Laporan Dwi Bulan V 2013

ID-CERT[1]

Ringkasan
Di laporan Dwi Bulan V 2013 ini disajikan hasil pengumpulan pengaduan selama dua bulan, September dan Oktober 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 3 Januari 2014*

Daftar Isi

1 Pendahuluan **1**
2 Metoda **2**
3 Uraian **3**
3.1 Bagian 1: *spam*, *malware*, dan *network incident* 4
3.2 Bagian 2: *IPR*, *spoof*, dan komplain *spam* 5
4 Rangkuman **5**
4.1 Rekomendasi 5
5 Ucapan terima kasih **6**
6 Lampiran **6**
6.1 Kasus penamaan domain dan *malware* 6
6.2 Contoh beberapa email pengaduan 6

1. Pendahuluan

Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi 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, September dan Oktober 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 V 2013 ini, *spam* menempati jumlah pengaduan terbanyak, sampai dengan empat kali lipat total pengaduan lainnya. Fenomena lainnya adalah penurunan jumlah pengaduan dari September ke Oktober.

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.

[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`

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, bulan September dan Oktober 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.

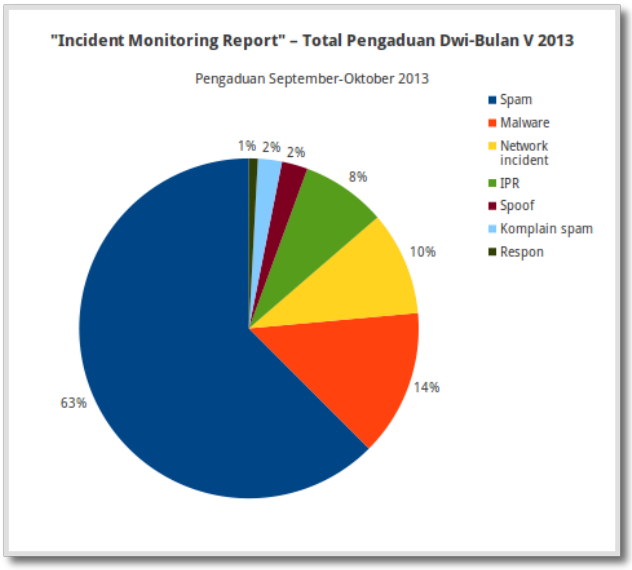
Grafik semua kategori *Incident Monitoring Report* untuk Dwi Bulan V 2013 berdasarkan jumlah pengaduan per bulan ditampilkan pada *Gambar 1*.

Jumlah pengaduan masing-masing dapat dilihat dengan lebih seksama di *Tabel 1* dengan kategori pengaduan ditampilkan berdasarkan urutan abjad. Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama, September, dan bernilai negatif jika terjadi penurunan. Secara umum terjadi penurunan jumlah pengaduan pada bulan Oktober dibanding September walaupun tetap landai, sehingga hampir merata.

