

Incident Monitoring Report - 2017

Laporan Dwi Bulan VI 2017

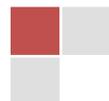
Bulan November dan Desember 2017



Januari 2018

Daftar Isi

1. Pendahuluan	3
2. Metoda.....	5
3. Uraian	7
3.1 Kelompok Pengaduan yang Mengalami Peningkatan	11
3.2 Kelompok Pengaduan yang Mengalami Penurunan	12
4. Rangkuman.....	15
4.1 Rekomendasi.....	15
5. Ucapan Terima Kasih.....	17



1. Pendahuluan

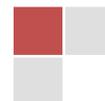
Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi lebih penting, dari komunikasi antar warga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lanjut usia, para pekerja di lapangan 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-CERT¹ 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, November dan Desember 2017.

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

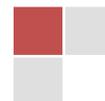
Penting ditekankan dalam hal ini adalah tindak lanjut terhadap laporan tentang penyalahgunaan Internet (*Internet abuse*) sebagai respon positif dan langkah untuk memperbaiki keadaan. Hal ini juga bagian interaksi positif antara kita, pengguna Internet di Indonesia dengan pihak-pihak di mancanegara terkait 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 VI 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 43,13% atau berjumlah total 14.499 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam* dan HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)) pada kelompok pertama yang memiliki jumlah pelaporan di atas 10.000 laporan, dan *Network Incident*, *Komplain Spam*, *Spoofing/Phishing*, *Malware*, dan *Respon* pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 10.000 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 VI 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 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).

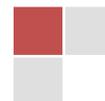
Komplain Spam Keluhan/pengaduan email *spam* dari dalam negeri terhadap pengirim di Indonesia dan luar negeri.

Malware Program komputer yang dibuat untuk maksud jahat³.

Network Incident Aktivitas yang dilakukan terhadap jaringan pihak lain dan semua aktivitas terkait dengan penyalahgunaan jaringan.

² *Fraud*, <http://en.wikipedia.org/wiki/Fraud>

³ *Malware*, <http://en.wikipedia.org/wiki/Malware>



Respon Respon terhadap laporan yang masuk.

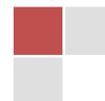
Spam Penggunaan sistem pengolahan pesan elektronik untuk mengirim pesan-pesan tidak diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih⁴.

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna⁵.

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

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



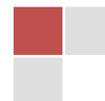
3. Uraian

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

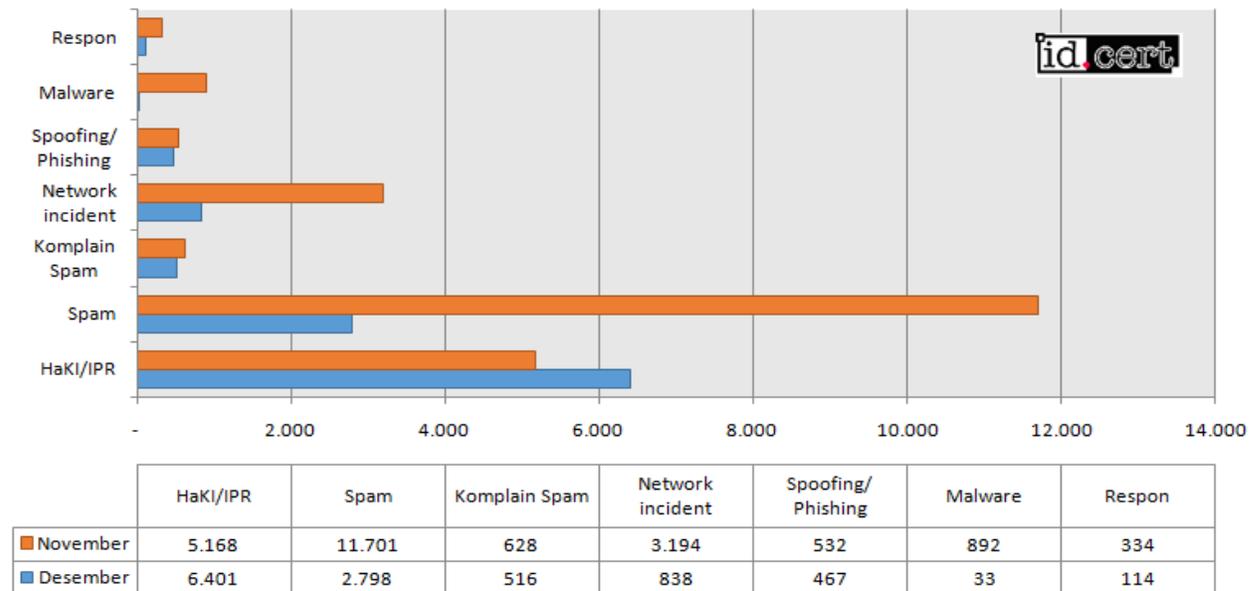
Pengolahan data dilakukan dengan dua cara, yaitu:

