.INCIDENT MONITORING REPORT

.2012

LAPORAN DWI BULAN V TAHUN 2012

Bulan SEPTEMBER hingga OKTOBER

Edisi: UMUM

10 NOPEMBER 2012

Disusun oleh:

DIDUKUNG OLEH:

.DAFTAR ISI

I. PENGANTAR

Keamanan berinternet merupakan salah satu faktor terpenting dalam menjalankan usaha maupun bisnis.

Selain bertujuan memberikan deskripsi tentang insiden keamanan informasi di Indonesia, laporan ini juga dapat dijadikan contoh agar Indonesia mempunyai data primer tentang salah satu indikator keamanan informasi di Indonesia.

Terhitung mulai bulan Maret 2012, nama penelitian ini mengalami perubahan menjadi INCIDENT MONITORING REPORT 2012 dan berubah statusnya menjadi sebuah aktifitas permanen.

Setiap lembaga sangatlah penting menindaklanjuti berbagai keluhan/pengaduan yang diterimanya khususnya terkait insiden internet.

Keluhan/pengaduan yang terjadi menunjukkan betapa lemahnya sistem yang dibangun sehingga membutuhkan perbaikan ke depannya. Kita tentu tidak ingin, situs web yang kita bangun ditumpangi oleh *Malware* ataupun *Phishing* yang terkait dengan *Fraud* akibat lemahnya sistem yang kita bangun.

Tidak hanya sebatas menindaklanjuti keluhan/pengaduan, tetapi kita juga harus bisa lebih pro-aktif melaporkannya bila menjadi korban dari perilaku jahat di internet. ID-CERT ingin mendorong kepada komunitas maupun pengguna internet di Indonesia agar pro-aktif dalam melaporkan insiden internet yang terjadi untuk selanjutnya dapat dilakukan eskalasi penanganan insiden. Sejauh ini, langkah penanganan insiden dengan melibatkan CSIRT/CERT lainnya sangat memiliki peran yang signifikan, mengingat bahwa proses komunikasi antar CSIRT/CERT ditingkat Sektoral, Regional dan Internasional menggunakan jalur yang “terpercaya” dan memiliki prioritas tersendiri dalam penanganannya.

Dalam beberapa bulan terakhir ini, ID-CERT menerima lonjakan aduan *Malware* dan *Network Incident*. Hal ini akan menjadi sorotan edisi Dwi Bulan V tahun 2012 ini.

Dalam *Incident Monitoring Report* ini, kami berhasil mengambil data dari tiga puluh delapan (38) responden yang terdiri dari: **ID-CERT**, **PANDI**, **DETIK.NET, Zone-h, Anti Fraud Command Center (AFCC), RSA, Spamcop,** **3 Operator** Telekomunikasi, **6 NAP** dan **22 ISP**.

Statistik ini juga mendapatkan dukungan sponsor dari APJII dan PANDI.

II. Metodologi penelitian

Metodologi yang digunakan dalam penelitian ini adalah:

- Pengambilan data dari sejumlah responden.
- Metode analisis berdasarkan:

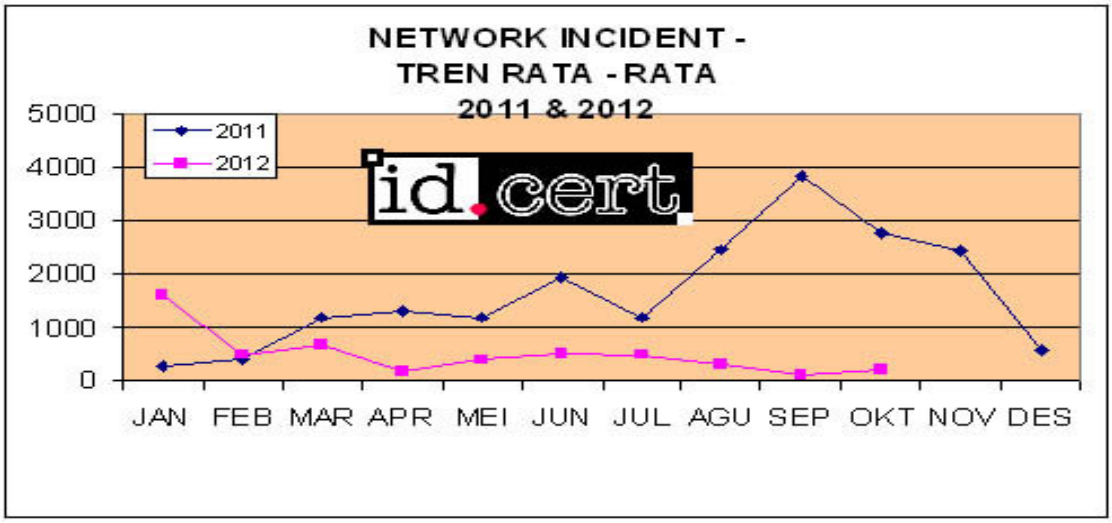
  B.1. Tembusan laporan yang masuk via email akun abuse ISP/ Operator Telekomunikasi/lembaga non-ISP.