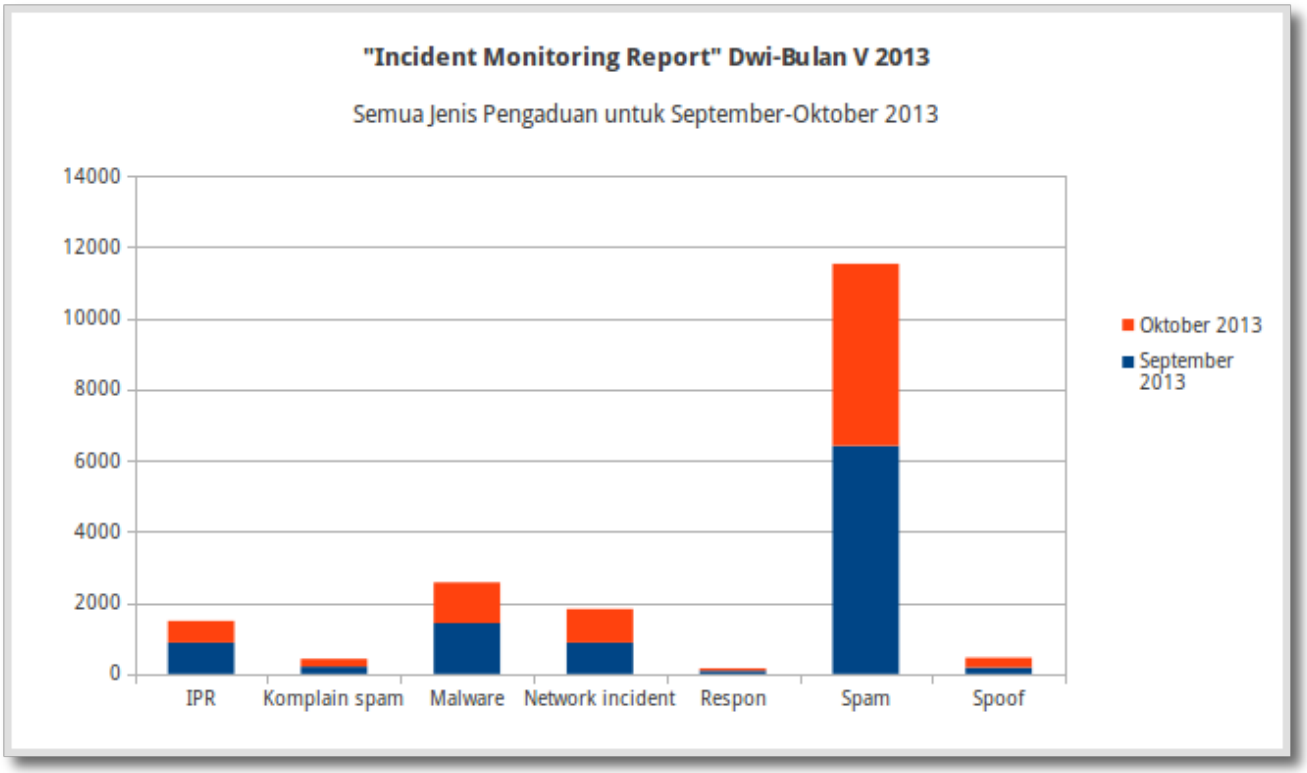
Kategori	September	Oktober	Perkembangan
IPR	877	613	−30,10%
Komplain spam	207	2.16	4,35%
Malware	1.428	1.143	−19,96%
Network incident	878	944	7,52%
Spam	6.410	5.118	−20,16%
Spoof	181	273	50,83%

Table 1. Perkembangan jenis pengaduan selama September dan Oktober 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*.



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



Gambar 1. *Incident Monitoring Report* Dwi Bulan V 2013 untuk semua kategori

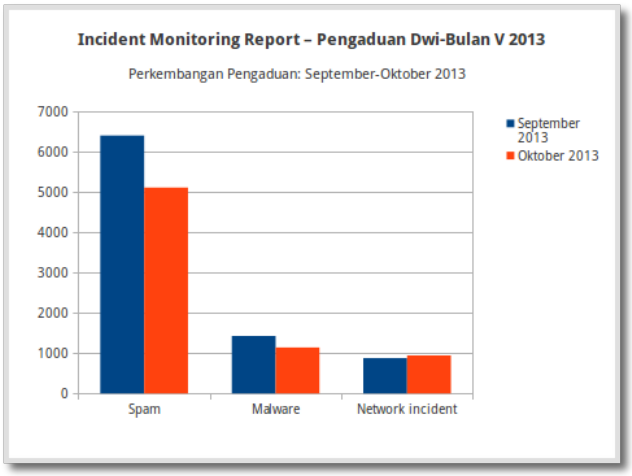
Jenis	September	Oktober	Total	Persentase
Spam	6.410	5.118	11.528	62,51%
Malware	1.428	1.143	2.571	13,94%
Network incident	878	944	1.822	9,88%
IPR	877	613	1.490	8,08%
Spoof	181	273	454	2,46%
Komplain *spam*	207	216	423	2,29%

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

3.1 Bagian 1: *spam*, *malware*, dan *network incident*

Pada periode September-Oktober 2013 ini, jumlah pengaduan terbanyak adalah kategori *spam* dengan jumlah 11.528 atau 62,51% dari total pengaduan. Dengan jumlah lebih dari separuh pengaduan, *spam* mendominasi pengaduan dan terlihat angka tsb. di atas empat kali kategori berikutnya.

