

Laporan Dwi Bulan III 2018

Bulan Mei dan Juni 2018



Juli 2018

Daftar Isi

1.Pendahuluan.....	3
2.Metoda.....	5
3.Uraian.....	7
3.1Kelompok Pengaduan yang Mengalami Peningkatan.....	11
3.2Kelompok Pengaduan yang Mengalami Penurunan.....	13
4.Rangkuman.....	16
4.1 Rekomendasi.....	16
5.Ucapan Terima Kasih.....	18

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 2 (dua) bulan, Mei dan Juni 2018.

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 III 2018 ini, HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)) menempati jumlah pengaduan terbanyak yaitu mencapai 43,28% atau berjumlah total 8.053 pengaduan. Dilihat dari sisi jumlah pengaduan selama 2 (dua) bulan tersebut, terdapat dua kelompok: HaKI/IPR, *Spam*, dan *Network Incident* pada kelompok pertama yang memiliki jumlah pelaporan di atas 2.000 laporan, dan *Malware*, *Spoofing/Phishing*, *Komplain Spam*, dan *Respon* pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 2.000 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 III 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

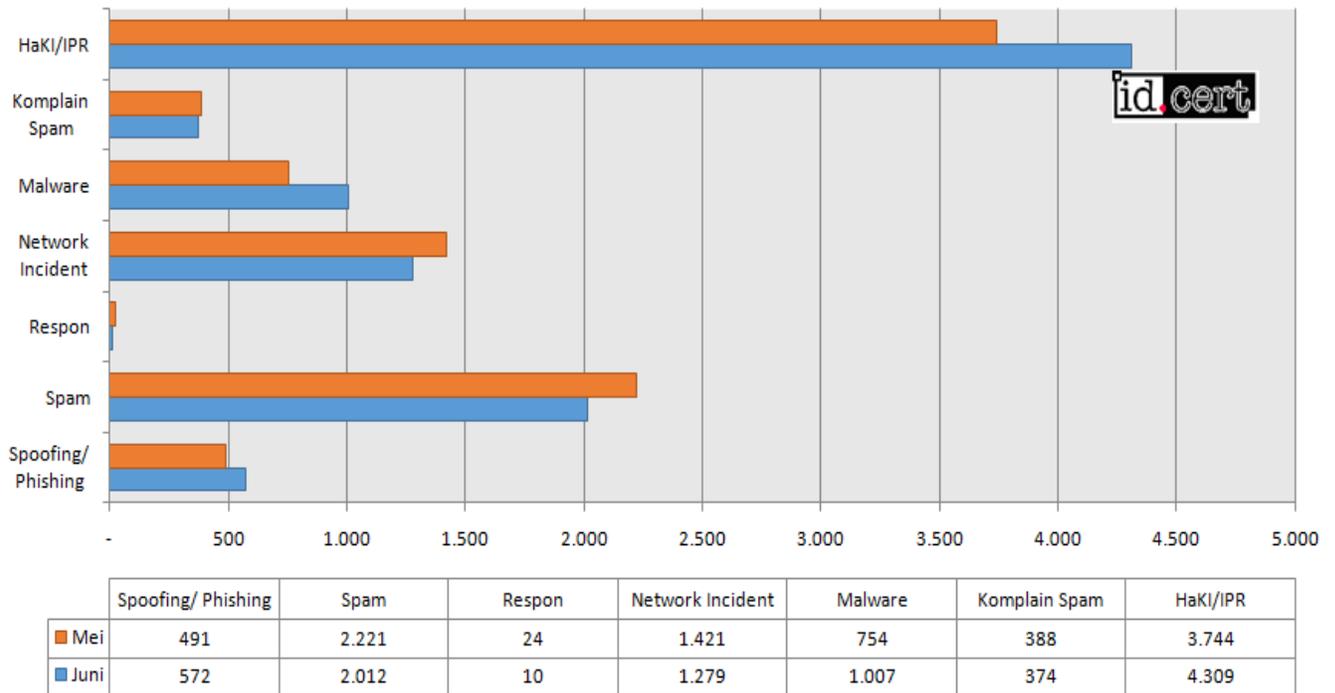
Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, yaitu bulan Mei dan Juni 2018. Kategori pengaduan terdiri atas HaKI/IPR, *Spam*, *Network Incident*, *Malware*, *Spoofing/Phishing*, *Komplain Spam*, dan *Respon*.