  B.2. Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi yang dimaksud adalah: data-data yang telah dihitung dan dikategorisasi oleh responden tersebut.

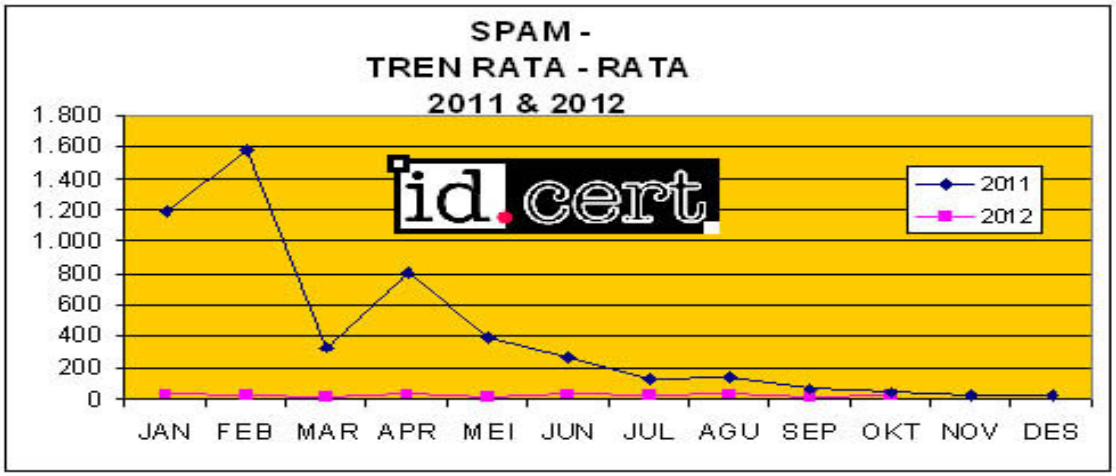
- Dari laporan tersebut, kami melakukan pengkategorian laporan sebagai berikut:

C.1.	Spam	Transmisi pesan-pesan massal yang tidak diminta
C.2.	Spam Komplain	Keluhan/pengaduan email spam dari dalam negeri terhadap network di Indonesia dan luar negeri
C.3.	Respon	Respon yang diberikan semua pihak terhadap laporan yang masuk
C.4.	Network Incident	Aktivitas yang dilakukan terhadap jaringan milik orang lain serta segala aktivitas terkait dengan penyalahgunaan jaringan
C.5.	Fraud	Laporan kepada penegak hukum/instansi terkait yang mengakibatkan kerugian finansial
C.6.	Spoofing/Phishing	Pemalsuan e-mail dan situs untuk menipu pengguna
C.7.	Malware	Sebuah program komputer yang dibuat dengan maksud jahat
C.8.	Lain-lain	Laporan penyalahgunaan yang diterima selain dari kategori yang ada di atas

