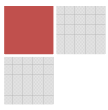
Incident Monitoring Report - 2017

Laporan Dwi Bulan IV 2017

Bulan Juli dan Agustus 2017

September 2017

Daftar Isi



1. Pendahuluan

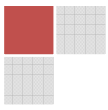
Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi lebih penting, dari komunikasi antar warga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lanjut usia, para pekerja di lapangan 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 2017.

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 Bulan IV 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 43,09% atau berjumlah total 15.233 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam,* HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)), *Network Incident, Spoofing/Phishing,* dan Komplain *Spam* pada kelompok pertama yang memiliki jumlah pelaporan di atas 1.000 laporan, dan Respon dan *Malware* pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 1.000 pengaduan. Penjelasan lengkap tentang kedua kelompok tersebut dipaparkan di bagian Uraian.

Pembuatan laporan ini berdasarkan pada data-data yang diperoleh dan diambil dari 41 (empat puluh satu) responden yang diantaranya terdiri dari: Kominfo, ID-CERT, PANDI, APJII, Detik.net, Zone-h, Anti Fraud Command Center (AFCC), dan Kaspersky, 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 menjadi kategori berikut ini:

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

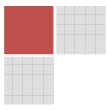
Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR).

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`



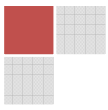
Respon Respon terhadap laporan yang masuk.

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`



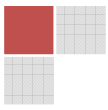
3. Uraian

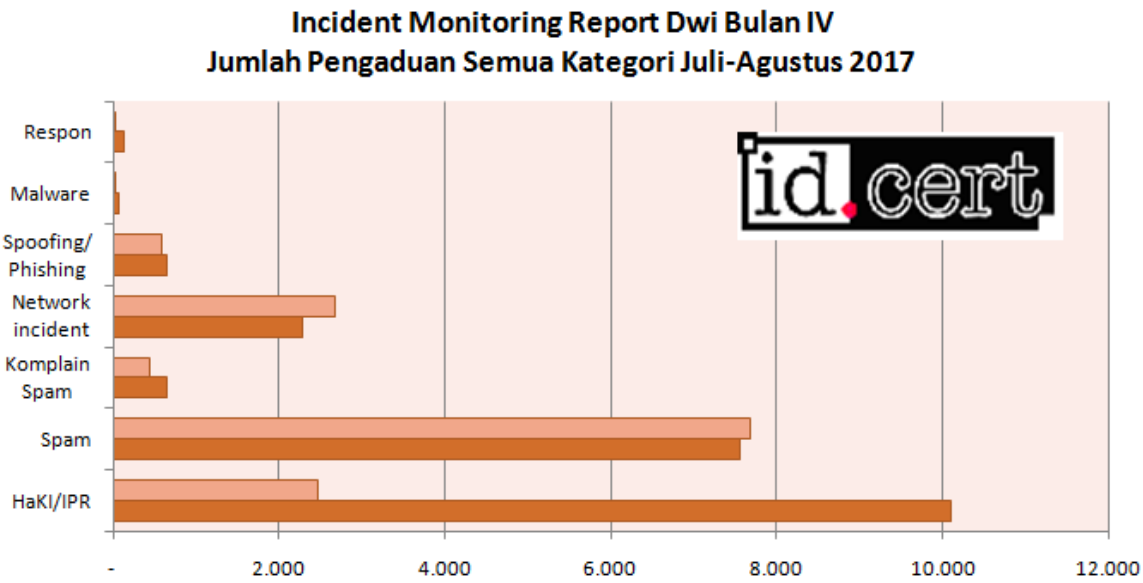
Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, yaitu bulan Juli dan Agustus 2017. Kategori pengaduan terdiri atas *Spam,* HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)), *Network Incident, Spoofing/Phishing,* Komplain *Spam*, Respon, dan *Malware*.

Pengolahan data dilakukan dengan dua cara, yaitu:

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 2017 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1 di bawah ini.





	HaKI/IPR	Spam	Komplain Spam	Network incident	Spoofing/ Phishing	Malware	Respon
Juli	2.475	7.672	449	2.674	591	22	12
Agustus	10.101	7.561	650	2.288	648	71	134

