Incident Monitoring Report - 2018

Laporan Dwi Bulan II 2018

Bulan Maret dan April 2018

Mei 2018

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 2 (dua) bulan, Maret dan April 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 II 2018 ini, HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)) menempati jumlah pengaduan terbanyak yaitu mencapai 51,12% atau berjumlah total 10.553 pengaduan. Dilihat dari sisi jumlah pengaduan selama 2 (dua) bulan tersebut, terdapat dua kelompok: HaKI/IPR dan *Spam* pada kelompok pertama yang memiliki jumlah pelaporan di atas 5.000 laporan, dan *Network Incident*, *Malware, Spoofing/Phishing,* Komplain *Spam,* dan Respon pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 5.000 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 II 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

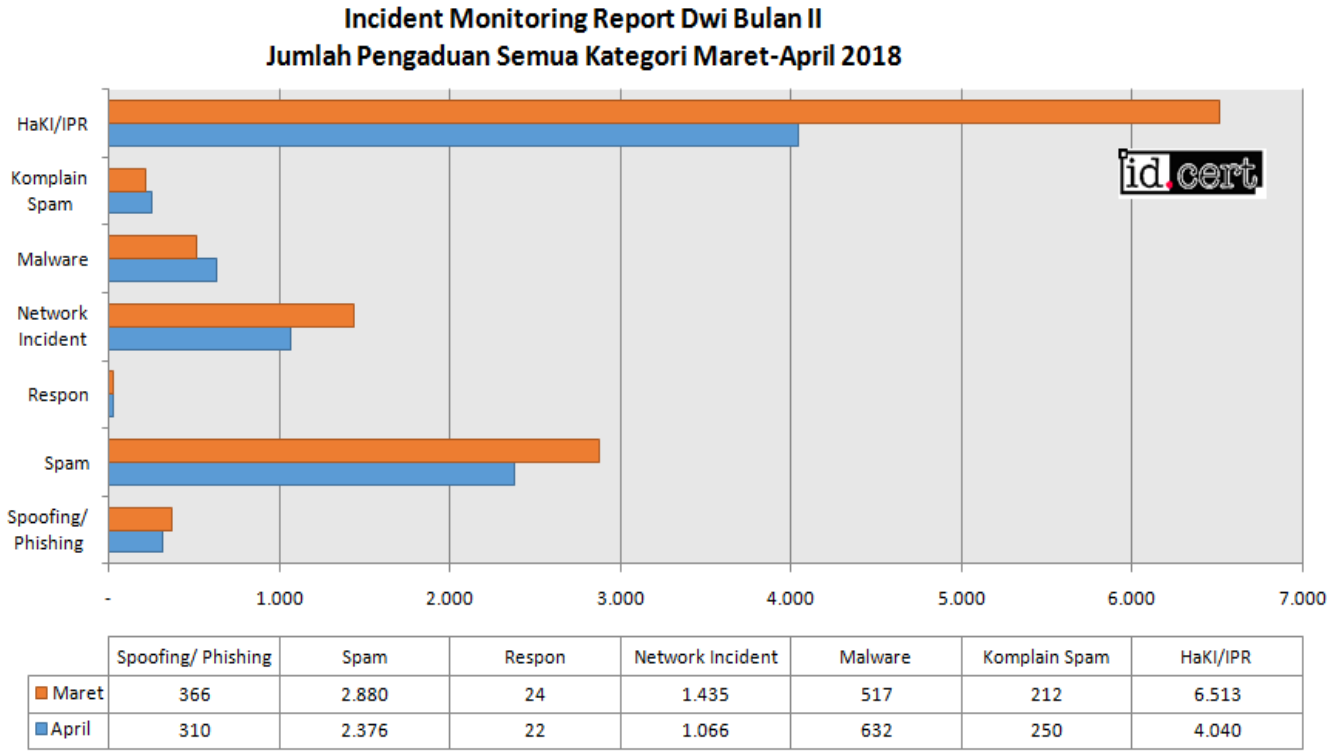
3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, yaitu bulan Maret dan April 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 II 2018 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1 di bawah ini.