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 III 2018 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1 di bawah ini.

Incident Monitoring Report Dwi Bulan III
Jumlah Pengaduan Semua Kategori Mei-Juni 2018



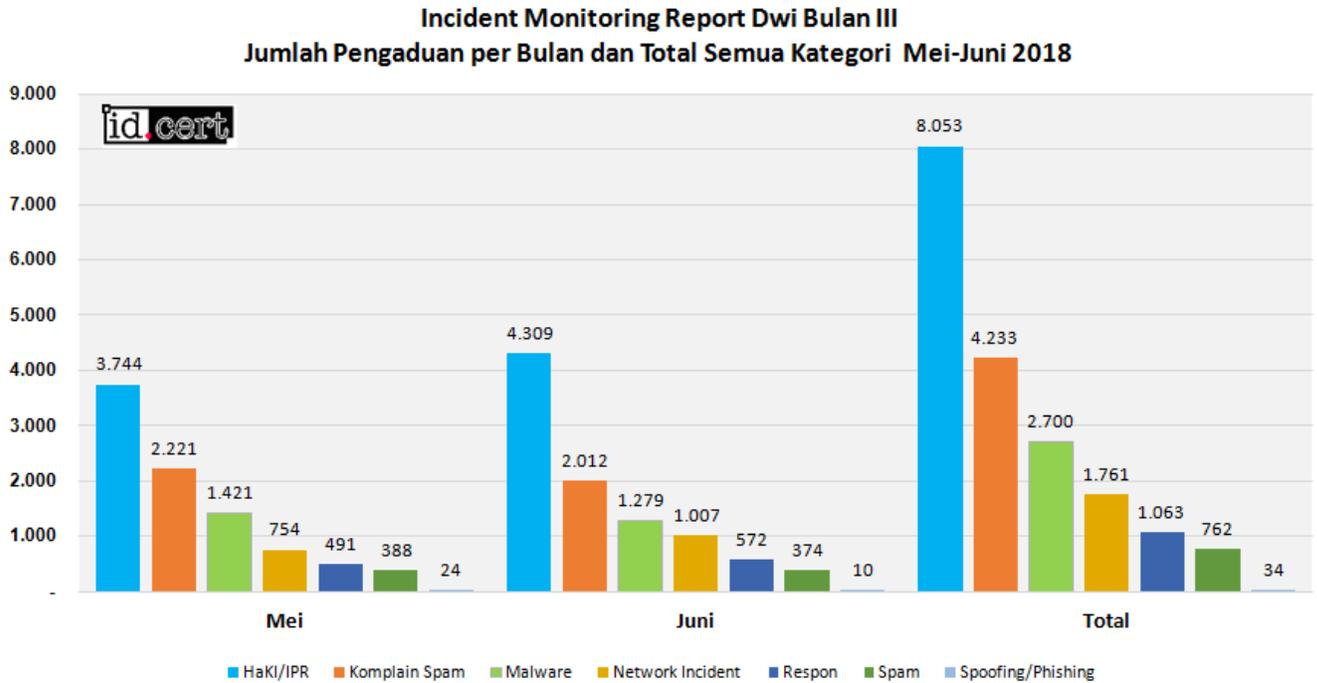
Gambar 1 Jumlah pengaduan semua kategori Mei – Juni 2018

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 Mei – Juni 2018

Kategori	Mei	Juni	Total	%
HaKI/IPR	3.744	4.309	8.053	43,28%
Spam	2.221	2.012	4.233	22,75%
Network Incident	1.421	1.279	2.700	14,51%
Malware	754	1.007	1.761	9,46%
Spoofing/Phishing	491	572	1.063	5,71%
Komplain Spam	388	374	762	4,10%
Respon	24	10	34	0,18%