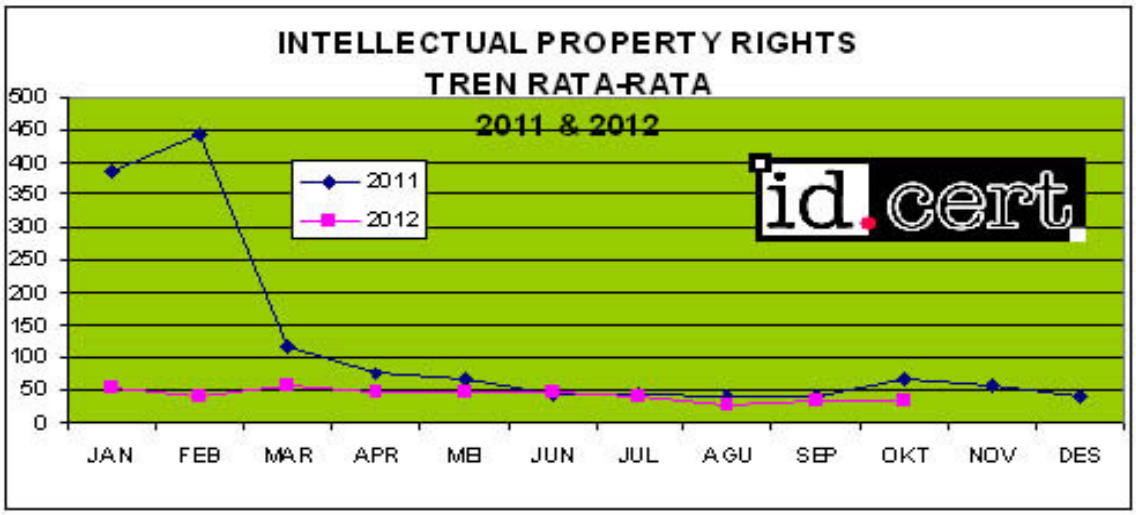
III. STATISTIK JANUARI – OKTOBER



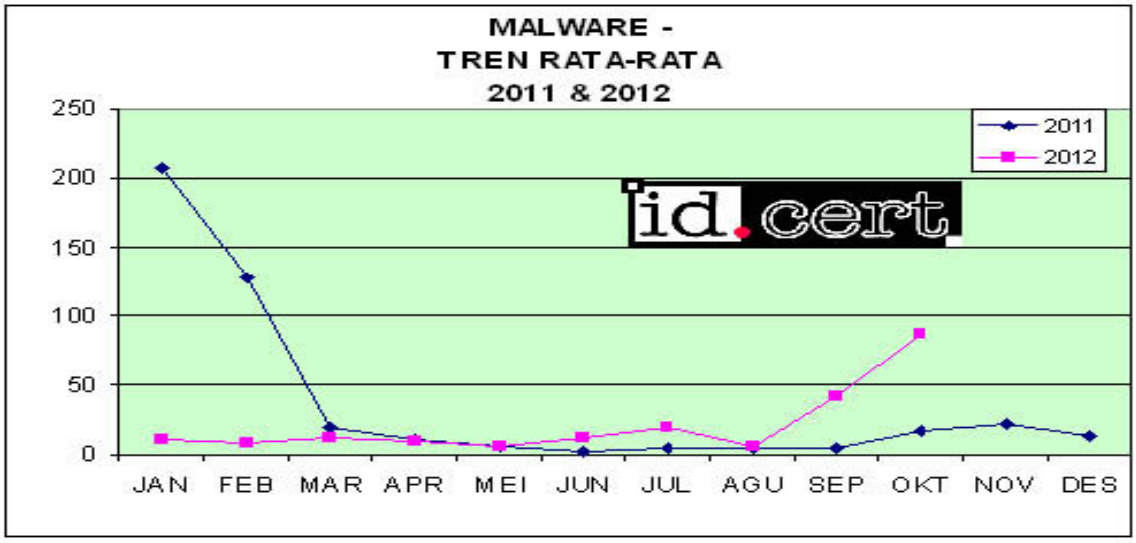
GRAFIK-I: Network Incident rata-rata



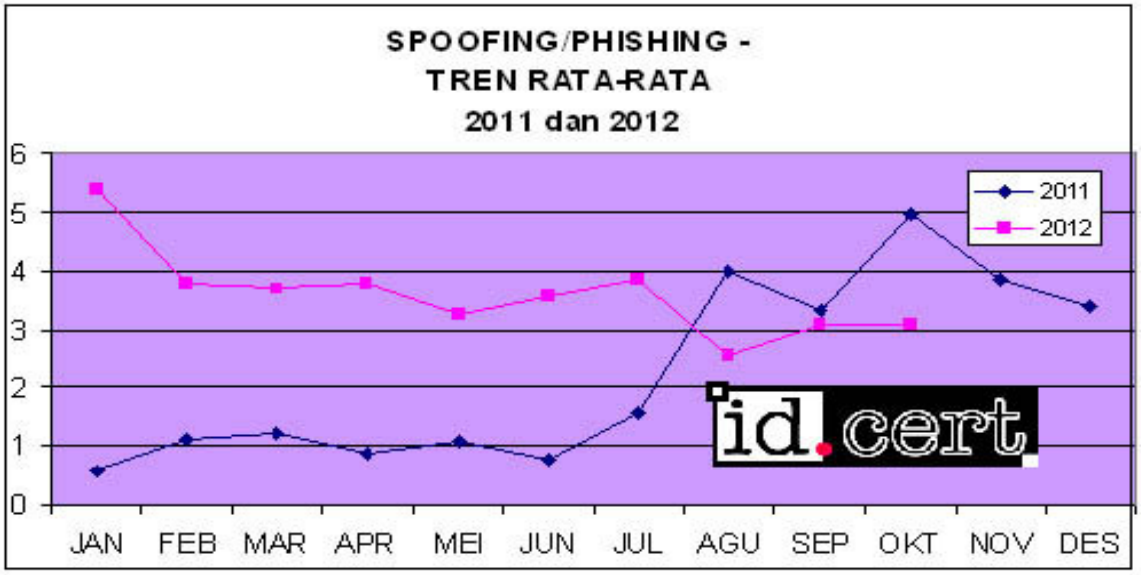
GRAFIK-II: Kategori SPAM rata-rata



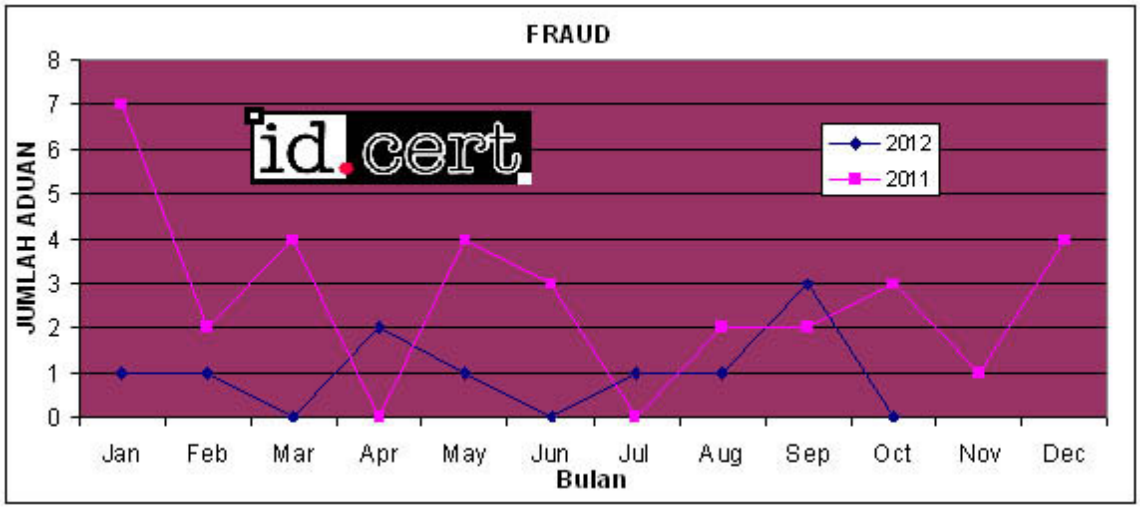
GRAFIK-III: IPR rata-rata



GRAFIK-IV: Malware rata-rata