	Spoofing/ Phishing	Spam	Respon	Network Incident	Malware	Komplain Spam	HaKI/IPR
Maret	366	2.880	24	1.435	517	212	6.513
April	310	2.376	22	1.066	632	250	4.040

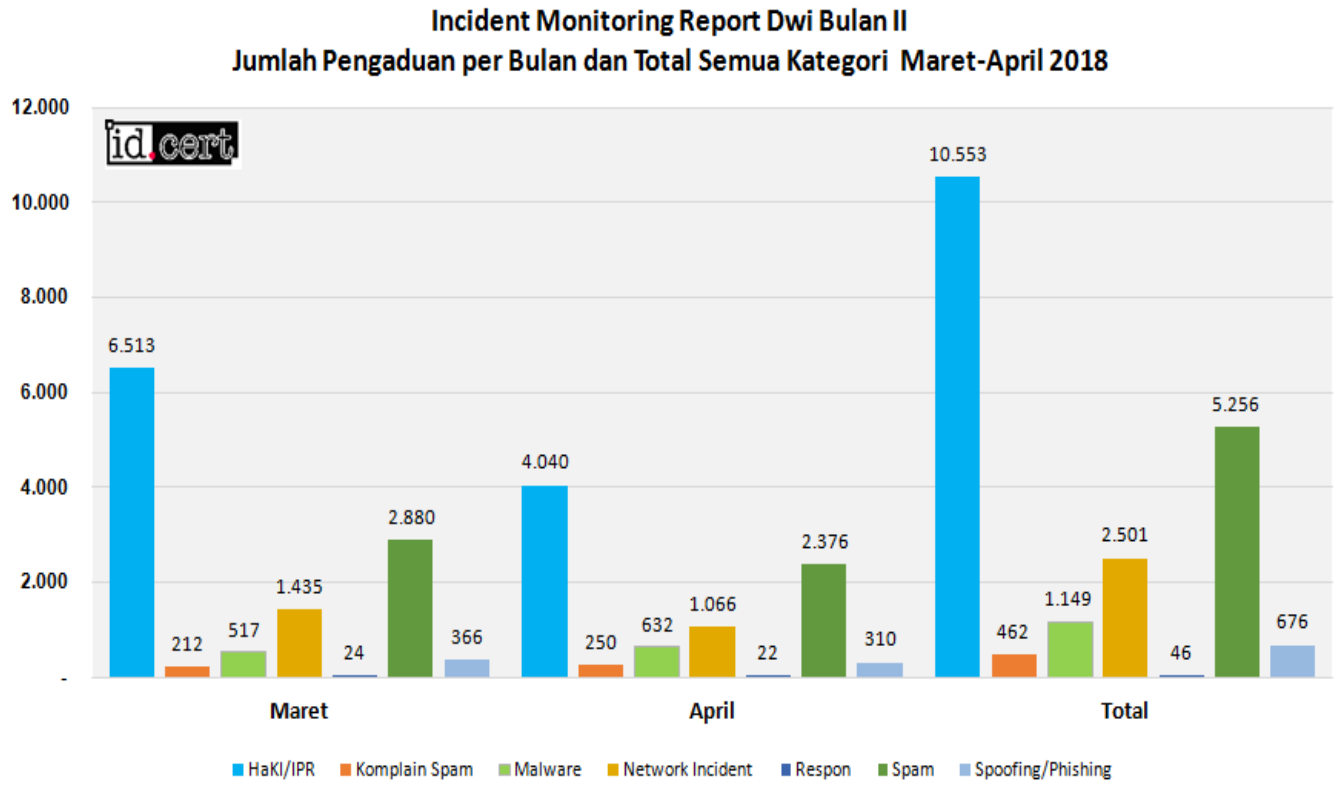
Gambar 1 Jumlah pengaduan semua kategori Maret - April 2018

