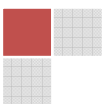
Incident Monitoring Report - 2016

Laporan Dwi Bulanan IV 2016

Bulan Juli dan Agustus 2016

Agustus 2016

Daftar Isi



1. Pendahuluan

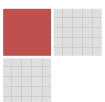
Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi lebih penting, dari komunikasi antar warga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lanjut usia, para pekerja di lapangan hingga *bot otomatis.* Batas-batas yang telah ada sebelumnya juga mengalami pergeseran dengan adanya Internet, menciptakan kemungkinan baru yang perlu dicermati. Seiring dengan perkembangan yang demikian pesatnya, terutama penyalahgunaan dan kejahatan melalui internet, maka aspek keamanan Internet (*Internet security*) juga menjadi sisi yang perlu secara khusus menjadi perhatian dan kerja sama banyak kalangan.

Sebagai bagian dari pemantauan keamanan Internet, ID-CERT[1] juga telah mengadakan kerjasama dengan beberapa pihak serta menerima pengaduan lewat email yang diterima dari beberapa responden. Dari pengaduan yang masuk tersebut dilakukan pengelompokan 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 2016.

Selain gambaran tersebut, penyediaan laporan ini juga dimaksudkan sebagai contoh data primer keamanan teknologi informasi (TI) di Indonesia.

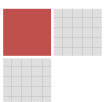
Penting ditekankan dalam hal ini adalah tindak lanjut terhadap laporan tentang penyalahgunaan Internet (*Internet abuse*) sebagai respon positif dan langkah untuk memperbaiki keadaan. Hal ini juga bagian interaksi positif antara kita, pengguna Internet di Indonesia dengan pihak-pihak di mancanegara terkait penanganan laporan. Pengaduan yang diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antar lembaga, dan untuk membantu penyusunan rencana ke depan.

[1] Indonesia Computer Emergency Response Team



Pada laporan Dwi Bulanan IV 2016 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 72,02%, sedangkan Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) menempati urutan pengaduan kedua dengan persentase jumlah pengaduan sebesar 12,46%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: *Spam* pada kelompok pertama yang mencapai jumlah di atas 10.000 pengaduan, diikuti Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR), Komplain Spam, dan *Network Incident* pada kelompok ke dua yang memiliki jumlah pelaporan sedang yaitu di bawah 10.000 di atas 1.000 laporan, dan *Spoofing/Phishing*, Respon, dan *Malware* pada kelompok terakhir berjumlah pengaduan rendah yaitu di bawah 1.000 pengaduan. Penjelasan lengkap tentang ketiga kelompok tersebut dipaparkan di bagian Uraian.

Pembuatan laporan ini berdasarkan pada data-data yang diperoleh dan diambil dari 39 (tiga puluh sembilan) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), 3 (tiga) operator telekomunikasi, 7 (tujuh) NAP, 22 (dua puluh dua) Penyedia Jasa Internet (PJI/ISP), dan KEMDIKBUD.



2. Metoda

Penyusunan dokumen Dwi Bulan IV ini mengambil data 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 dalam beberapa kategori sebagai berikut:

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

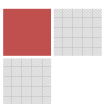
Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR).

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.

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



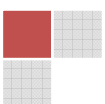
Respon Respon terhadap laporan yang masuk.

Spam Penggunaan sistem pengolahan 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 yang di atas.