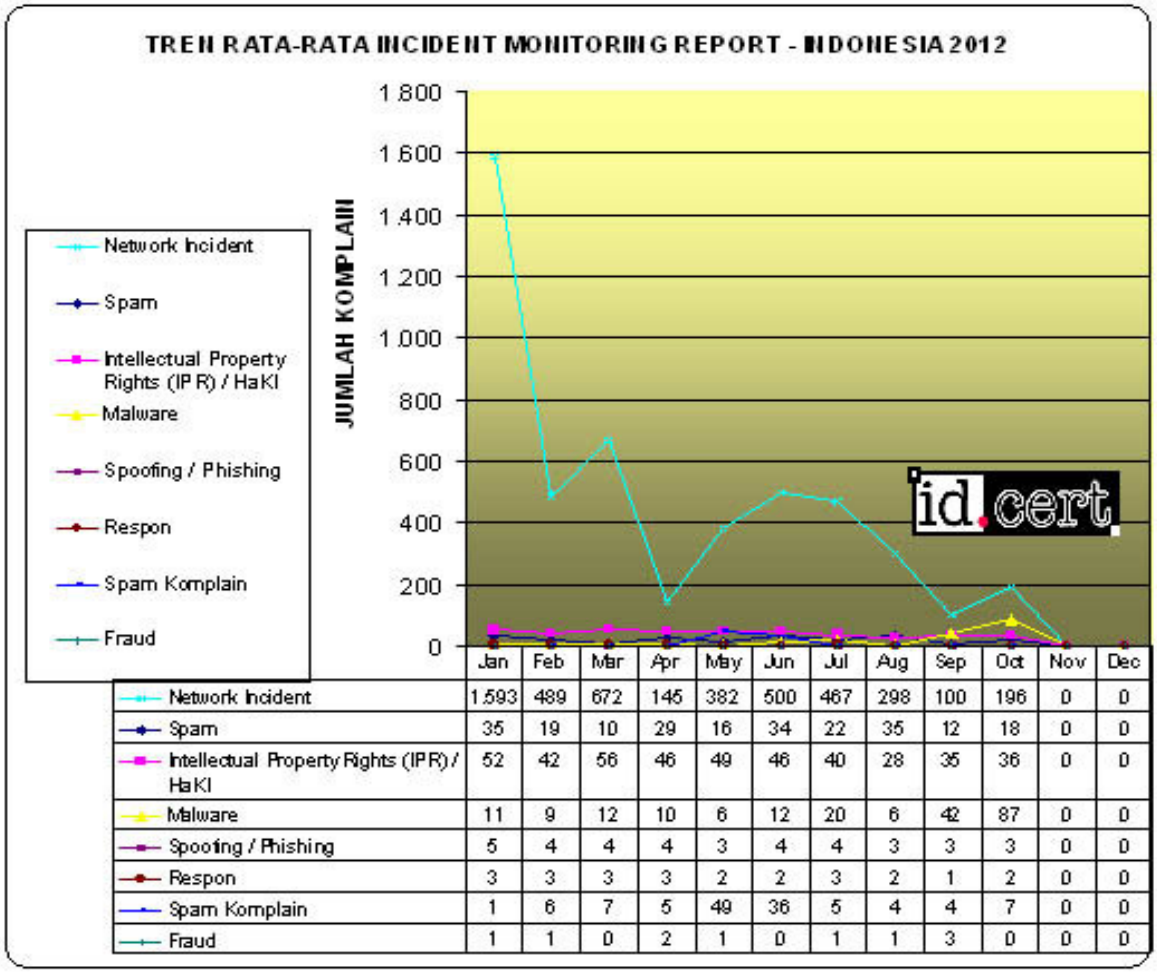


GRAFIK-V: Spoof/Phishing rata-rata



GRAFIK-VI: Laporan Fraud

IV. URAIAN



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Network Incident	1.593	489	672	145	382	500	467	298	100	196	0	0
Spam	35	19	10	29	16	34	22	35	12	18	0	0
Intellectual Property Rights (IPR) / HaKI	52	42	56	46	49	46	40	28	35	36	0	0
Malware	11	9	12	10	6	12	20	6	42	87	0	0
Spoofing / Phishing	5	4	4	4	3	4	4	3	3	3	0	0
Respon	3	3	3	3	2	2	3	2	1	2	0	0
Spam Komplain	1	6	7	5	49	36	5	4	4	7	0	0
Fraud	1	1	0	2	1	0	1	1	3	0	0	0

GRAFIK – VII: TREN RATA-RATA 2012

A. *Network Incident*

Posisi pertama tertinggi adalah Network incident.