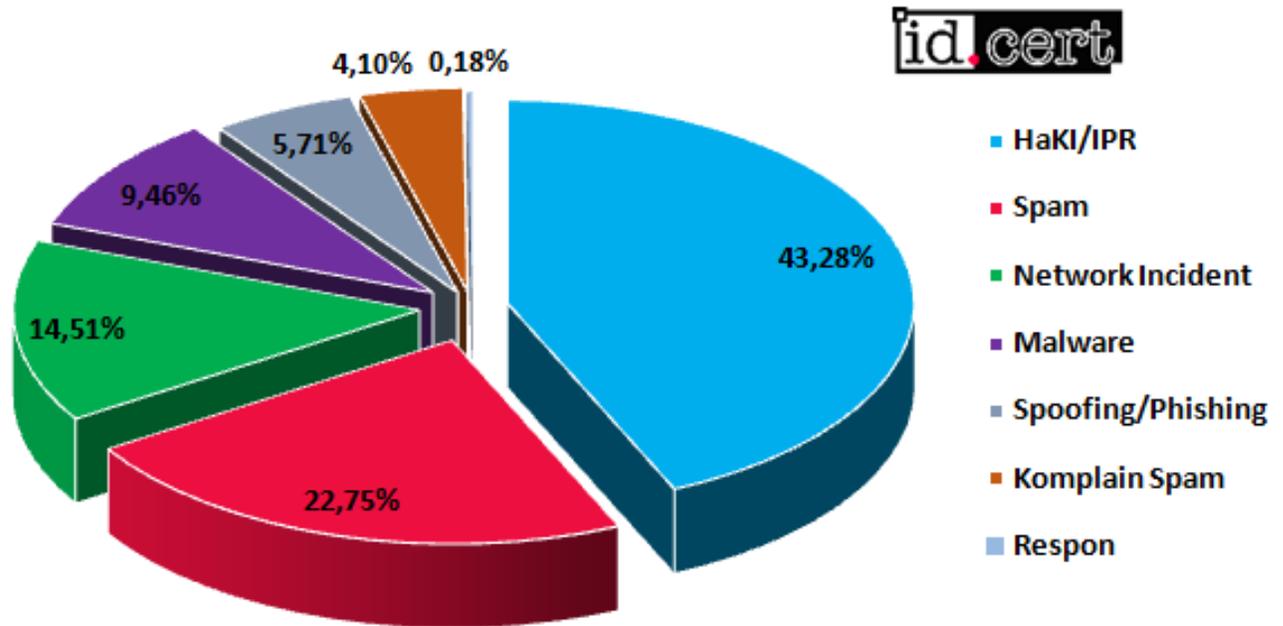
Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Mei – Juni 2018 dan jumlah total 2 (dua) bulan.



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Mei-Juni 2018

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Mei dan bulan kedua Juni, akan bernilai positif jika terjadi peningkatan jumlah dan bernilai negatif jika terjadi penurunan jumlah. Tren untuk Dwi Bulan III ini terdapat 3 (tiga) kategori yang mengalami peningkatan jumlah pengaduan, yaitu *Malware*, *Spoofing/Phishing*, dan *HaKI/IPR*, dan 4 (empat) kategori lainnya, *Komplain Spam*, *Spam*, *Network Incident*, dan *Respon*, yang mengalami penurunan jumlah pengaduan pada bulan kedua, yaitu bulan Juni. 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 III Persentase Pengaduan per Kategori Mei-Juni 2018



Gambar 3 Persentase pengaduan per kategori Dwi Bulan III 2018

HaKI/IPR menduduki peringkat pertama untuk jumlah total pengaduan selama 2 (dua) bulan, Mei dan Juni, yaitu 8.053 pengaduan atau sebesar 43,28%. *Spam* berada di peringkat kedua dengan persentasi sebesar 22,75% atau sejumlah 4.233 pengaduan. Di peringkat ketiga ditempati oleh *Network Incident* dengan jumlah total 2 (dua) bulan 2.700 pengaduan atau sebesar 14,51%. Peringkat keempat dan kelima adalah *Malware* dan *Spoofing/Phishing*, dengan jumlah total masing-masing adalah 1.761 dan 1.063 pengaduan, atau sebesar 9,46% dan 5,71%. *Komplain Spam* dan *Respon* berada di dua peringkat terbawah dengan persentasi masing-masing sebesar 4,10% dan 0,18% dan mempunyai jumlah total sebesar 762 dan 34 pengaduan.