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



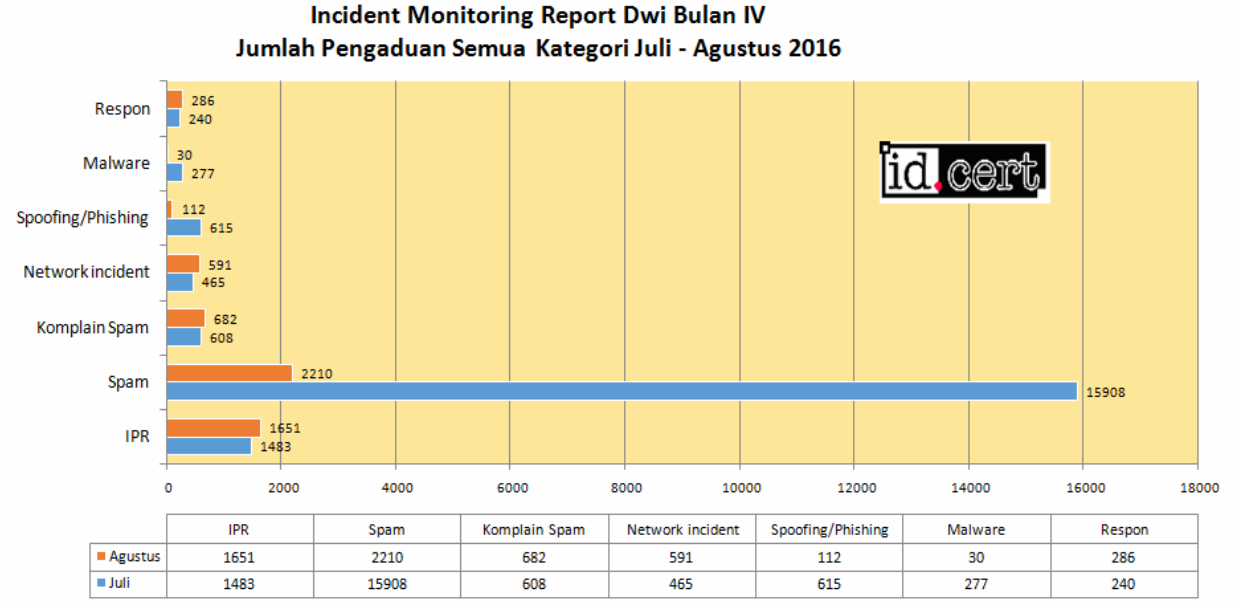
3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan penerimaan laporan, dengan demikian terdapat dua kelompok besar, bulan Juli dan Agustus 2016. Kategori pengaduan terdiri atas Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR), komplain spam, *malware*, *network incident*, respon, *spam*, dan *spoofing/phishing*.

Pengolahan data dilakukan dengan dua cara:

1. Penghitungan jumlah dari *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 jumlah dari isi (*body*) email. 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 2016 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



	IPR	Spam	Komplain Spam	Network incident	Spoofing/Phishing	Malware	Respon
Agustus	1651	2210	682	591	112	30	286
Juli	1483	15908	608	465	615	277	240

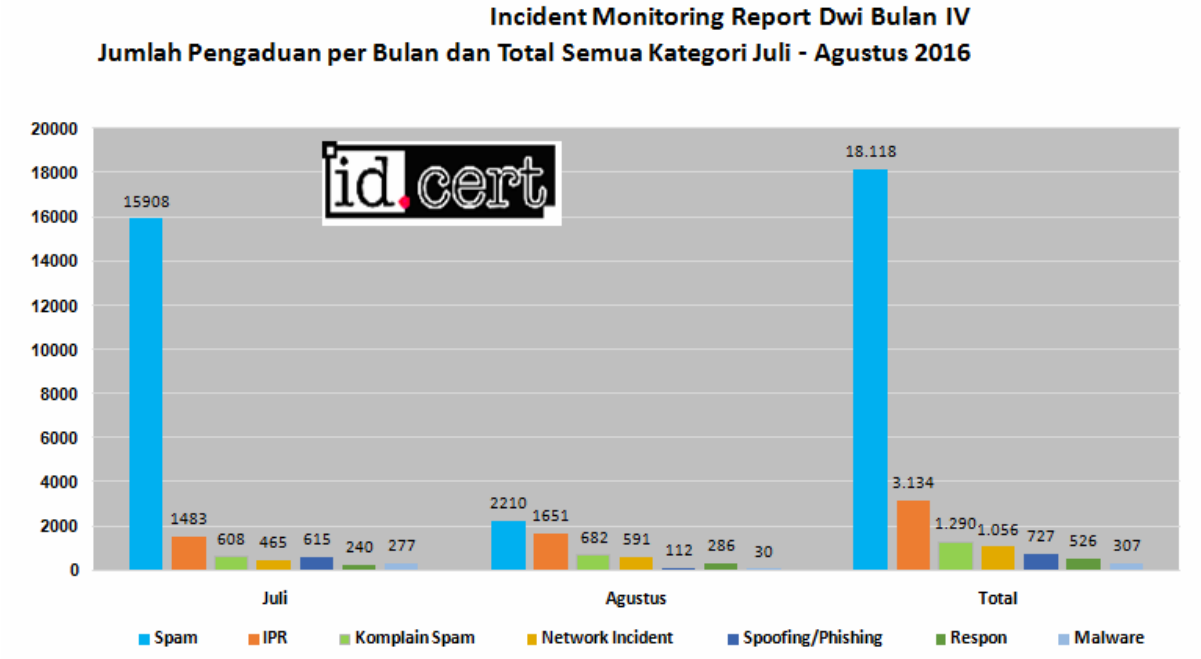
Gambar 1. Jumlah pengaduan semua kategori Juli - Agustus 2016

Jumlah pengaduan masing-masing per bulan dan total dua bulan dapat dilihat lebih seksama di Tabel 1 dengan kategori pengaduan ditampilkan berdasarkan jumlah laporan yang tertinggi ke terendah.