Laporan terbanyak yang diterima pada bulan September hingga Oktober 2012 ini umumnya adalah *3 failed login (Brute Force), deface* dan *DDoS attack*.

Brute Force sangat berbahaya, mengingat cara kerja yang dilakukan oleh si penyerang adalah dengan menebak-nebak data kerahasiaan pengguna/sistem seperti username dan password. Dan ketika user name dan password diketahui, maka data tersebut akan dikumpulkan dan digunakan untuk kepentingan lainnya termasuk salah satunya diperdagangkan/dipertukarkan secara illegal kepada pihak lainnya.

B. Malware

Posisi kedua tertinggi adalah MALWARE. Posisi ini naik dibandingkan dwi bulan sebelumnya.

ID-CERT juga menerima lonjakan aduan terkait penyebaran Malware GRUMBOT pada kurun waktu 27 September hingga 02 Oktober dan kembali berlanjut pada 11 hingga 20 Oktober 2012. Selengkapnya mengenai Malware GRUMBOT dapat dibaca di website ID-CERT <http://www.cert.or.id/indeks_berita/berita/8/>

C. Intellectual Property Rights (IPR)/HaKI

Posisi ketiga tertinggi adalah kategori Intellectual Property Rights (IPR)/ HaKI. Yang termasuk dalam kategori ini adalah semua yang terkait dengan pelanggaran HaKI (Hak Atas Kekayaan Intelektual) baik itu untuk Piranti Lunak, musik maupun Film.

Umumnya pengirim keluhan/pengaduan ini berasal dari luar negeri.

D. Spam

Dari total laporan yang masuk, *SPAM* menduduki peringkat keempat dari total laporan rata-rata yang diterima.

E. Spam Komplain

SPAM KOMPLAIN menempati peringkat kelima.

Yang masuk pada kategori ini adalah laporan korban spam dari network di Indonesia maupun luar negeri. Jumlah ini mengalami sedikit penurunan di bulan April.

F. *Spoofing / Phishing*

Posisi keenam tertinggi adalah Spoofing/phishing.

Terdapat sejumlah situs Phishing yang menyebarkan *Malware.*

Laporan rata-rata pada bulan September hingga Oktober 2012 memiliki kecenderungan menurun.

Dalam masalah Phishing Finansial, terdapat sejumlah aduan yang terkait dengan login bank palsu, situs penyedia ijazah palsu dan situs aduan palsu.

Terkait dengan masalah situs penyedia Ijazah palsu, sebagian besar merupakan masalah hukum dan IPR karena mencantumkan nama institusi dan logo bank.

G. *Respon*

Respon menduduki posisi terakhir.

Kecenderungan respon pada periode ini mengalami sedikit penurunan.

Sedangkan bila dibandingkan dengan jumlah komplain keseluruhan, respon masih terbilang rendah. Adapun penyebabnya adalah selain setiap keluhan/pengaduan yang masuk tidak/belum direspon, dimungkinkan pula bahwa respon dilakukan tanpa ditembuskan dalam proses riset ini.

H. Fraud

Laporan terbanyak yang diterima (berdasarkan sumber dari salah satu instansi pemerintah) adalah pengaduan transaksi perdagangan melalui sejumlah situs seperti alibaba.com dan situs perusahaan ybs.

Adapun jenis transaksi yang dilakukan adalah secara Tunai/Transfer via bank (80%) yang didahului dengan kesepakatan setelah bertemu secara fisik (non-internet), permintaan verifikasi sebelum transaksi dilaksanakan (20%) dan sisanya adalah penyertaan bukti transfer palsu.

Adapun jumlah Negara yang mengadukan mencapai 9 negara dengan total nilai kerugian finansial yang mencapai USD **114.321** ditahun 2012 ini. Adapun potensi kerugiannya (bila transaksi terlaksana secara penuh) mencapai USD **187.776**.

