Laporan Dwi Bulan III 2013

ID-CERT[1]

Ringkasan
Di laporan Dua Bulan III 2013 ini disajikan hasil pengumpulan pengaduan selama dua bulan, Mei dan Juni 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 September 26, 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, Mei dan Juni 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 III 2013 ini, *spam* menempati jumlah pengaduan terbanyak, jauh meninggalkan jenis pengaduan lain. Perlu dijelaskan bahwa telah dilakukan pembahasan tentang jenis pelaporan yang paling banyak kami terima dan selama ini dikategorikan sebagai *insiden jaringan*; setelah dipertimbangkan lebih seksama, akhirnya ditetapkan bahwa pelaporan tsb. termasuk jenis *spam*. Penjelasan tentang perubahan ini sudah disinggung pada laporan Dwi Bulanan II 2013 sebagai rencana dan sekarang direalisasikan. Alhasil, perubahan kategorisasi ini penyebab terjadinya penggantian jumlah pengaduan terbanyak.

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

[2] *Fraud*, `http://en.wikipedia.org/wiki/Fraud`
[3] *Malware*, `http://en.wikipedia.org/wiki/Malware`

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 Juni dan Juli 2013. Kategori pengaduan terdiri atas Hak atas Kekayaan Intelektual (HaKI) 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.

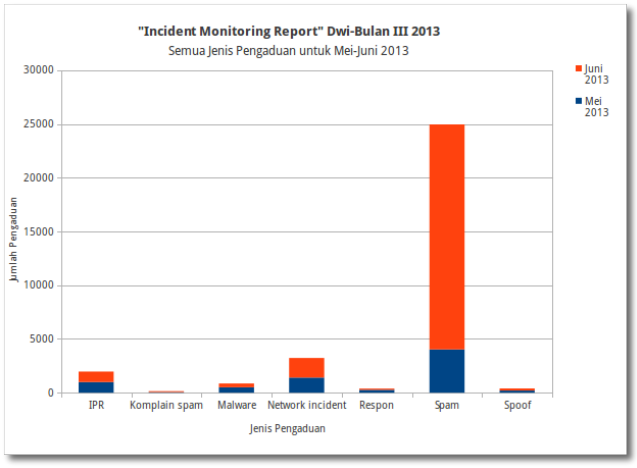
2. Penghitungan cacah dari isi email (*body*). Pengaduan *network incident* dan *malware* sebagai misal, menggunakan format pesan yang baku dan nama domain yang diadukan dapat diperoleh dari isi email pada bagian yang menggunakan format tertentu.

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

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, Mei, dan

[4] *Spam (electronic)*, `http://en.wikipedia.org/wiki/Spam_(electronic)`

[5] *Spoofing attack*, `http://en.wikipedia.org/wiki/Spoofing_attack`



Gambar 1. *Incident Monitoring Report* Dwi Bulan III 2013 Semua Kategori

bernilai negatif jika terjadi penurunan. Kenaikan terjadi pada jumlah pelaporan bulan Juni dibanding Mei, paling banyak pada *spam* dan terjadi penurunan banyak untuk respon.

Kategori	Mei	Juni	Perkembangan
IPR	994	971	−2,31%
Komplain *spam*	60	84	40,00%
Malware	507	353	−30,37%
Network incident	1.408	1.824	29,55%
Respon	263	125	−52,47%
Spam	4.026	20.931	419,90%
Spoof	205	191	−6,83%

Table 1. Perkembangan jenis pengaduan selama Mei dan Juni 2013

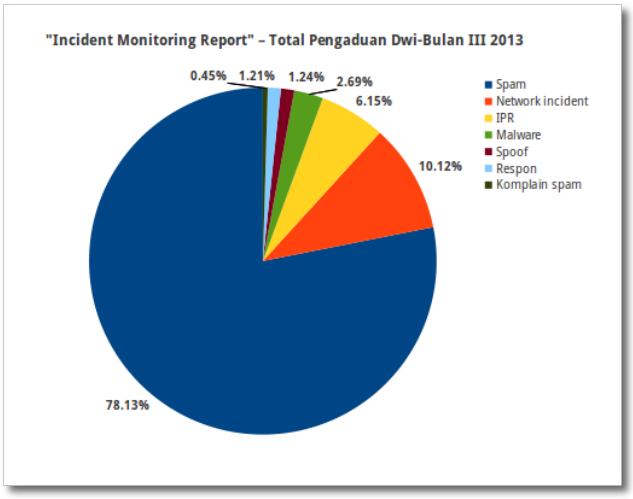
Total pengaduan selama dua bulan dan persentase masing-masing, dihitung terhadap jumlah pengaduan keseluruhan, dapat dilihat pada *Tabel 2*. Tampilan tabel tsb. berdasarkan urutan persentase kategori dari terbanyak. Tampilan dalam bentuk diagram lingkaran disajikan pada *Gambar 2*.