Tabel 1. Perkembangan jenis pengaduan selama Juli - Agustus 2016

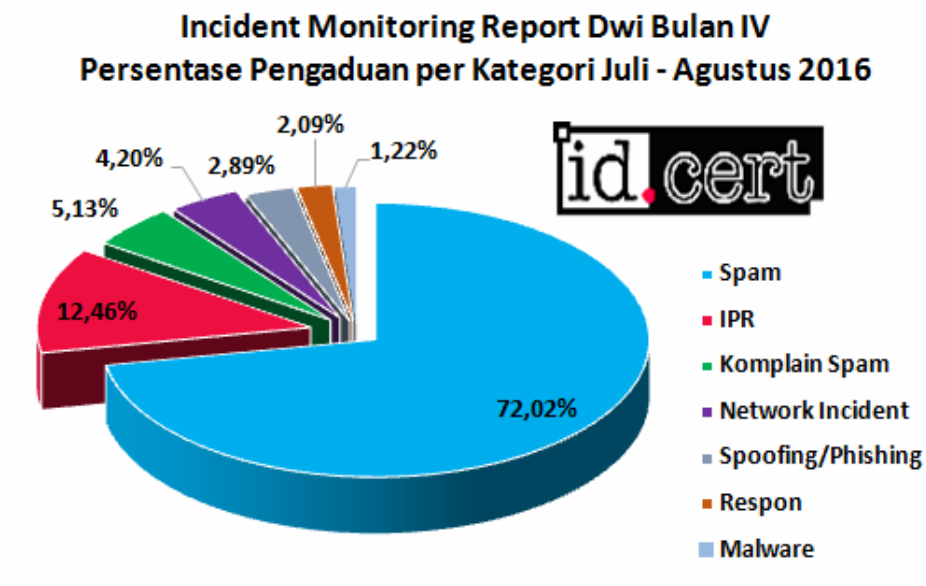
Kategori	Juli	Agustus	Total	%
Spam	15908	2210	18.118	72,02%
IPR	1483	1651	3.134	12,46%
Komplain Spam	608	682	1.290	5,13%
Network Incident	465	591	1.056	4,20%
Spoofing/Phishing	615	112	727	2,89%
Respon	240	286	526	2,09%
Malware	277	30	307	1,22%

Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Juli - Agustus 2016 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori Juli - Agustus 2016

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Juli, bulan kedua Agustus dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan IV ini yaitu masing-masing kategori sebagian mengalami peningkatan dan sebagian mengalami penurunan jumlah pengaduan pada bulan Agustus. Persentase detail dari masing-masing, dihitung terhadap jumlah pengaduan keseluruhan dapat dilihat pada Tabel 1. Tampilan tabel tersebut berdasarkan urutan persentase kategori dari yang terbanyak. Untuk melihat perbandingan besar persentase jumlah laporan antar semua kategori ditampilkan dalam bentuk diagram lingkaran yang disajikan pada Gambar 3.



Gambar 3. Persentase pengaduan per kategori Dwi Bulan IV 2016

Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

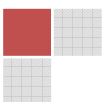
Tabel 2. Perkembangan jumlah pengaduan dalam persentase

Kategori	Juli	Agustus	%
Network incident	465	591	27,10%
Respon	240	286	19,17%
Komplain Spam	608	682	12,17%
IPR	1483	1651	11,33%
Spoofing/Phishing	615	112	-81,79%
Spam	15908	2210	-86,11%
Malware	277	30	-89,17%