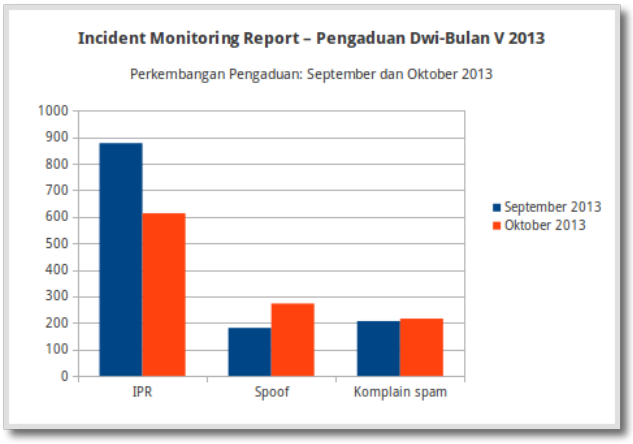
Terjadi penurunan jumlah pengaduan pada dua kategori terbanyak pertama, *spam* dan *malware*. Terlihat perbedaan yang mencolok pada jumlah pengaduan dari *spam* yang menduduki peringkat pertama dan *malware* pada peringkat kedua. Pada peringkat ketiga, yakni *network incident*, terjadi peningkatan jumlah pengaduan.



Gambar 3. Jumlah pengaduan *spam*, *malware*, dan *network incident* untuk September-Oktober 2013

3.2 Bagian 2: *IPR*, *spoof*, dan komplain *spam*

Kelompok kedua pengaduan diawali oleh *IPR* dengan total pengaduan 1.490 atau 8,08%, diikuti oleh *spoof* dan komplain *spam*, masing-masing dengan persentase sedikit lebih dari 2%.



Gambar 4. Jumlah pengaduan *IPR*, *spoof*, dan komplain *spam*

Jika dilihat dari pesan pengaduan yang diterima, kelompok 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 pengaduan *spam* masih tertinggi, 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 keempat ini, September dan Oktober, jumlah pengaduan *spam* sangat dominan dibanding kategori lainnya dan terjadi penurunan pada bulan kedua.

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[6] secara intensif dalam periode lama atau berulang-ulang.
4. Administrator jaringan memblokir semua *port* akses ke Internet, kecuali untuk *port* yang dianggap diperlukan.

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

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

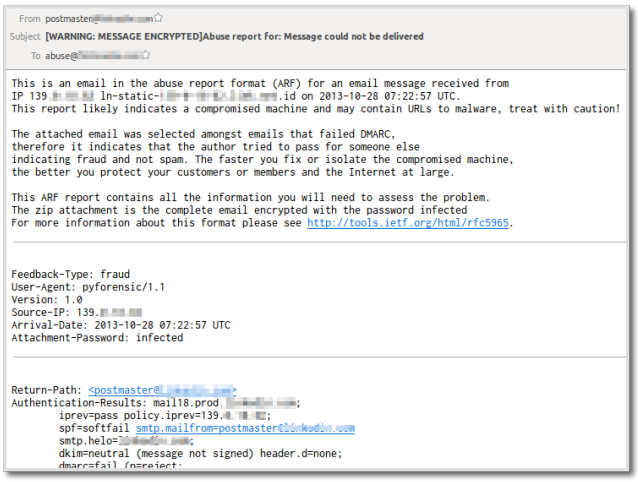
6.1 Kasus penamaan domain dan *malware*

Salah satu laporan pengaduan menarik diterima pada akhir September lalu, yaitu adanya nama domain yang hampir sama di salah satu instansi pemerintah (domain `go.id`). Perbedaan kedua nama domain tsb. hanya pada satu huruf penanda instansi tsb. di daerah, sehingga berpotensi menimbulkan kerancuan. Pengaduan tsb. sudah ditindaklanjuti dengan meneruskannya ke pengelola nama domain `id` dan instansi yang memiliki kewenangan pengaturan nama domain untuk instansi pemerintah.

Hal lain dalam pengaduan adalah adanya *malware* di situs web tsb. dan lebih-lebih situs web ini milik instansi pemerintah –berdomain `id`– menjadi kewajiban untuk segera diperbaiki.

6.2 Contoh beberapa email pengaduan

Berikut contoh beberapa email pengaduan yang diterima pada periode September-Oktober 2013.


From postmaster
Subject [WARNING: MESSAGE ENCRYPTED]Abuse report for: Message could not be delivered
To abuse@

This is an email in the abuse report format (ARF) for an email message received from
IP 139. on 2013-10-28 07:22:57 UTC.
This report likely indicates a compromised machine and may contain URLs to malware, treat with caution!

The attached email was selected amongst emails that failed DMARC,
therefore it indicates that the author tried to pass for someone else
indicating fraud and not spam. The faster you fix or isolate the compromised machine,
the better you protect your customers or members and the Internet at large.