3.1 *Spam* pada posisi tertinggi

Spam menempati posisi tertinggi, berjumlah total hampir 25.000 email pengaduan yang diterima. Pengaduan paling banyak berupa laporan gangguan kedatangan *spam* oleh server mail, sebanyak 98,22%. Pengaduan ini ditandai

Jenis	Mei	Juni	Total	Persentase
Spam	4.026	20.931	24.957	78,13%
Network incident	1.408	1.824	3.232	10,12%
IPR	994	971	1.965	6,15%
Malware	507	353	860	2,69%
Spoof	205	191	396	1,24%
Respon	263	125	388	1,21%
Komplain *spam*	60	84	144	0,45%

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



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

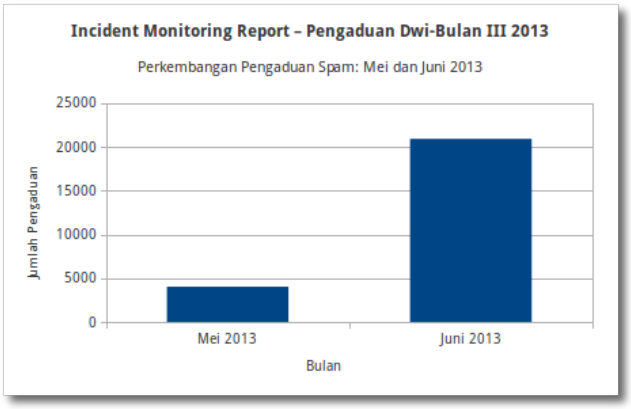
dengan adanya kata kunci `postfix`[6] di dalam pesan email.

Terjadi kenaikan yang sangat tinggi untuk pengaduan *spam*, tercatat jumlah pengaduan pada bulan Juni sebesar empat kali lipat jumlah pengaduan pada bulan Mei, 420%. Belum terdapat penjelasan terkait lonjakan luar biasa pengaduan *spam* ini, karena jika diamati sumber pengirimnya tetap didominasi oleh satu pihak yang sama dengan bulan-bulan sebelumnya.

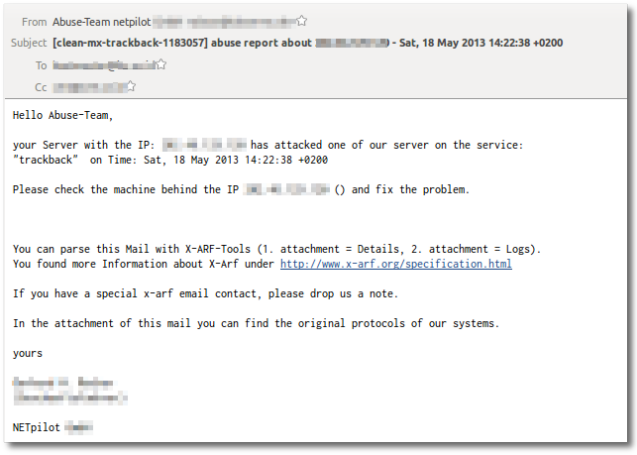
3.2 Bagian 2: *network incident*, *IPR*, dan *malware*

Pada Bagian 2 pelaporan, yang diisi *network incident*, *IPR*, dan *malware*, pelaporan masing-masing berkisar pada angka

[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 3. Jumlah pengaduan *spam* untuk Mei dan Juni 2013