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	Mei	Juni	%
Malware	754	1.007	33,55%
Spoofing/Phishing	491	572	16,50%
HaKI/IPR	3.744	4.309	15,09%
Komplain Spam	388	374	-3,61%
Spam	2.221	2.012	-9,41%
Network Incident	1.421	1.279	-9,99%
Respon	24	10	-58,33%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Pada Tabel 2 di atas, dapat dilihat bahwa dari 7 (tujuh) kategori pengaduan, pada Dwi Bulan III ini terdapat 3 (tiga) kategori yang mengalami peningkatan jumlah pada bulan kedua, yaitu bulan Juni.

Kategori yang mengalami peningkatan jumlah adalah:

1. *Malware*

Malware mengalami peningkatan jumlah terbesar secara persentase di antara 7 kategori, yaitu 33,55%. Peningkatan jumlah sebesar 253 pengaduan tersebut ketika pada bulan Mei berjumlah 754 pengaduan dan pada bulan Juni meningkat menjadi 1.007 pengaduan.

2. *Spoofing/Phishing*

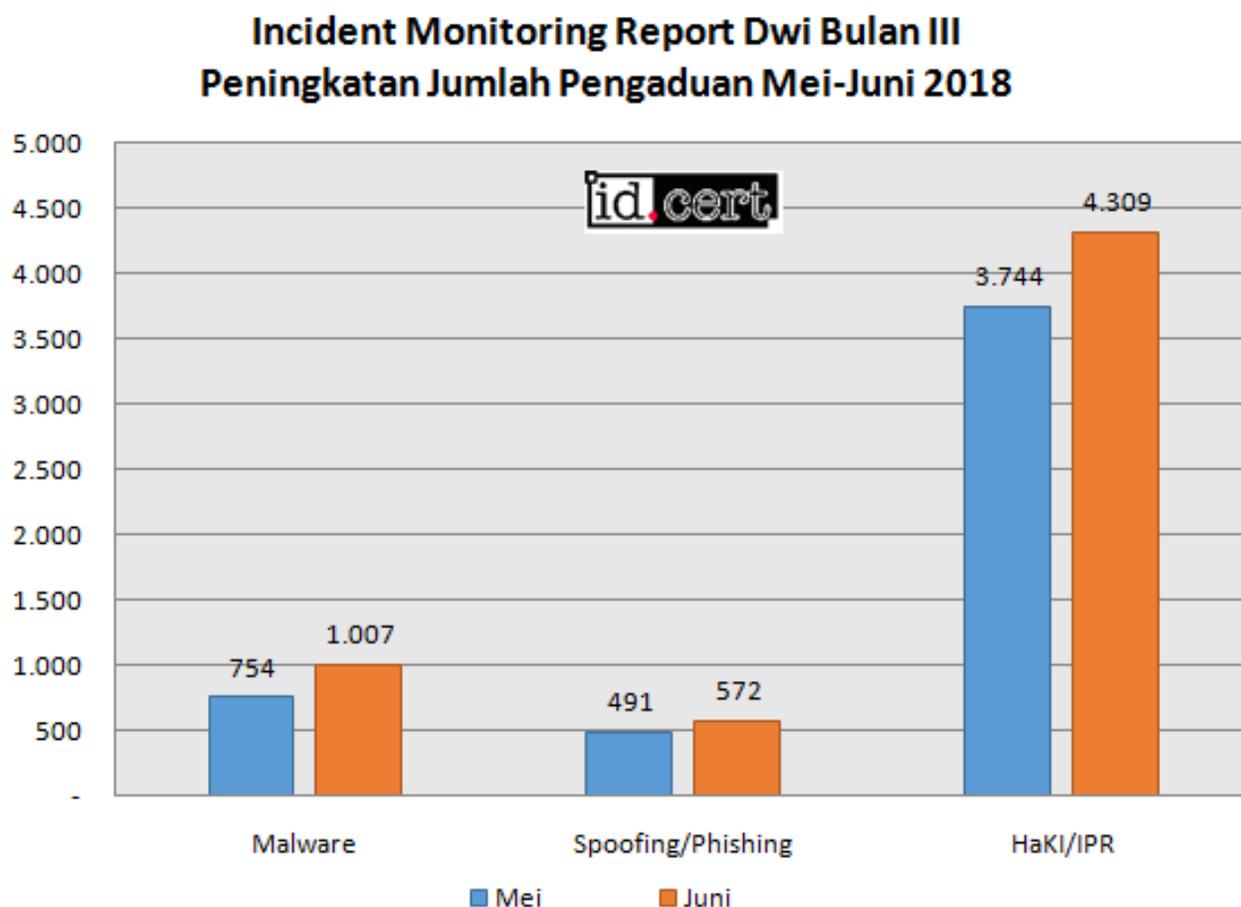
Spoofing/Phishing mengalami peningkatan jumlah pengaduan dari 491 pada bulan Mei dan naik sebesar 16,50% atau 81 pengaduan di bulan Juni dengan jumlah pengaduan sebanyak 572.

