

Laporan Dwi Bulan V 2014

September – Oktober

Ringkasan

Di Laporan Dwi Bulan V ini disajikan pengumpulan pengaduan selama dua bulan yaitu September dan Oktober 2014. Pengaduan tersebut 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/phishing, dan malware merupakan kategori yang dipilih untuk pengelompokan pengaduan masuk.

Kata Kunci

Security – Pelaporan – Laporan Dwi Bulan

ID-CERT¹

¹ Indonesian Computer Emergency Response Team



Daftar Isi

1. Pendahuluan.....	2
2. Metoda	3
3. Uraian.....	3
3.1 Kelompok pengaduan yang mengalami peningkatan.....	5
3.2 Kelompok pengaduan yang mengalami penurunan.....	5
4. Rangkuman	6
4.1 Rekomendasi.....	6
5. Ucapan Terima Kasih.....	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 menerima pengaduan lewat email yang diterima dari beberapa responden. Pengaduan tersebut 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 2014.

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.

Pada laporan Dwi Bulanan V 2014 ini, *spam* masih menempati jumlah pengaduan terbanyak yaitu mencapai 47,74%, sedangkan IPR menempati urutan pengaduan kedua dengan selisih sekitar 28% dari *spam* yaitu sebesar 19,67%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: *spam* pada kelompok pertama yang mencapai jumlah di atas 10.000 pengaduan, diikuti kelompok ke dua yang memiliki jumlah pelaporan sedang yaitu di bawah 10.000 di atas 1.000 laporan, dan 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 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 Internet (PJI/ISP), Kemendikbud.

2. Metoda

Penyusunan dokumen Dwi Bulan 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 dikelompokkan oleh responden

Dari laporan yang sudah terkumpul, dilakukan pengelompokan sebagai berikut:

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain² 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 jahat³.

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 pengolahan pesan elektronik untuk mengirim pesan-pesan tidak diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih⁴.

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna⁵.

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

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, bulan September dan Oktober 2014. 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 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*

² *Fraud*,

<http://en.wikipedia.org/wiki/Fraud>

³ *Malware*,

<http://en.wikipedia.org/wiki/Malware>

⁴ *Spam (electronic)*,

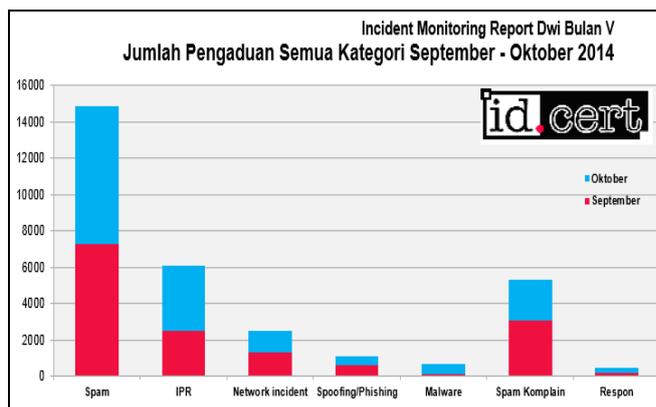
[http://en.wikipedia.org/wiki/Spam_\(electronic\)](http://en.wikipedia.org/wiki/Spam_(electronic))

⁵ *Spoofing attack*,

http://en.wikipedia.org/wiki/Spoofing_attack

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 2014 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



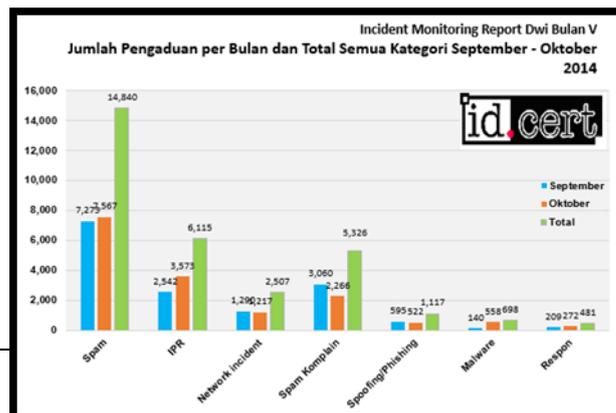
Gambar 1 Jumlah pengaduan semua kategori September - Oktober 2014

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 diakhiri dengan Respon.

Tabel 1. Perkembangan jenis pengaduan selama September - Oktober 2014

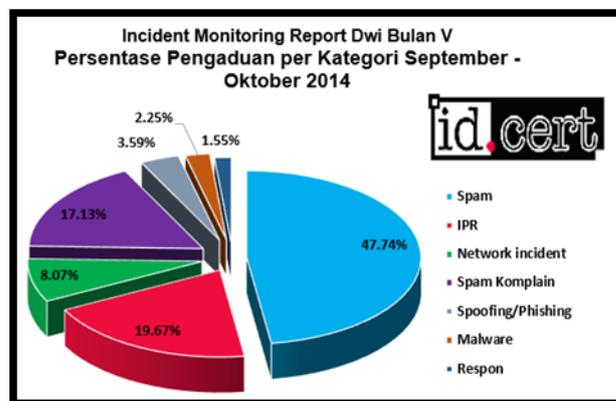
Kategori	September	Oktober	Total	%
Spam	7,273	7,567	14,840	47.74%
IPR	2,542	3,573	6,115	19.67%
Spam Komplain	3,060	2,266	5,326	17.13%
Network incident	1,290	1,217	2,507	8.07%
Spoofing/Phishing	595	522	1,117	3.59%
Malware	140	558	698	2.25%
Respon	209	272	481	1.55%

Pada Gambar 2 dapat dilihat perkembangan dari naik atau turunnya jumlah pengaduan antara bulan September dan Oktober 2014 dan jumlah total dua bulan.