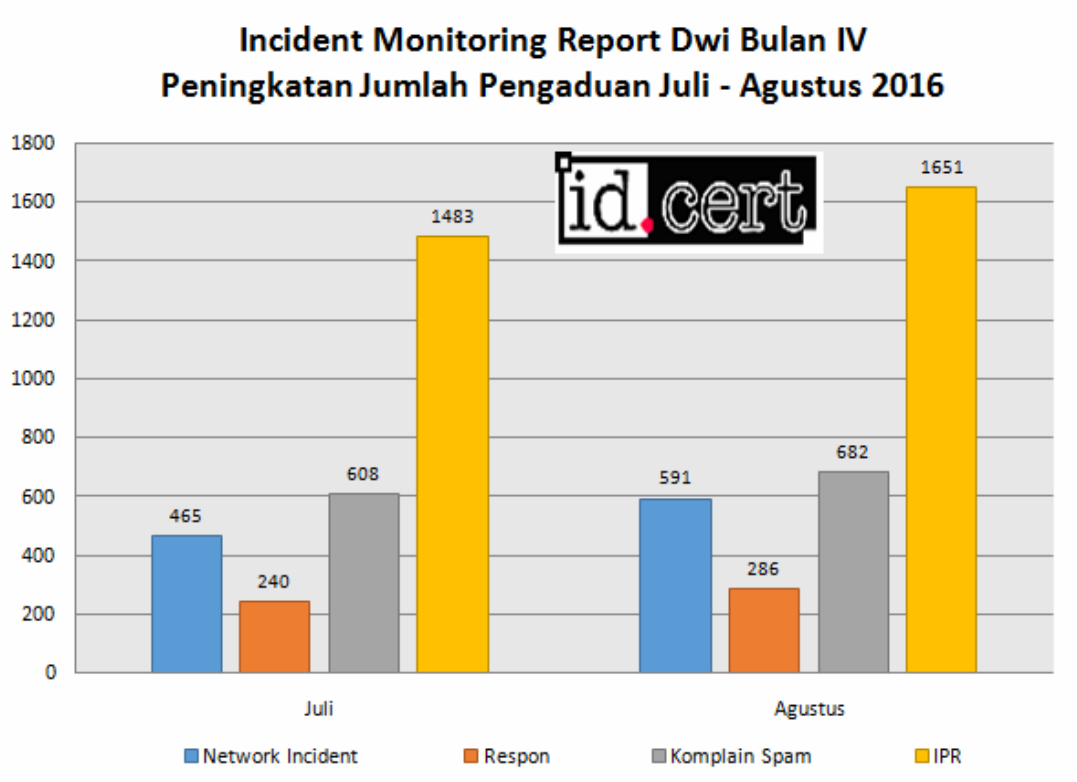
3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, terdapat kategori yang mengalami peningkatan jumlah pengaduan yaitu:

1. *Network Incident* pada bulan Juli berjumlah 465 pengaduan dan meningkat sebesar 27,1% di bulan Agustus dengan jumlah *Network Incident* sebanyak 591 pengaduan.
2. Respon memiliki jumlah 240 pada bulan Juli dan mengalami peningkatan sebesar 19,17% di bulan Agustus dengan jumlah sebanyak 286.
3. Komplain Spam memiliki jumlah pengaduan sejumlah 608 di bulan Juli. Pada bulan Agustus, terjadi peningkatan jumlah pengaduan dibandingkan dengan bulan Juli dengan persentase peningkatan sebesar 12,17% dengan jumlah 682 pengaduan.
4. Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) memiliki jumlah pengaduan sebanyak 1.483 pada bulan Juli dan naik sebesar 11,33% di bulan Agustus dengan jumlah pengaduan sebanyak 1.651.



Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.