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



Incident Monitoring Report Dwi Bulan VI
Jumlah Pengaduan Semua Kategori November-Desember 2017

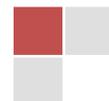


Gambar 1 Jumlah pengaduan semua kategori November-Desember 2017

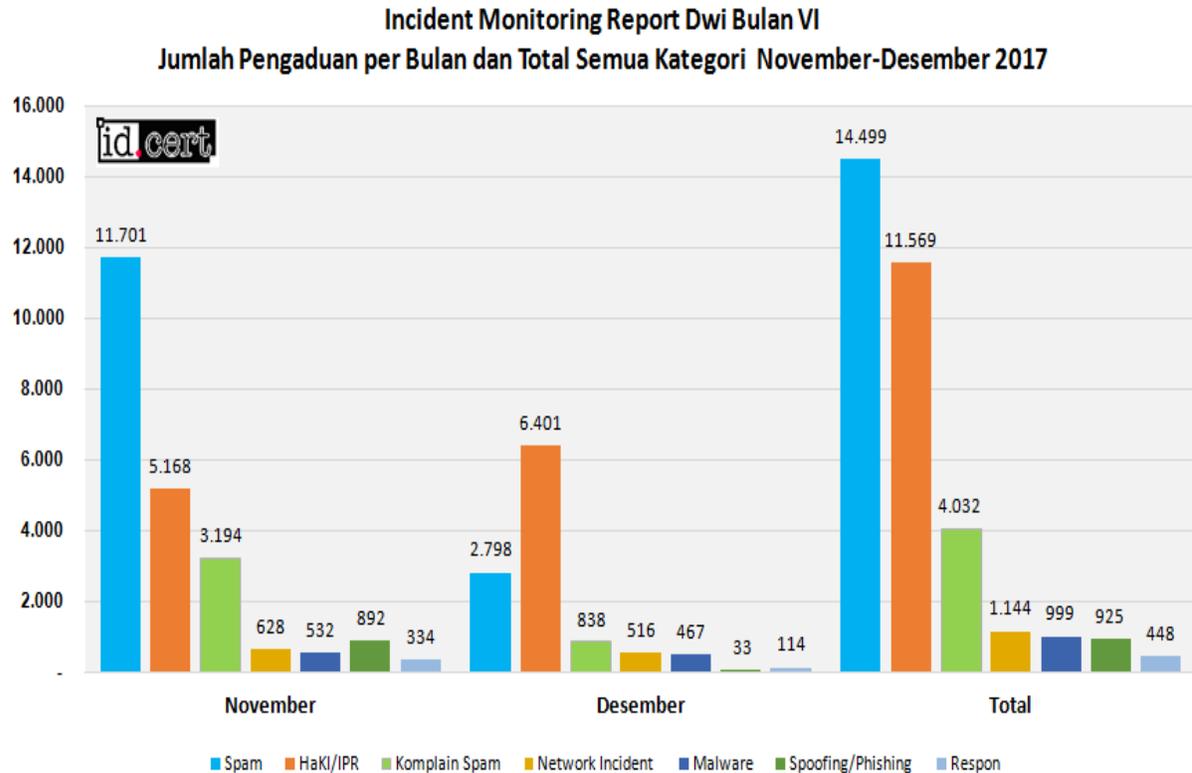
Jumlah pengaduan masing-masing per bulan dan total dua bulan dapat dilihat lebih seksama di Tabel 1 dengan kategori pengaduan ditampilkan berdasarkan jumlah laporan yang tertinggi ke terendah.