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori September - Oktober 2014

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama September, bulan kedua Oktober dan bernilai negatif jika terjadi penurunan. Secara umum tidak ada tren yang terjadi dari jumlah pengaduan September di banding Oktober karena masing-masing kategori ada yang meningkat yaitu *Malware*, *IPR*, *Spam*, *Respon* tetapi ada pula yang menurun yaitu *Spam Komplain*, *Spoofing/Phishing*, *Network Incident*. Persentase detail dari masing-masing, dihitung terhadap jumlah pengaduan keseluruhan dapat dilihat pada **Error! Reference source not found.** 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 V 2014

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

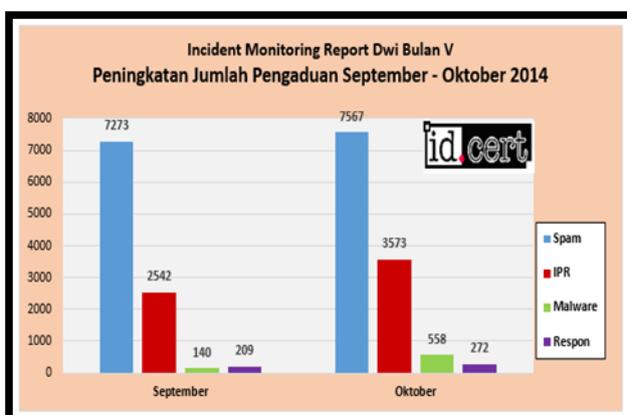
Kategori	September	Oktober	%
Spam	7273	7567	4.04%
IPR	2542	3573	40.56%
Network incident	1290	1217	-5.66%
Spoofing/Phishing	595	522	-12.27%
Malware	140	558	298.57%
Spam Komplain	3060	2266	-25.95%
Respon	209	272	30.14%

Tabel 2 Perkembangan jumlah pengaduan dalam persentase

3.1 Kelompok pengaduan yang mengalami peningkatan

Ada beberapa kategori yang mengalami peningkatan jumlah pengaduan pada September – Oktober yaitu :

Spam dari 7273 pada September menjadi 7567 di Oktober mengalami peningkatan 4,04%, IPR dari 2542 pada September menjadi 3573 di Oktober mengalami peningkatan 40,56%, Malware dari 140 pada September menjadi 558 di Oktober mengalami peningkatan 298,57%, dan Respon dari 209 pada September menjadi 272 di Oktober mengalami peningkatan 30,14%, seperti disajikan pada Gambar 4 di bawah.

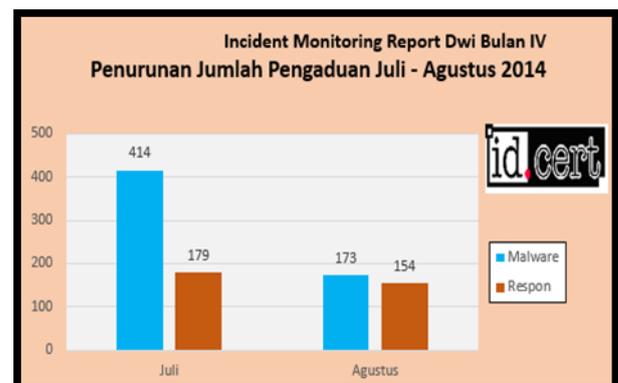


Gambar 4 Peningkatan jumlah pengaduan dari September – Oktober 2014

3.2 Kelompok pengaduan yang mengalami penurunan

Dari sekian banyak kategori pengaduan terdapat dua kategori yang mengalami penurunan jumlah pengaduan yaitu :

Network Incident yang mempunyai jumlah pengaduan sebesar 1290 di September turun menjadi 1217 di Oktober mengalami penurunan sebesar 5,66%. Kemudian, *Spoofing/Phishing* juga mengalami penurunan sebesar 12,27% dari 595 pada bulan September turun menjadi 522 di bulan Oktober. Spam Komplain juga mengalami penurunan sebesar 25,95% dengan jumlah pengaduan pada bulan September sebesar 3060 dan Oktober sebesar 2266. Grafik penurunan pengaduan tersebut disajikan pada Gambar 5 berikut.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan September – Oktober 2014

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 menjangkau 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*.

Pada bulan September dan Oktober ini, jumlah pengaduan *spam* sangat dominan dibanding kategori lainnya meskipun 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 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 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, misalnya akses ke port email/Postfix⁶ 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.

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. Kementerian Komunikasi dan Informatika (Kominfo)

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_\(software\)](http://en.wikipedia.org/wiki/Postfix_(software))

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. Kemendikbud