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 Maret - April 2018

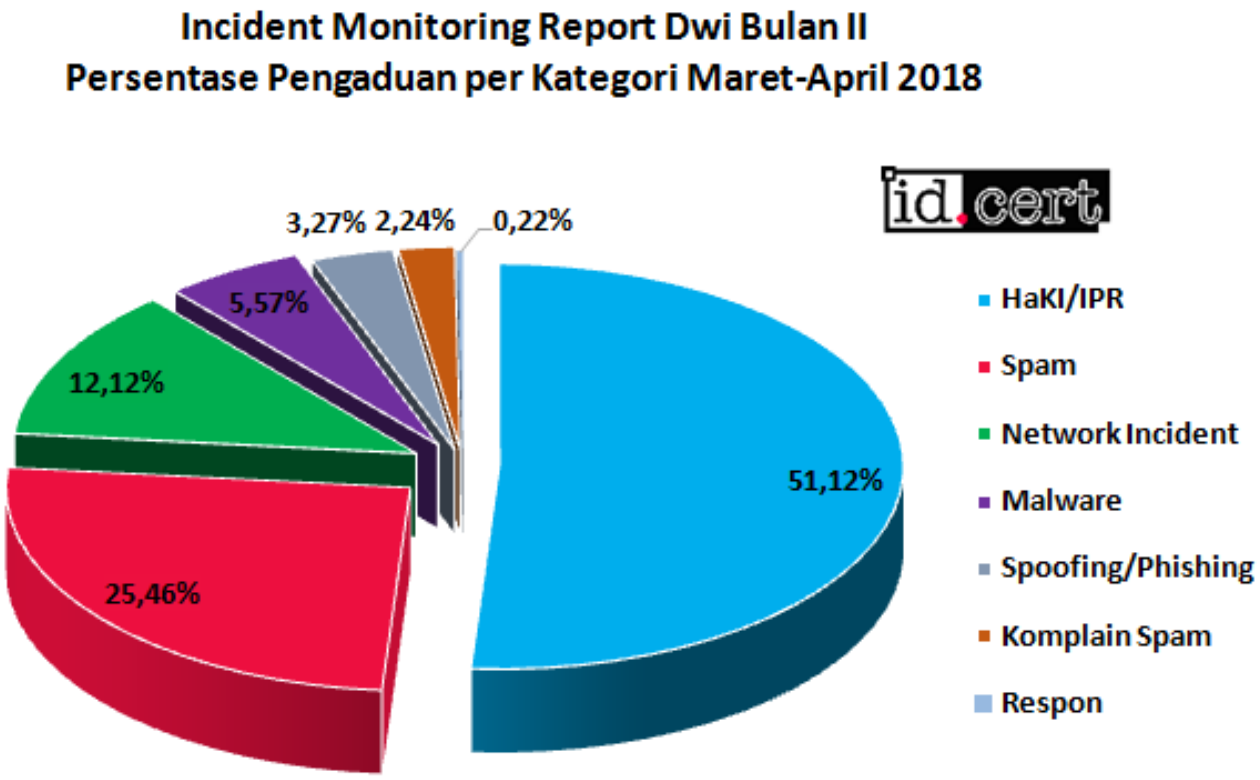
Kategori	Maret	April	Total	%
HaKI/IPR	6.513	4.040	10.553	51,12%
Spam	2.880	2.376	5.256	25,46%
Network Incident	1.435	1.066	2.501	12,12%
Malware	517	632	1.149	5,57%
Spoofing/Phishing	366	310	676	3,27%
Komplain Spam	212	250	462	2,24%
Respon	24	22	46	0,22%

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



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Maret – April 2018

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Maret, bulan kedua April dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan II ini terdapat 2 (dua) kategori yang mengalami peningkatan jumlah pengaduan, yaitu Malware dan Komplain *Spam*, dan 5 (lima) kategori lainnya yang mengalami penurunan jumlah pengaduan pada bulan kedua, yaitu bulan April. 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 Bulan II 2018

HaKI/IPR menduduki peringkat pertama untuk jumlah total pengaduan selama 2 (dua) bulan, Maret dan April, yaitu 10.553 pengaduan atau sebesar 51,12%. *Spam* berada di peringkat kedua dengan persentasi sebesar 25,46% atau sejumlah 5.256 pengaduan. Di peringkat ketiga ditempati oleh *Network Incident* dengan jumlah total 2 (dua) bulan 2.501 pengaduan atau sebesar 12,12%. Peringkat keempat dan kelima adalah *Malware* dan *Spoofing/Phishing*, dengan jumlah total masing-masing adalah 1.149 dan 676 pengaduan, atau sebesar 5,57% dan 3,27%. Komplain *Spam* dan Respon berada di peringkat terbawah dengan persentasi masing-masing sebesar 2,24% dan 0,22% dan mempunyai jumlah total sebesar 462 dan 46 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	Maret	April	%
Malware	517	632	22,24%
Komplain Spam	212	250	17,92%
Respon	24	22	-8,33%
Spoofing/Phishing	366	310	-15,30%
Spam	2.880	2.376	-17,50%
Network Incident	1.435	1.066	-25,71%
HaKI/IPR	6.513	4.040	-37,97%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

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

Kategori yang mengalami peningkatan jumlah adalah:

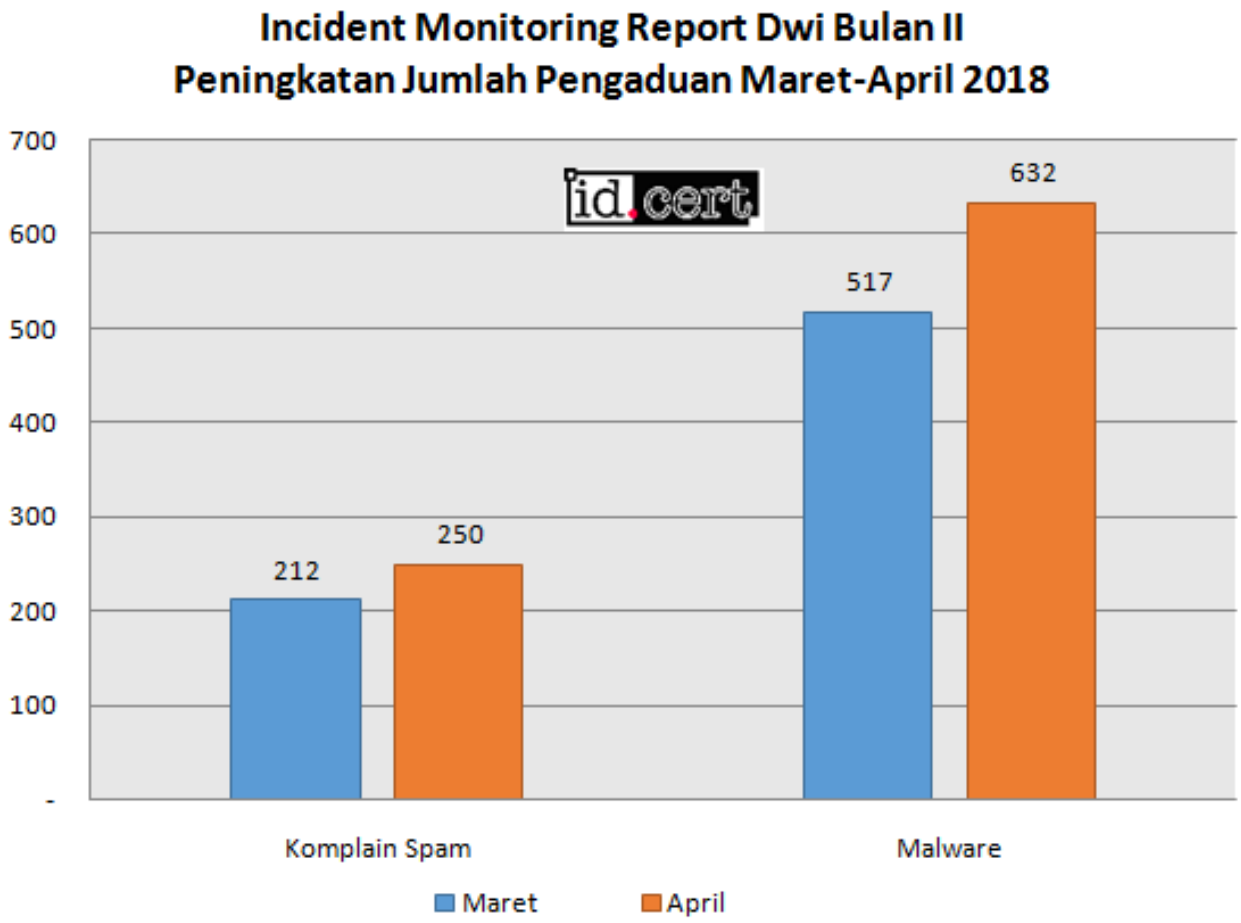
1. *Malware*

   Malware mengalami peningkatan jumlah sebesar 22,24%, yaitu 115 pengaduan. Peningkatan jumlah sebesar 115 pengaduan tersebut ketika pada bulan Maret berjumlah 517 pengaduan dan pada bulan April meningkat menjadi 632 pengaduan.

2. Komplain *Spam*

   Komplain *Spam* memiliki persentase peningkatan jumlah pengaduan sebesar 17,92%, atau meningkat 38 pengaduan. Di bulan Maret jumlah pengaduan sebesar 212 dan meningkat menjadi 250 di bulan April.

Berikut grafik peningkatan jumlah pengaduan yang terjadi selama bulan Maret dan April disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Maret-April 2018

3.2 Kelompok Pengaduan yang Mengalami Penurunan

Pada bulan Maret – April terdapat 5 (lima) kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. HaKI/IPR

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

37,97%, dan memiliki jumlah total pengaduan yang paling tinggi atau banyak selama 2 (dua) bulan tersebut. Penurunan jumlah sebesar 37,97% tersebut, atau 2.473 pengaduan, ketika pada bulan Maret berjumlah 6.513 pengaduan dan menurun menjadi 4.040 pada bulan April.