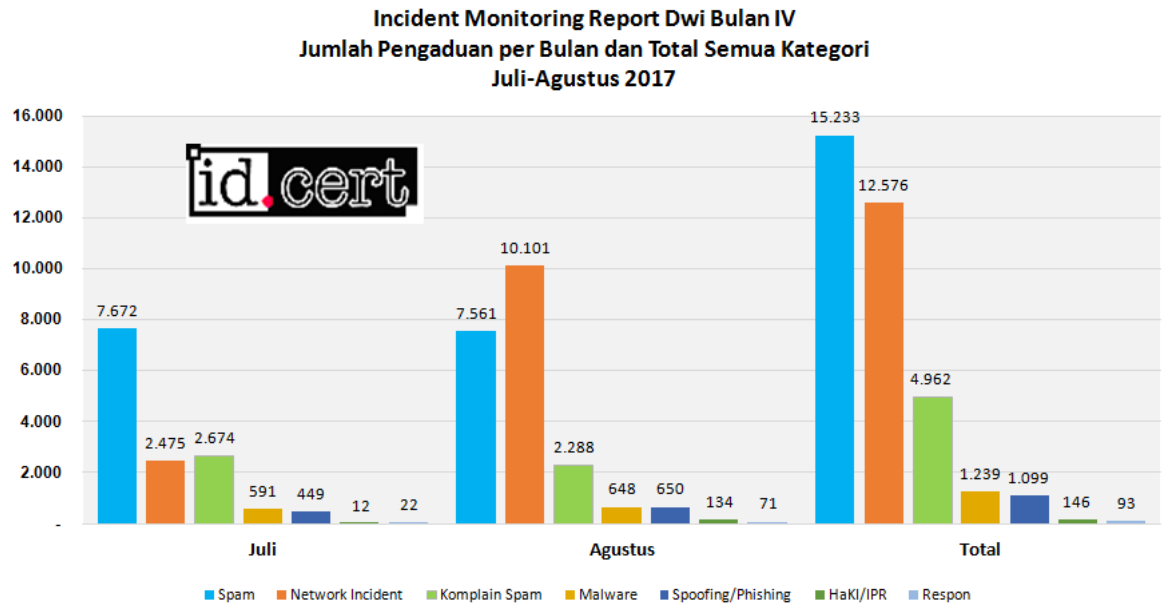
Gambar 1 Jumlah pengaduan semua kategori Juli-Agustus 2017

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 2017

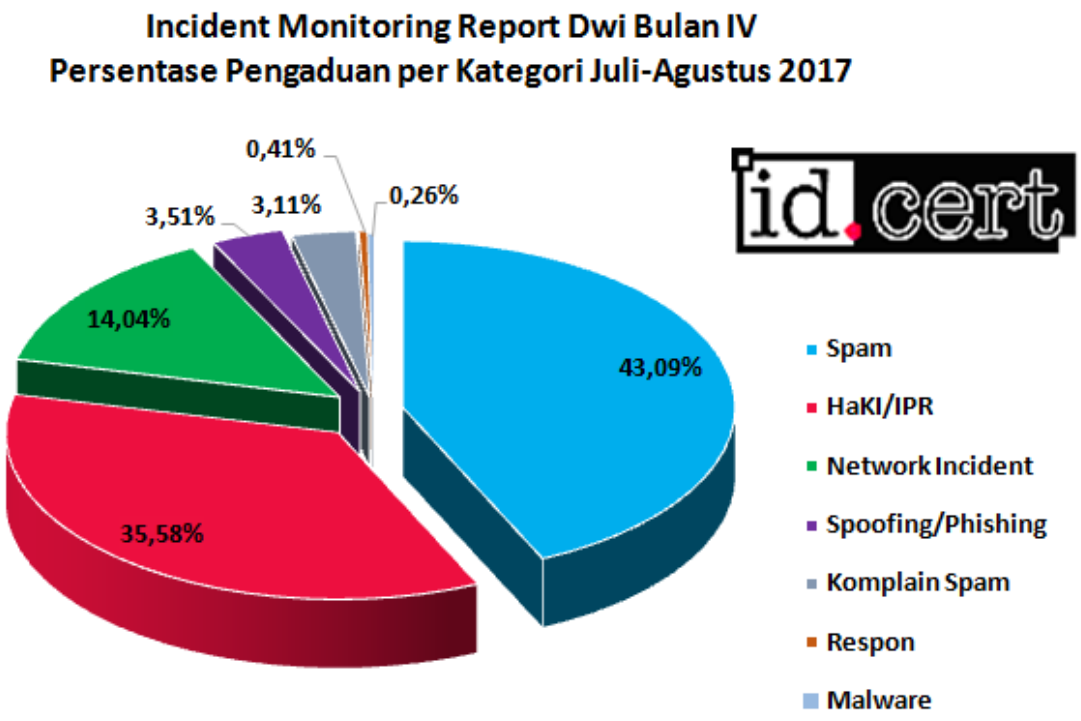
Kategori	Juli	Agustus	Total	%
Spam	7.672	7.561	15.233	43,09%
HaKI/IPR	2.475	10.101	12.576	35,58%
Network Incident	2.674	2.288	4.962	14,04%
Spoofing/Phishing	591	648	1.239	3,51%
Komplain Spam	449	650	1.099	3,11%
Respon	12	134	146	0,41%
Malware	22	71	93	0,26%

Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Juli – Agustus 2017 dan jumlah total dua bulan.