Tabel 1 Perkembangan jenis pengaduan selama November-Desember 2017

Kategori	November	Desember	Total	%
Spam	11.701	2.798	14.499	43,13%
HaKI/IPR	5.168	6.401	11.569	34,42%
Network Incident	3.194	838	4.032	11,99%
Komplain Spam	628	516	1.144	3,40%
Spoofing/Phishing	532	467	999	2,97%
Malware	892	33	925	2,75%
Respon	334	114	448	1,33%



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

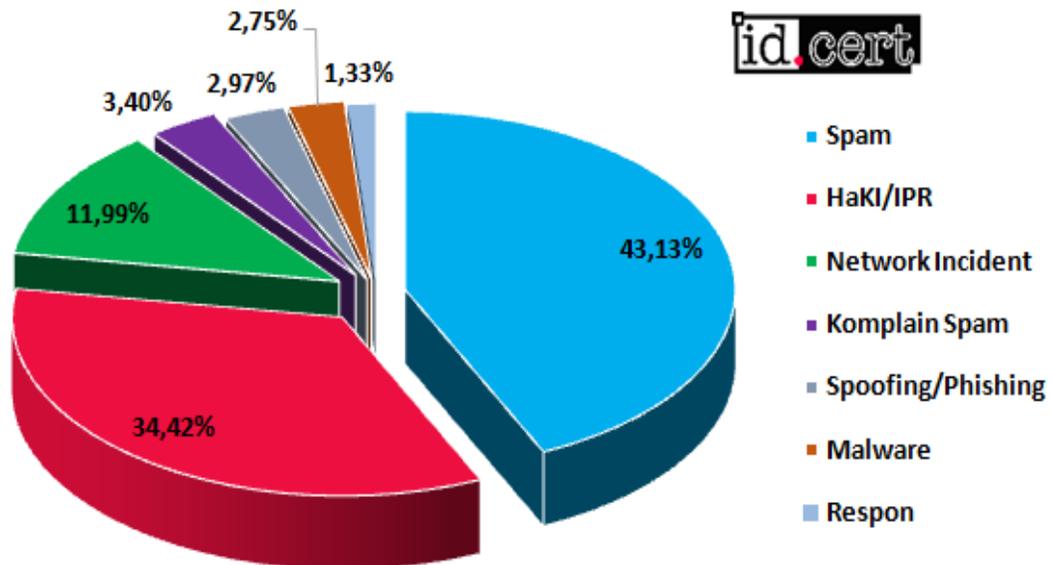


Gambar 2 Jumlah pengaduan per bulan dan total semua kategori November-Desember 2017

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama November, bulan kedua Desember dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan VI ini yaitu satu kategori mengalami peningkatan dan 6 (enam) kategori lainnya mengalami penurunan jumlah pengaduan pada bulan Desember. 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.



Incident Monitoring Report Dwi Bulan VI Persentase Pengaduan per Kategori November-Desember 2017

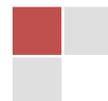


Gambar 3 Persentase pengaduan per kategori Dwi Bulan VI 2017

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	November	Desember	%
HaKI/IPR	5.168	6.401	23,86%
Spoofing/Phishing	532	467	-12,22%
Komplain Spam	628	516	-17,83%
Respon	334	114	-65,87%
Network Incident	3.194	838	-73,76%
Spam	11.701	2.798	-76,09%
Malware	892	33	-96,30%