3. HaKI/IPR

HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)) mengalami peningkatan jumlah yang paling besar secara angka,

yaitu 565, tetapi secara persentase paling kecil, yaitu 15,09%. Di bulan Mei jumlah pengaduan sebesar 3.744 meningkat menjadi 4.309 di bulan Juni.

Berikut grafik peningkatan jumlah pengaduan yang terjadi selama bulan Mei dan Juni disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Mei-Juni 2018

3.2 Kelompok Pengaduan yang Mengalami Penurunan

Dari Tabel 2 di atas juga dapat dilihat bahwa dari 7 (tujuh) kategori pengaduan, pada Dwi Bulan III ini terdapat 4 (empat) kategori yang mengalami penurunan jumlah pada bulan Juni.

Kategori yang mengalami penurunan jumlah adalah:

1. *Komplain Spam*

Di bulan Mei jumlah pengaduan *Komplain Spam* sebesar 388, di bulan Juni turun sebesar 14 menjadi 374 pengaduan. Penurunan tersebut secara persentase adalah 3,61%.

2. *Spam*

Spam mengalami penurunan jumlah pengaduan terbanyak, yaitu 209. Dari 2.221 pengaduan *Spam* di bulan Mei, menurun jumlahnya menjadi 2.012 di bulan April. Persentase penurunannya mencapai sebesar 9,41%.