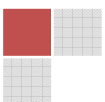


Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Juli - Agustus 2016

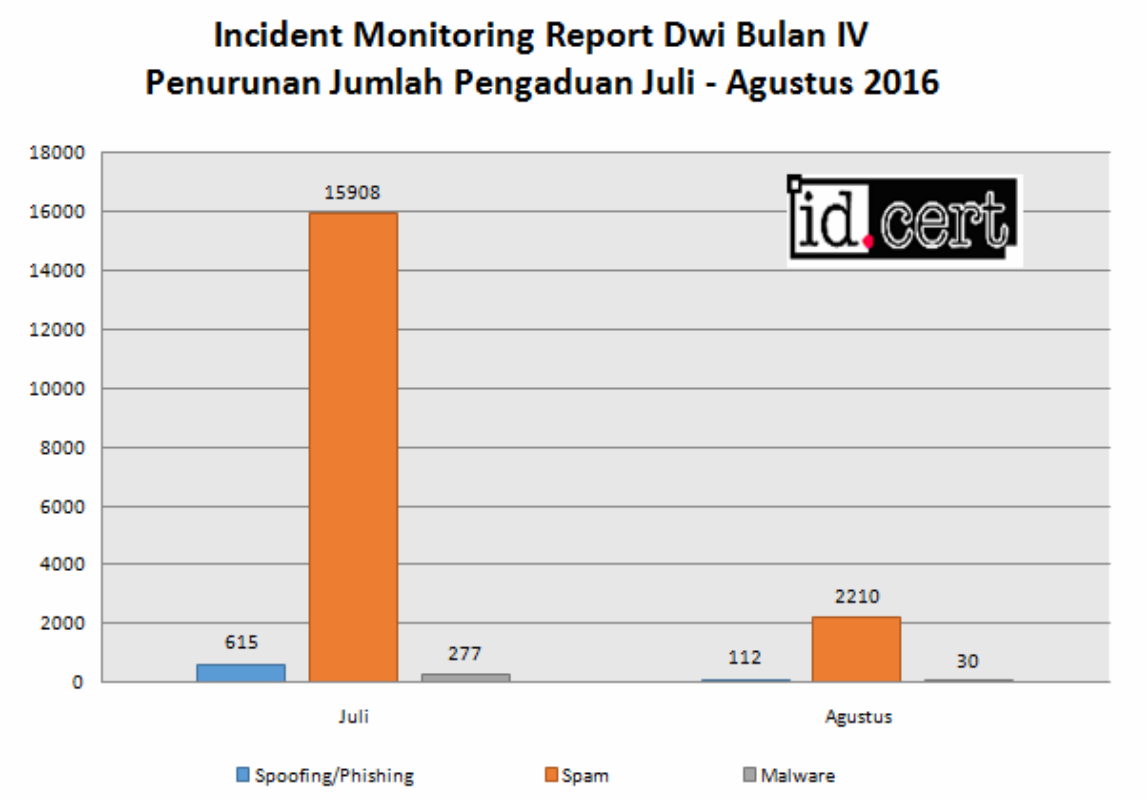
3.2 Kelompok Pengaduan yang Mengalami Penurunan

Bulan Juli - Agustus terdapat kategori yang mengalami penurunan jumlah pengaduan di bulan kedua yaitu:

1. *Spoofing/Phishing* mengalami penurunan jumlah pengaduan dari bulan Juli ke Agustus, dari 615 turun ke 112. Persentase penurunannya mencapai 81,79%.
2. *Spam* mengalami penurunan jumlah pengaduan yang tinggi untuk bulan Juli dan Agustus ini. *Spam* memiliki jumlah pengaduan sebanyak 15.908 pada bulan Juli dan turun sebesar 86,11% di bulan Agustus dengan jumlah pengaduan sebanyak 2.210.
3. *Malware* mengalami penurunan jumlah pengaduan di bulan Mei sebanyak 277 dan di bulan Agustus sebanyak 30. Persentase penurunan jumlah pengaduan dari bulan Juli ke Agustus mencapai 89,17%.



Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Juli - Agustus 2016

Jika dilihat dari pesan pengaduan yang diterima, pengaduan ini diterima dari pelaporan non-otomatis, yakni pengaduan yang dikirim oleh 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* yang masih sangat tinggi, 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*.

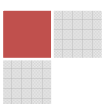
Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) juga termasuk tinggi jumlah aduannya. Perlu untuk lebih aktif lagi memonitor situs-situs atau laman-laman yang memuat penjualan on-line untuk barang-barang bermerk.

Dilihat dari volume pengaduan yang masuk, yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet menjadi tanggung jawab pihak-pihak terkait dengan bahan laporan tersebut 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

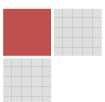
Sejumlah rekomendasi yang dapat dipertimbangkan:

1. Perangkat lunak anti-spam dipasang di server email sebagai antisipasi pengiriman pesan *spam* dari jaringan lokal ke Internet.
2. Perangkat lunak antivirus dan perangkat lunak keamanan dipasang untuk mengurangi risiko terinfeksi *malware*. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara tertatur.
3. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, misalnya 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.



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 yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.

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



5. Ucapan Terima Kasih

Laporan ini bisa disajikan karena adanya partisipasi dari beberapa pihak dalam hal pengumpulan bahan untuk penulisan laporan ID-CERT, yakni:

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