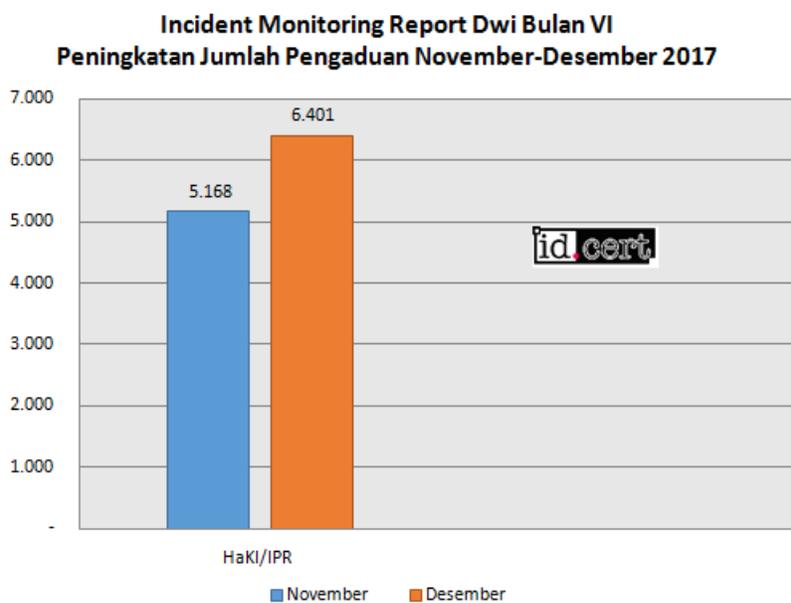
3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, hanya terdapat 1 (satu) kategori yang mengalami peningkatan jumlah pengaduan, yaitu:

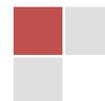
1. HaKI/IPR

Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami lonjakan peningkatan jumlah dari bulan November ke Desember ini, yaitu 1.233 pengaduan. HaKI/IPR memiliki jumlah sebanyak 5.168 pada bulan November dan naik dengan persentase sebesar 23,86% di bulan Desember dengan jumlah sebanyak 6.401. Total jumlah pengaduan HaKI/IPR selama 2 bulan adalah 11.569. Aduan HaKI/IPR sebagian besar adalah pengunduhan film secara ilegal di IP Address Indonesia.

Grafik peningkatan jumlah pengaduan selama bulan November dan Desember disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan November-Desember 2017



3.2 Kelompok Pengaduan yang Mengalami Penurunan

Bulan November – Desember 2017 terdapat 6 (enam) kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. *Malware*

Malware mengalami penurunan jumlah sebesar 96,30%, yaitu 859 pengaduan. Penurunan jumlah sebesar 859 pengaduan tersebut ketika pada bulan November berjumlah 892 pengaduan dan pada bulan Desember menurun menjadi 33 pengaduan. Total jumlah pengaduan *Malware* selama 2 bulan adalah 925, atau 2,75%.

2. *Spam*

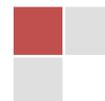
Meskipun *Spam* memiliki jumlah pengaduan total terbanyak selama bulan November dan Desember, yaitu 14.499 atau sebesar 43,13% dari keseluruhan jumlah di semua kategori, tetapi mengalami penurunan jumlah pengaduan yang cukup besar di bulan kedua, yaitu bulan Desember. Jumlah pengaduan *Spam* sebesar 11.701 di bulan November mengalami penurunan sebesar 8.903 menjadi 2.798 di bulan Desember. Persentase penurunannya mencapai sebesar 76,09%.

3. *Network Incident*

Total jumlah pengaduan *Network Incident* selama 2 bulan terakhir dari tahun 2017 adalah 4.032, atau sebesar 11,99% dari total jumlah keseluruhan kategori pengaduan yang berarti menempatkan *Network Incident* pada urutan ketiga. Jumlah pengaduan di bulan November adalah 3.194, turun sebesar 2.356 atau 73,76% di bulan Desember menjadi 838.