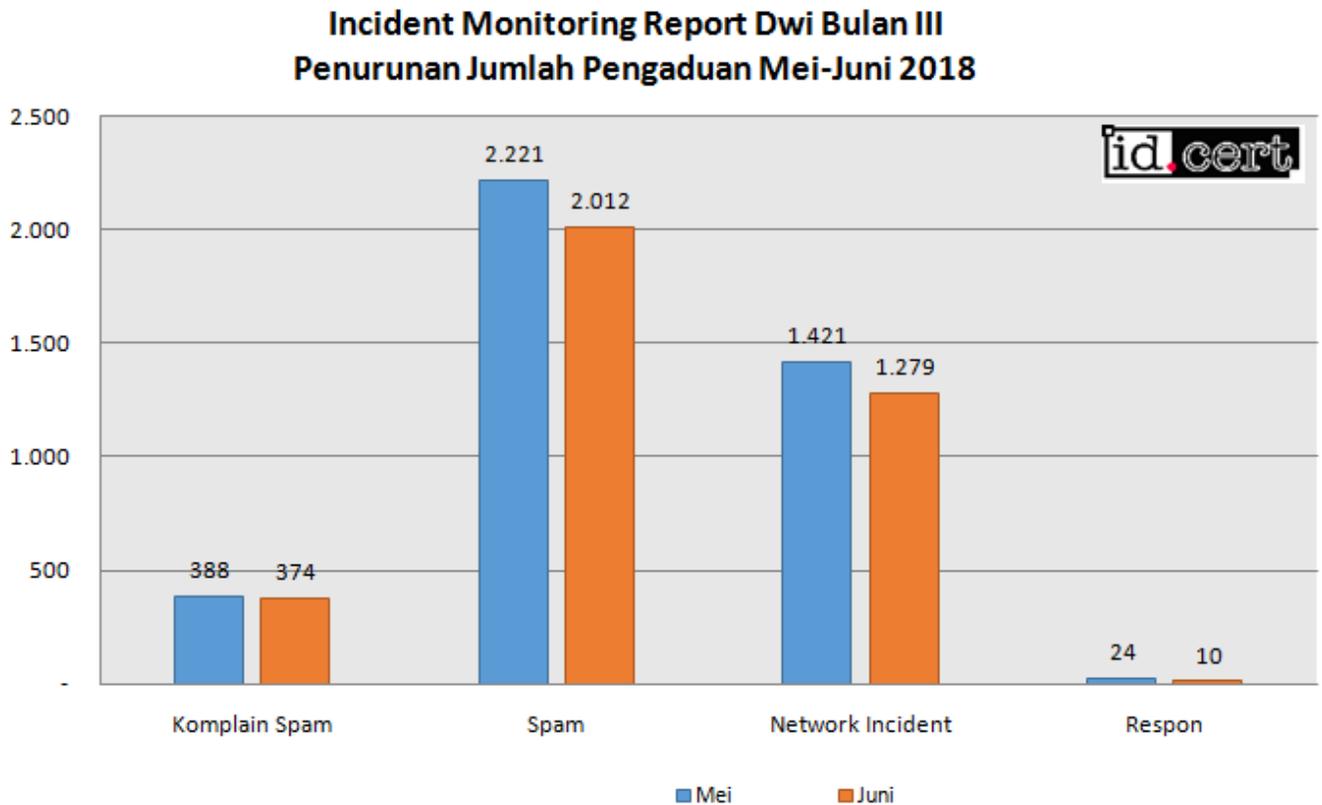
3. *Network Incident*

Network Incident memiliki jumlah penurunan pengaduan secara persentase sebesar 9,99%, atau sebesar 142 pengaduan. Jumlah 142 pengaduan tersebut karena di bulan Mei berjumlah 1.421 dan di bulan April menurun menjadi 1.279.

4. *Respon*

Respon mengalami jumlah penurunan sebesar 14, dari bulan Mei sebesar 24 menjadi 10 di bulan Juni. Secara persentase jumlah penurunan tersebut terbesar, yaitu 58,33%.

Grafik penurunan jumlah pengaduan yang terjadi selama bulan Mei dan Juni disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Mei-Juni 2018

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, 3 (tiga) hal perlu dipertimbangkan:

1. Untuk masalah HaKI (Hak atas Kekayaan Intelektual) atau IPR (*Intellectual Property Rights*), para pengguna Internet perlu dan harus mendisiplinkan diri sendiri untuk tidak mengunduh file-file bajakan dari manapun.
2. 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.

3. ID-CERT perlu terus merangkul pihak-pihak lain untuk sosialisasi mekanisme pengaduan agar dapat menjaring lebih banyak laporan.

4. Rangkuman

Dikarenakan kategori HaKI/IPR menjadi yang tertinggi jumlah pengaduannya pada Dwi Bulan III ini, salah satu tindakan yang perlu dilakukan para administrator jaringan adalah memblokir aplikasi BitTorrent atau aplikasi pengunduh lainnya sehingga tidak dapat digunakan untuk mengunduh file-file yang masih mempunyai HaKI/IPR.

Dengan pertimbangan jumlah pengaduan *spam* yang juga tinggi, perlu juga 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. 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.
2. Perangkat lunak anti-spam dipasang di server *email* sebagai antisipasi pengiriman pesan *spam* dari jaringan lokal ke Internet.
3. 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.

4. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, misalnya akses ke port email/Postfix secara intensif dalam periode lama atau berulang-ulang.
5. Administrator jaringan memblokir semua port akses ke Internet, kecuali untuk port yang dianggap diperlukan.
6. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (*Internet abuse*) guna kemudahan pelaporan.
7. Formulir pengaduan penyalahgunaan Internet (*Internet abuse*) dicantumkan di setiap situs web.

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 Dwi Bulan III, 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