diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih[4].

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna[5].

Lain-lain Laporan penyalahgunaan selain yang termasuk pada kategori di atas.

3. Uraian

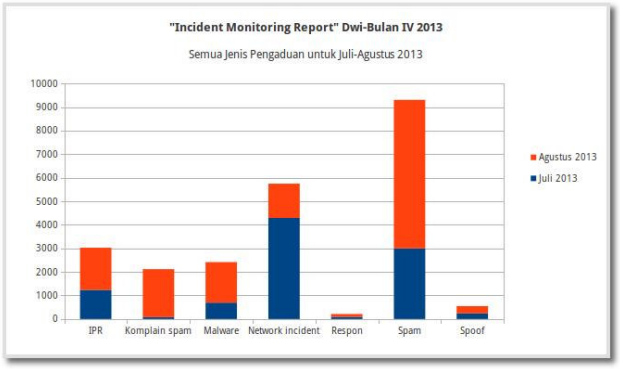
Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, bulan Juli dan Agustus 2013. Kategori pengaduan terdiri atas Hak atas Kekayaan Intelektual (HaKI)

[2] Fraud, http://en.wikipedia.org/wiki/Fraud
[3] Malware, http://en.wikipedia.org/wiki/Malware
[4] Spam (electronic), http://en.wikipedia.org/wiki/Spam_(electronic)
[5] Spoofing attack, http://en.wikipedia.org/wiki/Spoofing_attack

atau Intellectual Property Rights (IPR), komplain spam, malware, network incident, respon, spam, dan spoof. Pengolahan data dilakukan dengan dua cara:

1. Penghitungan cacah dari tajuk (header) email, seperti bagian From, To, Cc, dan Subject. Cara ini terutama digunakan untuk pengaduan dalam kondisi tidak terformat bagus, karena email tidak mengikuti format baku yang biasanya dihasilkan perangkat lunak pelapor. Kategori pengaduan seperti spam, spoof biasanya termasuk jenis ini.
2. Penghitungan cacah dari isi email (body). Pengaduan network incident dan malware sebagai misal, menggunakan format pesan yang baku dan nama domain yang diadukan dapat diperoleh dari isi email pada bagian yang menggunakan format tertentu.

Grafik semua kategori Incident Monitoring Report untuk Dwi Bulan IV 2013 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



Gambar 1. Incident Monitoring Report Dwi Bulan IV 2013 Semua Kategori

Jumlah pengaduan masing-masing dapat dilihat dengan lebih seksama di Tabel 1 dengan kategori pengaduan ditampilkan berdasarkan urutan abjad. Perhitungan perkembangan dilakukan terhadap jumlah pada bulan pertama, Juli, dan bernilai negatif jika terjadi penurunan. Kenaikan terjadi pada jumlah pelaporan bulan Agustus dibanding Juli, dengan persentase kenaikan terbanyak pada Komplain spam dan satu-satunya penurunan pada network incident.

Total pengaduan selama dua bulan dan persentase masing-masing, dihitung terhadap jumlah pengaduan keseluruhan, dapat dilihat pada Tabel 2. Tampilan tabel tsb. berdasarkan urutan persentase kategori dari terbanyak. Tampilan dalam bentuk diagram lingkaran disajikan pada Gambar 2.

Kategori	Juli	Agustus	Perkembangan
IPR	1:238	1789	44; 51%
Komplain spam	79	2:037	2478; 48%
Malware	696	1721	147; 27%
Network incident	4291	1:454	66; 12%
Respon	91	122	34; 07%
Spam	2:998	6:305	110; 31%
Spoof	240	310	29; 17%

Table 1. Perkembangan jenis pengaduan selama Juli dan Agustus 2013

Jenis	Juli	Agustus	Total	Persentase
Spam	2:998	6:305	9:303	39; 81%
Network incident	4:291	1:454	5:745	24; 58%
IPR	1:238	1:789	3:027	12; 95%
Malware	696	1:721	2:417	10; 34%
Komplain spam	79	2:037	2:116	9; 05%
Spoof	240	310	550	2; 35%
Respon	91	122	213	0; 91%