Saat ini pengaduan dan penanganan kasus Fraud Perdagangan ditangani oleh Direktorat Pengamanan Perdagangan, DITJEN DAGLU, Kementrian Perdagangan RI yang beralamat di Gedung 2 Lantai 10 Jl. M.I Ridwan Rais No.5 Jakarta Pusat.

JUMLAH PERUSAHAAN YANG DIADUKAN	TAHUN PENGADUAN	KERUGIAN YANG DI TIMBULKAN	POTENSI KERUGIAN	JUMLAH NEGARA YANG MENGADU
20	2011	**USD 65.040**	**USD 113.599**	14
10	2012	**USD 114.321**	**USD 187.776**	9

Tabel - I: Kerugian akibat FRAUD tahun 2011 dan 2012

Sedangkan dari produk yang paling banyak dibeli adalah mulai dari Ban, Kertas, buah naga, produk permainan hingga garmen.

Dari 10 kasus yang dilaporkan pada tahun 2012 ini, terdapat 2 transaksi yang dilakukan secara *online* melalui: www.alibaba.com dan www.samudraexpress.com . Sedangkan sisanya, transaksi dilakukan secara konvensional melalui transfer Bank.

V. RANGKUMAN

Yang perlu menjadi perhatian adalah penyebaran Malware GRUMBOT yang mulai terdeteksi di Indonesia pada akhir September. Akibat ulah malware ini, setiap PC yang terinfeksi akan mengirimkan spam.

Berikut ini sejumlah rekomendasi :

A. Gunakan piranti lunak anti virus dan piranti lunak tambahan untuk mengurangi resiko *spam.*
B. Hindari pencantuman alamat email di tempat umum seperti di situs web, forum, dan sebagainya. Gantikan dengan formulir isian.
C. Laporkan kepada ID-CERT bila menjadi korban dari tindakan *abuse* internet.
D. Cantumkan formulir pengaduan Internet Abuse di setiap website.
E. Terkait dengan HaKI, sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai konten yang melanggar HaKI, karena ISP maupun penyelenggara konten memerlukan landasan hukum yang jelas untuk menurunkan suatu konten yang bermasalah.
F. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada pihak penegak hukum.

VI. UCAPAN TERIMA KASIH

Dalam kesempatan ini, kami ingin mengucapkan terima kasih kepada berbagai pihak atas dukungan yang diberikan sehingga riset ini dapat terlaksana dengan baik dan lancar.

Ucapan terima kasih kami sampaikan kepada seluruh responden yang telah berpartisipasi dalam riset ini, yang terdiri dari:

[A] – Kementrian Komunikasi dan Informatika [KEMKOMINFO]

[B] – Kementrian Perdagangan [KEMENDAG]

[C] – Pengelola Nama Domain Internet Indonesia [PANDI]

[D] – APJII

[E] – DETIK.NET

[F] – 3 Operator Telekomunikasi, 7 NAP dan 22 ISP.

[G] – Responden Luar Negeri: Anti Fraud Command Center (AFCC), Zone-h, Spamcop/Spamhaus dan RSA.

VII. DAFTAR PUSTAKA

[1] – Statistik Incident Monitoring Report ID-CERT
http://www.cert.or.id/incident_handling/

[2] – DNS Changer
https://www.hkcert.org/my_url/en/blog/12022901

[3] – APCERT Annual Reports 2011
http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2011.pdf

[4] – CERT Vulnerability Reporting forms
https://forms.cert.org/VulReport/

[5] – Messagelabs
http://www.symanteccloud.com/globalthreats/overview/r_mli_reports

[6] – RFC 5039, SIP and SPAM
http://tools.ietf.org/html/rfc5039

VIII. LAMPIRAN: Penyebaran Malware GRUMBOT

-------- Original Message --------
Subject: Malware GRUMBOT
Date: Thu, 18 Oct 2012 10:54:29 +0700
From: Ahmad Alkazimy - ID-CERT <ahmad@cert.or.id>
Reply-To: ahmad@cert.or.id
Organisation: ID-CERT (Indonesian Computer Emergency Response Team)
To: responden@cert.or.id, "diskusi@cert.or.id" <diskusi@cert.or.id>

Dear all,

Sejak tiga pekan terakhir, kami menerima laporan adanya sejumlah jaringan di IP Address Indonesia yang terkena Malware GRUMBOT.