2. *Network Incident*

Network Incident memiliki jumlah penurunan pengaduan secara persentase sebesar 25,71%, atau sebesar 369 pengaduan. Jumlah 369 pengaduan tersebut karena di bulan Maret berjumlah 1.435 dan di bulan April menurun menjadi 1.066.

3. *Spam*

Spam mengalami penurunan jumlah pengaduan sebesar 504. Dari 2.880 pengaduan *Spam* di bulan Maret, menurun jumlahnya menjadi 2.376 di bulan April. Persentase penurunannya mencapai sebesar 17,50%.

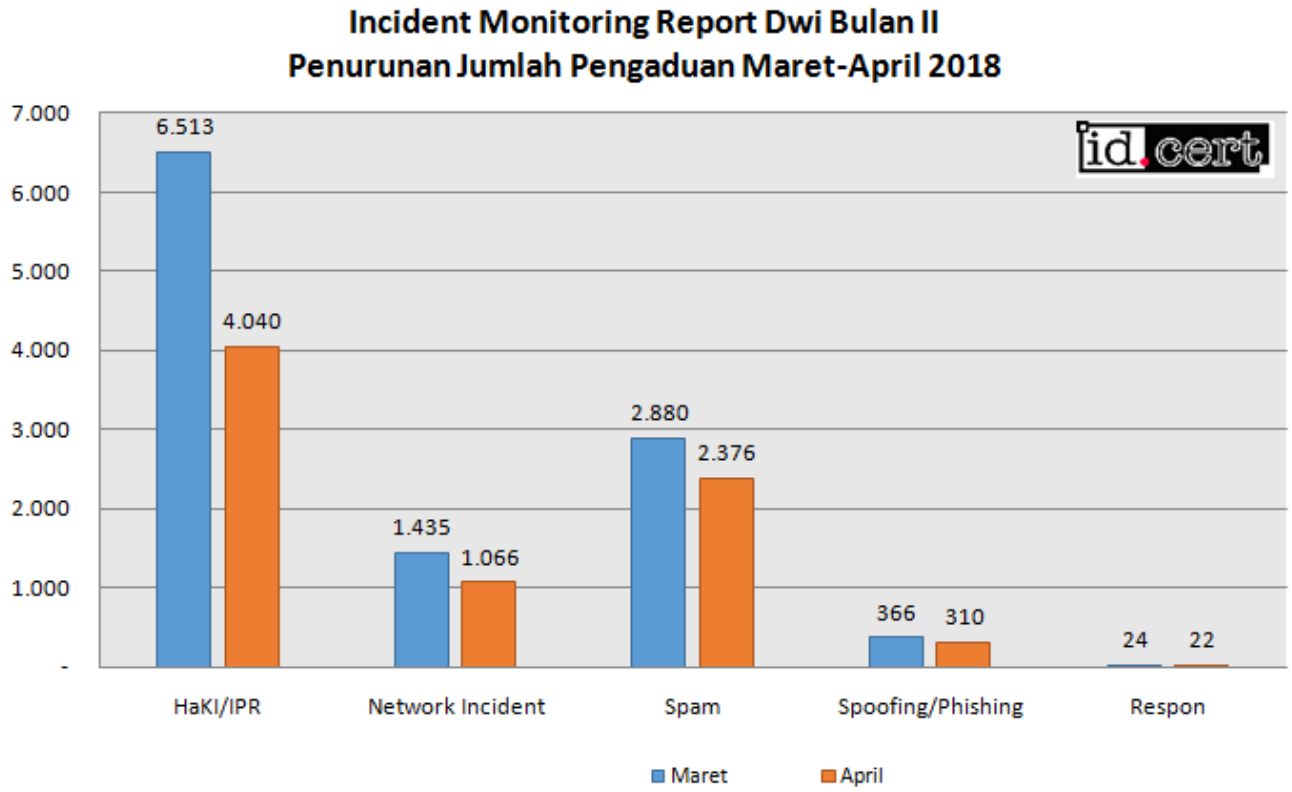
4. *Spoofing/Phishing*

Spoofing/Phishing mengalami penurunan jumlah pengaduan dari 366 pada bulan Maret dan turun sebesar 15,30%, yaitu 56, di bulan Maret dengan jumlah pengaduan sebanyak 310.

5. Respon

Respon hanya mengalami 2 (dua) jumlah penurunan dari bulan Maret sebesar 24 menjadi 22 di bulan April. Secara prosentase jumlah penurunan tersebut sebesar 8,33%.

Grafik penurunan jumlah pengaduan yang terjadi selama bulan Maret dan April disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Maret-April 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 mendisplinkan 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 II 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 II, 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