4. Respon

Respon memiliki jumlah pengaduan sejumlah 334 di bulan November. Pada bulan Desember menurun jumlah pengaduan dibandingkan dengan bulan November menjadi 114 dengan persentase penurunan sebesar 65,87%, atau sejumlah 220. Total jumlah pengaduan selama 2 (dua) bulan ini adalah 448 atau 1,33% dari total seluruh kategori.



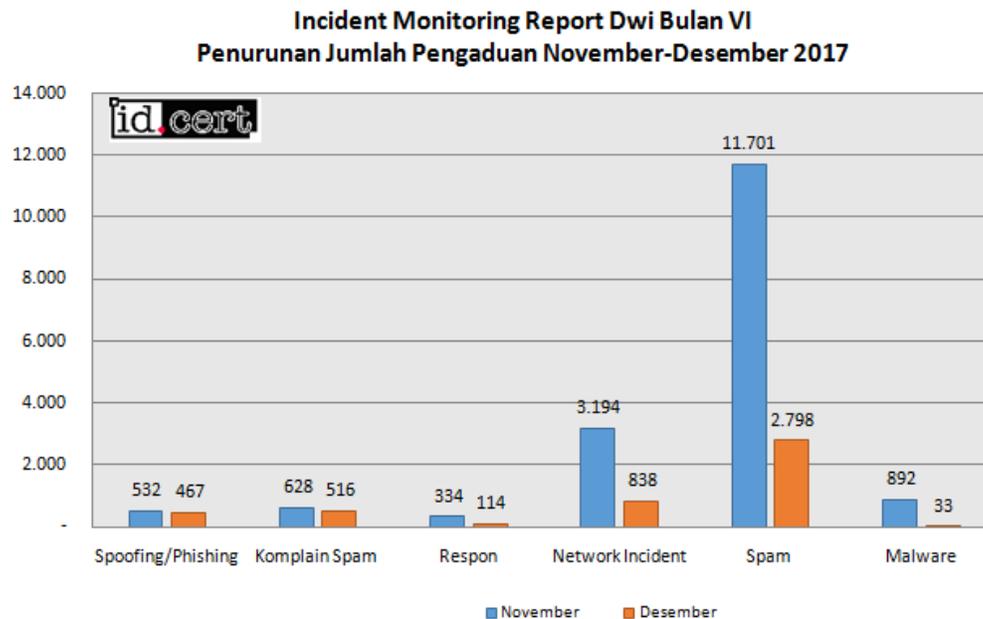
5. Komplain Spam

Komplain Spam adalah aduan spam yang diterima oleh user di Indonesia. Total Komplain Spam selama bulan November dan Desember adalah 1.144 pengaduan, atau 3,40% dari total keseluruhan kategori selama 2 (dua) bulan tersebut. Pada bulan November jumlah pengaduan adalah 628, turun sebesar 17,83% atau sejumlah 112 di bulan Desember menjadi 516.

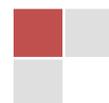
6. Spoofing/Phishing

Spoofing/Phishing juga mengalami sedikit penurunan jumlah pengaduan dari 532 pada bulan November dan turun sebesar 12,22%, yaitu 467, di bulan Desember dengan jumlah pengaduan sebanyak 467. Total jumlah pengaduan selama 2 (dua) bulan adalah 999, atau 2,97% dari total seluruh kategori.

Grafik penurunan jumlah pengaduan selama bulan November dan Desember disajikan pada Gambar 5.



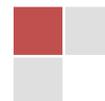
Gambar 5 Penurunan Jumlah Pengaduan pada bulan November-Desember 2017



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 menjangkau lebih banyak laporan.



4. Rangkuman

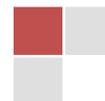
Dengan pertimbangan jumlah pengaduan *spam* yang masih sangat tinggi, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi “pintu gerbang” pengiriman *spam* (terutama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

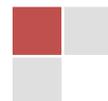
Sejumlah rekomendasi yang dapat dipertimbangkan:

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. Kementerian 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