Mengenai Grum botnet
==========
Grum botnet, juga dikenal dengan aliasnya Tedroo dan Reddyb, dulunya adalah botnet (http://en.wikipedia.org/wiki/Botnet) yang paling terlibat dalam pengiriman spam-spam e-mail (http://en.wikipedia.org/wiki/E-mail_spam) farmasi.[1] Pernah menjadi botnet terbesar di dunia, Grum dapat dilacak di awal 2008.[2] Grum dilaporkan bertanggung jawab atas 18% trafik spam di seluruh dunia pada saat ditutup pada tgl 19 Juli 2012.[3][4]

Grum memakai 2 tipe server kontrol untuk operasinya. 1 tipe digunakan mem-push update konfigurasi ke komputer2 yang terinfeksi, dan 1 tipe lainnya digunakan untuk memberi perintah ke botnet jenis spam email apa yang harus dikirimkan.[5]

Di bulan Juli 2010, botnet Grum terdiri dari sekitar 560.000-840.000 komputer yang diinfeksi dengan rootkit (http://en.wikipedia.org/wiki/Rootkit) Grum.[6][7] Botnetnya sendiri mengirimkan sekitar 39,9 milyar[8] pesan spam di bulan Maret 2010, sebesar sekitar 26% dari total global volume spam di sleuruh dunia, dan untuk sementara waktu menjadikan Grum sebagai botnet terbesar di dunia.[9][10] Pada akhir tahun 2010, botnet tersebut tampaknya semakin membesar, karena output meningkat kira-kira sebesar 51% bila dibandingkan dengan output tahun 2009 dan awal 2012.[11][12]

Grum menggunakan suatu panel yang ditulis dengan PHP (http://en.wikipedia.org/wiki/PHP) untuk mengontrol botnet.

Botnet "dimatikan"
==========
Pada bulan Juli 2012, perusahaan intelejen malware FireEye (http://en.wikipedia.org/wiki/FireEye) menerbitkan sebuah analisis (http://blog.fireeye.com/research/2012/07/killing-the-beast-part-5.html) mengenai (keberadaan) server-server command dan control (http://en.wikipedia.org/wiki/Command_and_control) botnet yang terletak/berlokasi di Belanda, Panama, dan Rusia. Satu minggu setelah analisis tersebut terbit, para peneliti FireEye melaporkan bahwa Colo/ISP Belanda langsung menangkap 2 server sekunder

yang bertanggung jawab mengirimkan instruksi spam setelah keberadaan 2 server tersebut dibuat publik.[13] Dalam waktu 1 hari, ISP Panama yang menjadi hosting salah satu server utama Grum dituntut dan menutup/mematikan server mereka.[14] Para kriminal cyber di belakang/yang mendalangi Grum dengan cepat meresponnya dengan mengirim instruksi melalui 6 server baru di Ukraina. [15] FireEye yang terhubung dengan Spamhaus (http://en.wikipedia.org/wiki/Spamhaus), CERT-GIB, dan seorang peneliti anonim untuk menutup/mematikan 6 server C&C yang tersisa, secara resmi mematikan botnet pada tgl 18 Juli 2012.[15]

LANGKAH ANTISIPASI:
==========
1. Segera update Patch OS anda

2. Segera update Antivirus dan lakukan pengecekan secara rutin.

BAHAN BACAAN:
==========
http://www.exterminate-it.com/malpedia/remove-grum

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

Terima kasih,

--

SEND YOUR INCIDENT REPORTS TO: <cert@cert.or.id>

KIRIMKAN KOMPLAIN INTERNET ABUSE YANG TERJADI,KE: <cert@cert.or.id>

AHMAD KHALIL ALKAZIMY,ST
INCIDENT RESPONSE TEAM
INDONESIA COMPUTER EMERGENCY RESPONSE TEAM (ID-CERT)
email: <ahmad@cert.or.id>
http://www.cert.or.id/
SKYPE/YM ID: ahmadkaz
HP: (+62)83-874-9292-15
Contact Desk: (+62)889-1400-700
==========