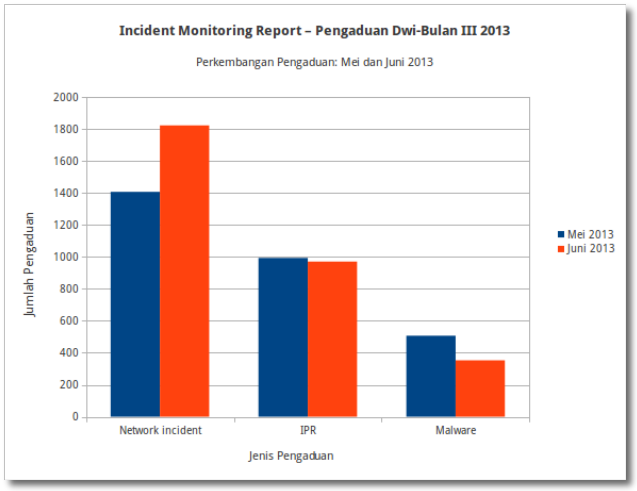


Gambar 4. Contoh pengaduan *spam* lewat email

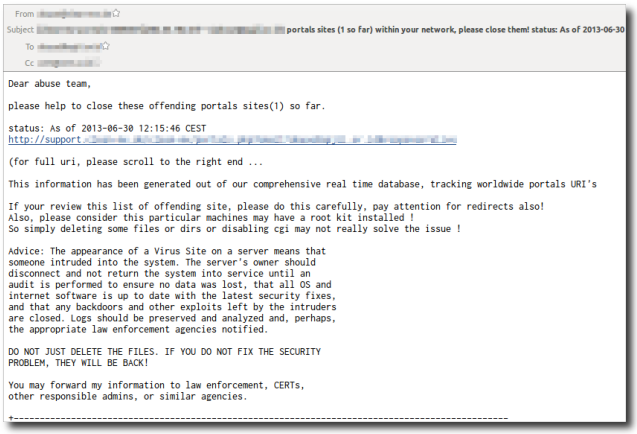
3.200-an hingga 860. *Network incident* mengalami kenaikan 30%, *IPR* stabil dengan jumlah pengaduan hampir sama selama dua bulan, dan *malware* turun sekitar 30%.

Jauh di bawah *spam*, *network incident* berada pada peringkat kedua jumlah pengaduan, sekitar 2.800 pesan (9,36%) dari total pengaduan – bandingkan dengan 80% untuk *spam*. *IPR* menempati posisi ketiga dengan jumlah pengaduan sekitar 1.800 pesan (6,22%), dan *malware* menempati posisi keempat dengan jumlah pengaduan sekitar 700 pesan (2,38%).

Contoh email pengaduan kasus *network incident* ditampilkan di Gambar 6.



Gambar 5. Grafik *network incident*, *IPR*, *malware*



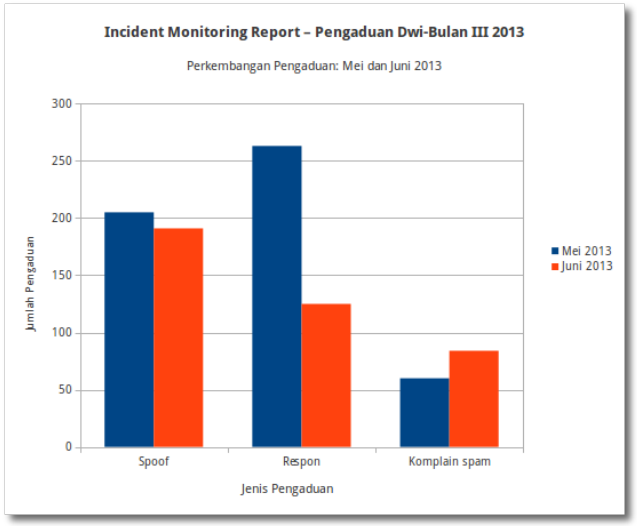
Gambar 6. Contoh pengaduan *network incident*

3.3 Bagian 3: *spoof*, respon, dan komplain *spam*

Pada Bagian 3 pengelompokan pengaduan, yang diisi *spoof*, *respon*, dan komplain *spam*, jumlah pengaduan masing-masing sangat rendah, yakni di bawah 400, dengan demikian bagian ini dapat disebut sebagai "grup empat ratusan".

Dari angka-angka di *Tabel 1* dan *Tabel 2*, terhitung jumlah pengaduan *spoof* sebesar 1,24% dari total pengaduan dan pada periode ini mengalami penurunan sebesar 6,83%. Untuk *respon* terkumpul 1,21% dari total pengaduan dan mengalami penurunan 52,47%. Terakhir untuk *komplain spam* terkumpul 0,45% dan mengalami kenaikan 40%.

Jika dilihat dari pesan pengaduan yang diterima, kelompok



Gambar 7. *Spoof*, respon, komplain *spam*

ketiga ini hasil dari pelaporan non-otomatis, yakni pengaduan yang dikirim pengguna komputer (bukan dari perangkat lunak atau alat bantu).

Dari beberapa kemungkinan akan fenomena di atas, dua hal perlu dipertimbangkan:

1. Pengguna Internet "menyelesaikan sendiri" urusan *spam*, baik menggunakan fasilitas pelaporan yang sudah disediakan layanan (sebagai misal hampir semua layanan email berbasis web sudah menyediakan penandaan "pesan sebagai *spam*") atau membiarkan *spam* ini dengan cukup menghapusnya.