This ARF report contains all the information you will need to assess the problem.
The zip attachment is the complete email encrypted with the password infected
For more information about this format please see http://tools.ietf.org/html/rfc5965.

Feedback-Type: fraud
User-Agent: pyforensic/1.1
Version: 1.0
Source-IP: 139.
Arrival-Date: 2013-10-28 07:22:57 UTC
Attachment-Password: infected

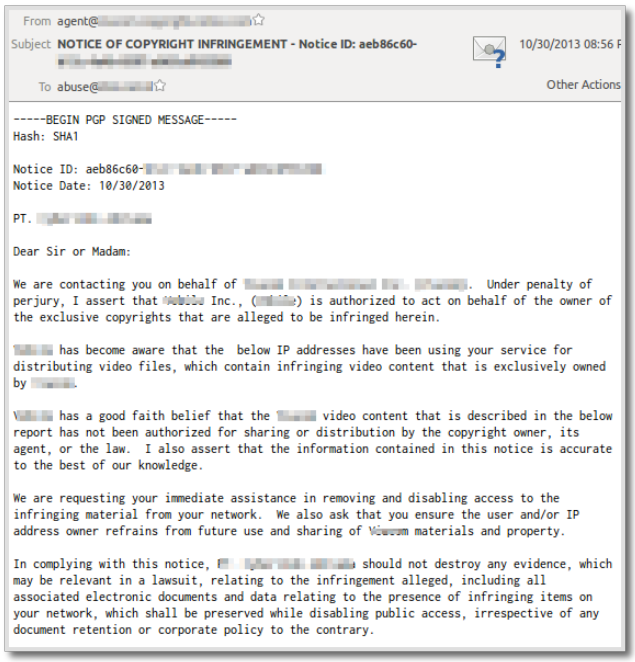
Return-Path: <postmaster@
Authentication-Results: mail18.prod.;
iprev=pass policy.iprev=139.;
spf=softfail smtp.mailfrom=postmaster@
smtp.helo=;
dkim=neutral (message not signed) header.d=none;
dmarc=fail (p=reject;

Gambar 5. Contoh pengaduan *malware*

Pada penjelasan email disebutkan adanya kemungkinan pesan dalam email tsb. berisi tautan (*link*) berisi *malware*. Pengaduan seperti ini dihasilkan secara otomatis oleh aplikasi di server penerima.

Email pengaduan *IPR* di atas dibuat dalam bentuk teguran akan dugaan adanya materi yang melanggar hak cipta yang dapat diakses oleh publik pada server.

Contoh pengaduan di atas ditulis sebagai laporan saksi mata akan adanya gangguan yang termasuk kategori *network incident*. Pengaduan ini juga menjadi contoh partisipasi warga pengguna Internet di Indonesia yang berpartisipasi melaporkan gangguan ke ID-CERT.



From agent@

Subject **NOTICE OF COPYRIGHT INFRINGEMENT - Notice ID: aeb86c60-**

10/30/2013 08:56 F

To abuse@

Other Actions

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Notice ID: aeb86c60-
Notice Date: 10/30/2013

PT.

Dear Sir or Madam:

We are contacting you on behalf of . Under penalty of perjury, I assert that Inc., ( ) is authorized to act on behalf of the owner of the exclusive copyrights that are alleged to be infringed herein.

has become aware that the below IP addresses have been using your service for distributing video files, which contain infringing video content that is exclusively owned by .

has a good faith belief that the video content that is described in the below report has not been authorized for sharing or distribution by the copyright owner, its agent, or the law. I also assert that the information contained in this notice is accurate to the best of our knowledge.

We are requesting your immediate assistance in removing and disabling access to the infringing material from your network. We also ask that you ensure the user and/or IP address owner refrains from future use and sharing of materials and property.

In complying with this notice, should not destroy any evidence, which may be relevant in a lawsuit, relating to the infringement alleged, including all associated electronic documents and data relating to the presence of infringing items on your network, which shall be preserved while disabling public access, irrespective of any document retention or corporate policy to the contrary.

Gambar 6. Contoh pengaduan *IPR*

Date: Fri, 18 Oct 2013 23:04:06 +0700
Subject: SQL Injection vulnerability di
From: "
To: @cert.or.id
User-Agent: SquirrelMail/1.4.23 [SVN]
MIME-Version: 1.0
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal

Ditemukan SQL Injection di situs tepatnya di url

/detail_informasi.php?id=11'

Gambar 7. Contoh pengaduan *network incident*