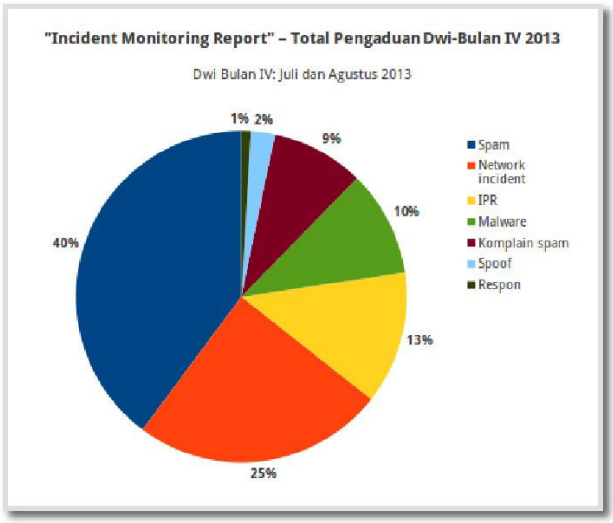
Table 2. Jenis pengaduan ditampilkan berdasarkan peringkat persentase masing-masing

3.1 Kelompok pertama: spam, network incident, dan IPR

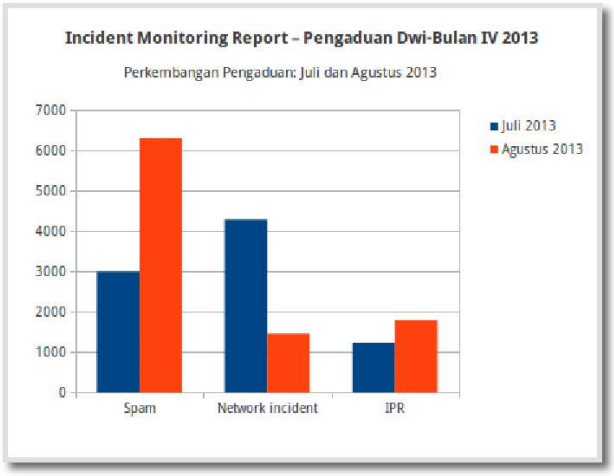
Spam menempati posisi tertinggi, berjumlah total sekitar 9.300 email pengaduan yang diterima atau 39,81% dari total pengaduan. Dari pengaduan yang diterima, paling banyak berupa laporan gangguan terhadap server mail, sebanyak 92%. Pengaduan ini ditandai dengan adanya kata kunci postfix[6] di dalam pesan email.

Kenaikan pengaduan spam dari Juli ke Agustus sebesar 110,31% termasuk sedang untuk kondisi saat ini, yakni pada peringkat ketiga. Akan halnya network incident yang berada pada posisi kedua dari jumlah pengaduan, yakni 24,58% justru mengalami penurunan jumlah pengaduan sebesar -66,12%. Pada peringkat ketiga, intellectual property rights

[6] Postfix adalah perangkat lunak server email atau dikenal dengan Mail Transfer Agent (MTA) dan berdasarkan perhitungan tahun 2012 disebut digunakan oleh 23% server email di Internet. Sumber: Wikipedia, http://en.wikipedia.org/wiki/Postfix_(software)



Gambar 2. Persentase pengaduan per kategori selama Dwi Bulan IV 2013



Gambar 3. Pengaduan spam, network incident, IPR untuk Juli dan Agustus 2013

(IPR), tercatat 12,95% pengaduan, mengalami kenaikan 44,51%.

Secara umum dari tiga besar kategori pengaduan ini terkumpul masing-masing lebih dari 3.000 pengaduan dan mendominasi pelaporan, sedangkan dari sisi perbedaan terhadap kelompok berikutnya relatif landai.

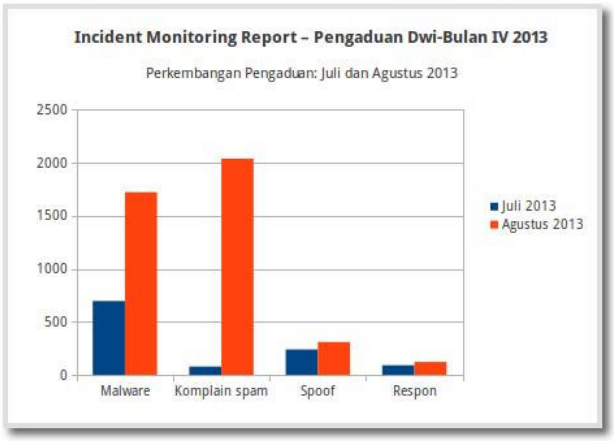
3.2 Bagian 2: malware, komplain spam, spoof, dan respon

Pada Bagian 2 pelaporan diisi malware, komplain spam, spoof, dan respon. Dengan total pengaduan masing-masing di bawah 3.000, empat kategori di bagian kedua ini terbagi dua besar: malware dan komplain spam pada angka 2.000-an dan terakhir, pengaduan spoof dan respon pada kisaran 500 pengaduan.