2. ID-CERT perlu terus merangkul pihak-pihak lain untuk sosialisasi mekanisme pengaduan agar dapat menjaring lebih banyak laporan.

4. Rangkuman

Dengan pertimbangan jumlah gangguan berupa *spam* yang masih teratas, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi "pintu gerbang" pengiriman *spam* (terutama lewat email) dan mengantisipasi kedatangan *spam*.

Dalam waktu dua bulan ketiga ini, Mei dan Juni, yang juga merupakan akhir semester I 2013, terjadi peningkatan volume gangguan *spam* dalam jumlah banyak pada bulan kedua. Belum diperoleh korelasi terhadap fenomena yang terjadi di dunia maya, sehingga sampai dengan laporan ini ditulis dicatat sebagai fenomena saja.

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.

[7] Terkait jumlah pengaduan *spam* yang sangat banyak.

5. Ucapan terima kasih

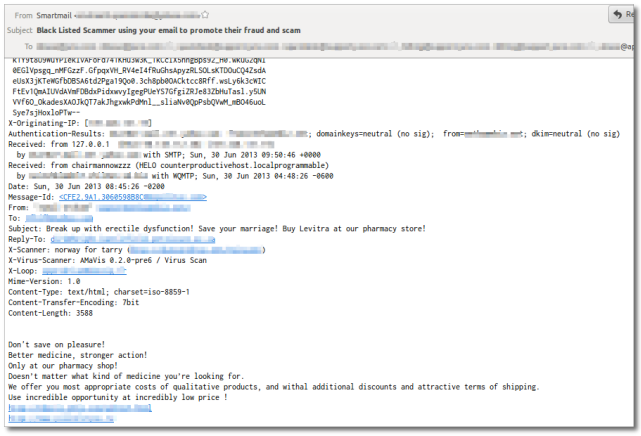
Terima kasih pada seluruh responden yang telah berpartisipasi pada pengumpulan bahan untuk penulisan laporan ID-CERT, yakni:

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

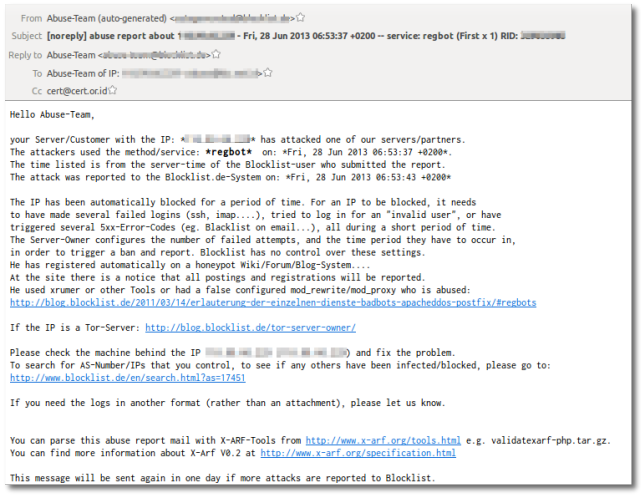
6.1 Contoh beberapa email pengaduan

Contoh email pengaduan *spam* dari dua puluh ribu lebih yang diterima pada bulan Juni 2013.



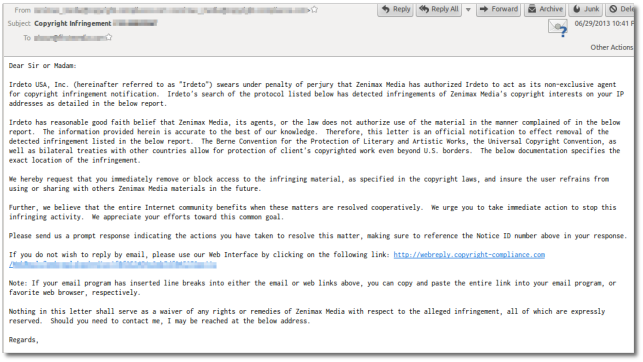
Gambar 8. Contoh email pengaduan spam

Contoh email pengaduan *malware* yang diterima pada bulan Juni 2013.



Gambar 9. Contoh email pengaduan *malware*

Contoh email pengaduan *Intellectual Property Right* yang diterima pada bulan Juni 2013.



Gambar 10. Contoh email pengaduan *Intellectual Property Right* (IPR)