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Juli-Agustus 2017

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 sebagian kategori mengalami peningkatan dan sebagian kategori lain mengalami penurunan jumlah pengaduan pada bulan Agustus. Persentase detil 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 Bulanan IV 2017

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

Tabel 2 Perkembangan jumlah pengaduan yang mengalami peningkatan dan penurunan dalam persentase

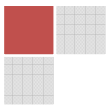
Kategori	Juli	Agustus	%
Respon	12	134	1016,67%
HaKI/IPR	2.475	10.101	308,12%
Malware	22	71	222,73%
Komplain Spam	449	650	44,77%
Spoofing/Phishing	591	648	9,64%
Spam	7.672	7.561	-1,45%
Network Incident	2.674	2.288	-14,44%

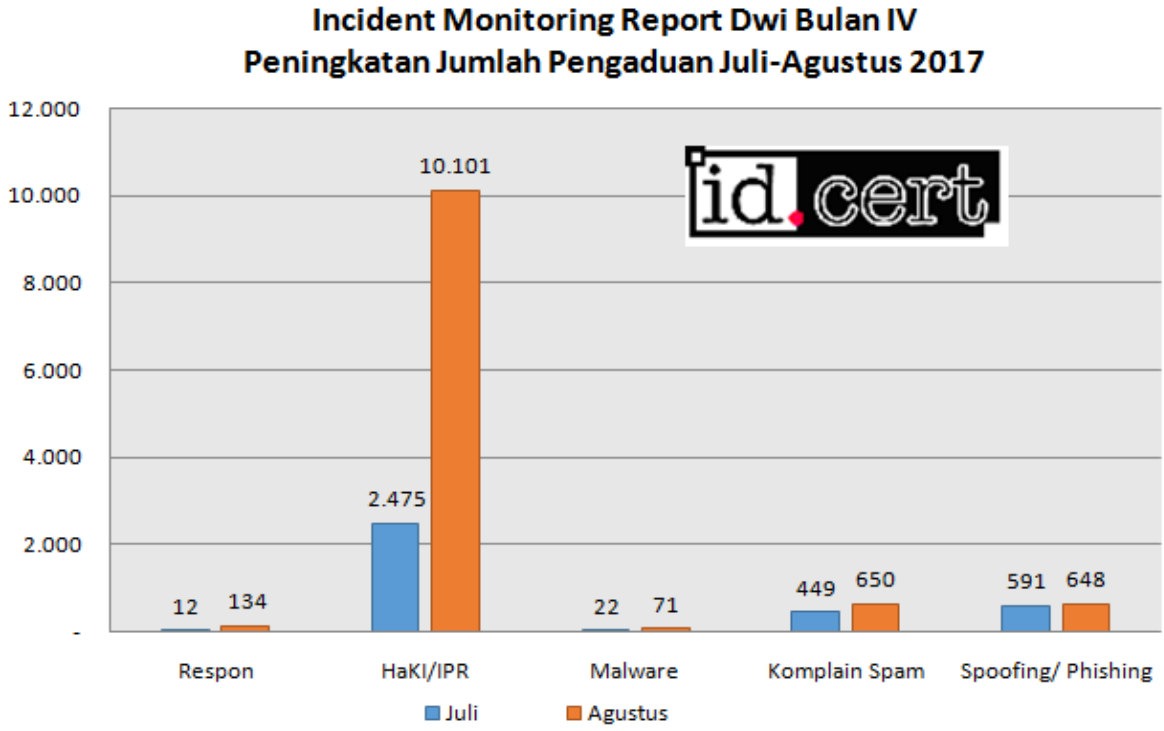
3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, terdapat 5 (lima) kategori yang mengalami peningkatan jumlah pengaduan, yaitu:

1. Respon memiliki jumlah pengaduan sejumlah 12 di bulan Juli. Pada bulan Agustus terjadi peningkatan jumlah pengaduan dibandingkan dengan bulan Juli dengan persentase peningkatan sebesar 1.016,67%. Secara persentase memang kelihatan sangat besar tetapi jumlah pengaduan di bulan Agustus hanya sebesar 134 pengaduan.
2. Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami peningkatan jumlah pengaduan dari bulan Juli ke Agustus, dari 2.475 naik drastis menjadi 10.101. Persentase peningkatannya sebesar 308,12% atau 7.626 jumlah pengaduan. Aduan IPR hampir semuanya adalah pengunduhan Film dan Musik secara ilegal di IP Address Indonesia.
3. *Malware* mengalami peningkatan jumlah pengaduan sebesar 222,73%. Secara persentase kelihatan besar tetapi sebenarnya hanya mengalami peningkatan 49 saja. Pada bulan Juli berjumlah 22 pengaduan, pada bulan Agustus meningkat menjadi 71 pengaduan.
4. Komplain *Spam* mengalami peningkatan jumlah dari bulan Juli ke Agustus ini. Komplain *Spam* memiliki jumlah sebanyak 449 pada bulan Juli dan naik dengan persentase sebesar 44,77% di bulan Agustus dengan jumlah sebanyak 650. Komplain Spam adalah aduan spam yang diterima oleh user di Indonesia.
5. *Spoofing/Phishing* mengalami peningkatan jumlah pengaduan dari 591 pada bulan Juli dan naik sebesar 9,64% di bulan Agustus dengan jumlah pengaduan sebanyak 648.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.





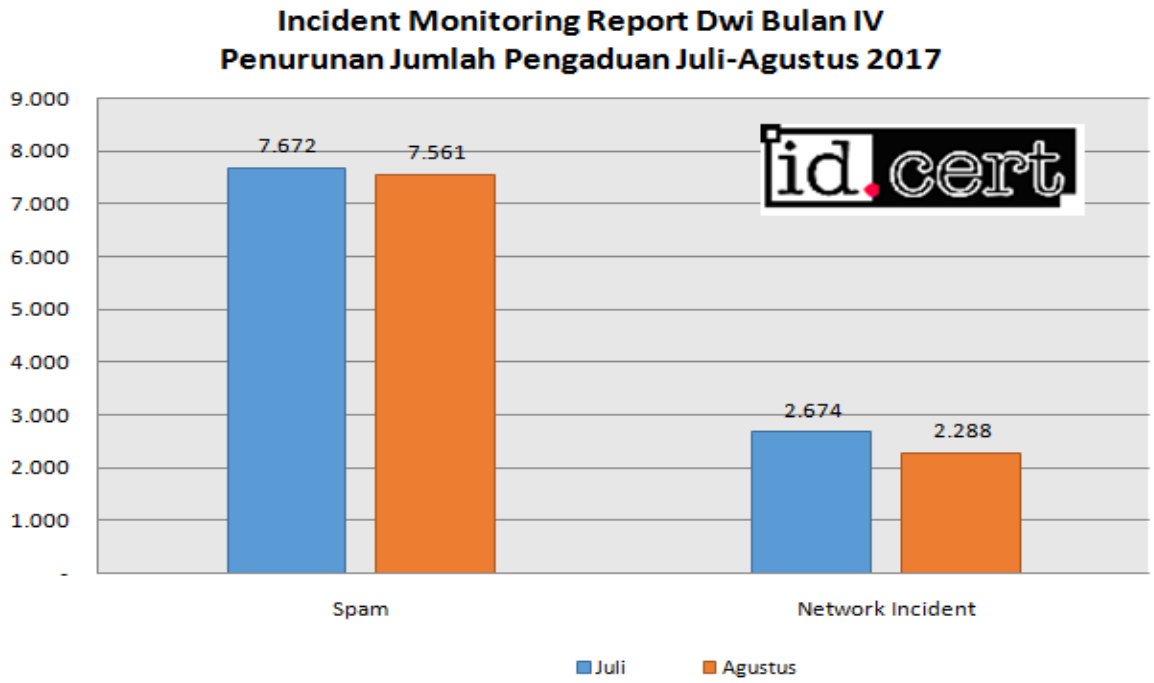
Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Juli-Agustus 2017

3.2 Kelompok Pengaduan yang Mengalami Penurunan

Bulan Juli - Agustus 2017 terdapat beberapa kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. Meskipun *Spam* memiliki jumlah pengaduan total terbanyak selama bulan Juli dan Agustus, tetapi mengalami penurunan jumlah pengaduan di bulan kedua. Jumlah pengaduan *Spam* sebesar 7.672 di bulan Juli, mengalami sedikit penurunan sebesar 111 menjadi 7.561. Persentase penurunannya mencapai sebesar 1,45%.
2. *Network Incident* jumlah pengaduannya menurun 14,44% di bulan kedua. Di bulan pertama Juli jumlahnya sebesar 2.674 menurun menjadi 2.288 pengaduan di bulan kedua Agustus.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Juli-Agustus 2017

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

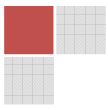
Dengan pertimbangan jumlah pengaduan *spam* yang masih sangat tinggi, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi "pintu gerbang" pengiriman *spam* (terutama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

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

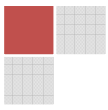
Sejumlah rekomendasi yang dapat dipertimbangkan:

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 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