Catatan yang menarik adalah lonjakan yang sangat tinggi pada komplain spam, hingga 2478% atau 24 kali lipat. Belum ada penjelasan tentang fenomena ini.

4. Rangkuman

Jumlah pengaduan spam masih teratas, sehingga perlu diperhatikan oleh administrator jaringan, baik untuk jaringan



Gambar 4. Grafik malware, komplain spam, spoof, dan respon

lokal atau pengguna layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi “pintu gerbang” pengiriman spam (terutama lewat email) dan mengantisipasi kedatangan spam.

Dilihat dari volume pengaduan yang masuk – yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet – menjadi tanggung jawab pihak-pihak terkait dengan bahan laporan tsb. untuk menindaklanjuti dalam bentuk respon atau aksi yang diperlukan. Dengan demikian, prosedur standar yang menjadi acuan dapat dijalankan dengan baik dan kepercayaan pihak pelapor terjaga atau meningkat.

4.1 Rekomendasi

Sejumlah rekomendasi yang dapat dipertimbangkan:

1. Perangkat lunak anti-spam dipasang di server email sebagai antisipasi pengiriman pesan spam dari jaringan lokal ke Internet.

2. Perangkat lunak anti virus dan perangkat lunak keamanan dipasang untuk mengurangi risiko terinfeksi malware. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara teratur.

3. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, semisal akses ke port email/Postfix[7] secara intensif dalam periode lama atau berulang-ulang.

4. Administrator jaringan memblokir semua port akses ke Internet, kecuali untuk port yang dianggap diperlukan.

5. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (Internet abuse) guna kemudahan pelaporan.

6. Formulir pengaduan penyalahgunaan Internet (Internet abuse) dicantumkan di setiap situs web.

7. Terkait Hak atas Kekayaan Intelektual (HaKI), sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai materi (content) yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.

8. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada penegak hukum.

5. Ucapan terima kasih

Terima kasih pada seluruh responden yang telah berpartisipasi pada pengumpulan bahan untuk penulisan laporan ID-CERT, yakni:

1. Kementerian Komunikasi dan Informatika (Kominfo).
2. Pengelola Nama Domain Internet Indonesia (PANDI).
3. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).
4. Detik (Detik.net).
5. Tiga operator telekomunikasi, tujuh NAP, dan dua puluh dua PJI/ISP.

6. Lampiran

6.1 Saling serang di dunia maya antara "peretas" Indonesia dan Bangladesh

Pada periode dwi bulan keempat ini, tepatnya di akhir Juli, terjadi insiden saling serang antara kelompok yang mengaku sebagai "peretas"[8] dari Indonesia dan Bangladesh.

Agak mengejutkan karena tidak ada kejadian khusus antara kedua negara ini yang menjadi pemicu, termasuk berita di media massa tentang insiden ini terbatas. Kabar yang sedikit lebih banyak dapat diperoleh di media sosial, seperti Facebook. Karena akhir Juli tsb. bertepatan dengan bulan Ramadan, seperti janggal ada insiden "saling serang" antara Indonesia dan Bangladesh yang sama-sama negara berpenduduk mayoritas muslim. Akhirnya, sebelum menjadi berlarut-larut, insiden ini berhasil dihentikan.

Salah satu rilis dari pihak Bangladesh sbb.

> Rotating Rotor To all the crews: After a meeting, we, admins decided to deface any server which we'll get from now..
> dont care about any country...just concentrate on mirror zones...
> no friends...no enemies....no peace...no war...

[7] Terkait jumlah pengaduan spam yang sangat banyak.

[8] peretas adalah padanan untuk hacker

If u find any server which is good to deface...just do it without hesitation....

No need to ask questions to anyone.. No need to answer anyones question.

just deface,deface & deface.....

from now start random defacing..

Thanks.... Share 4726 Sunday at 09:29 via Mobile