LAPORAN SURVEY MALWARE

PERIODE

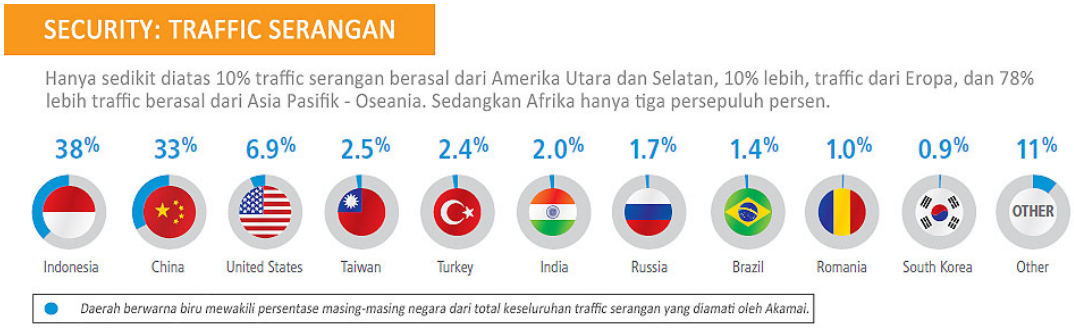
APRIL - MEI 2014

Daftar Isi

Bab 1

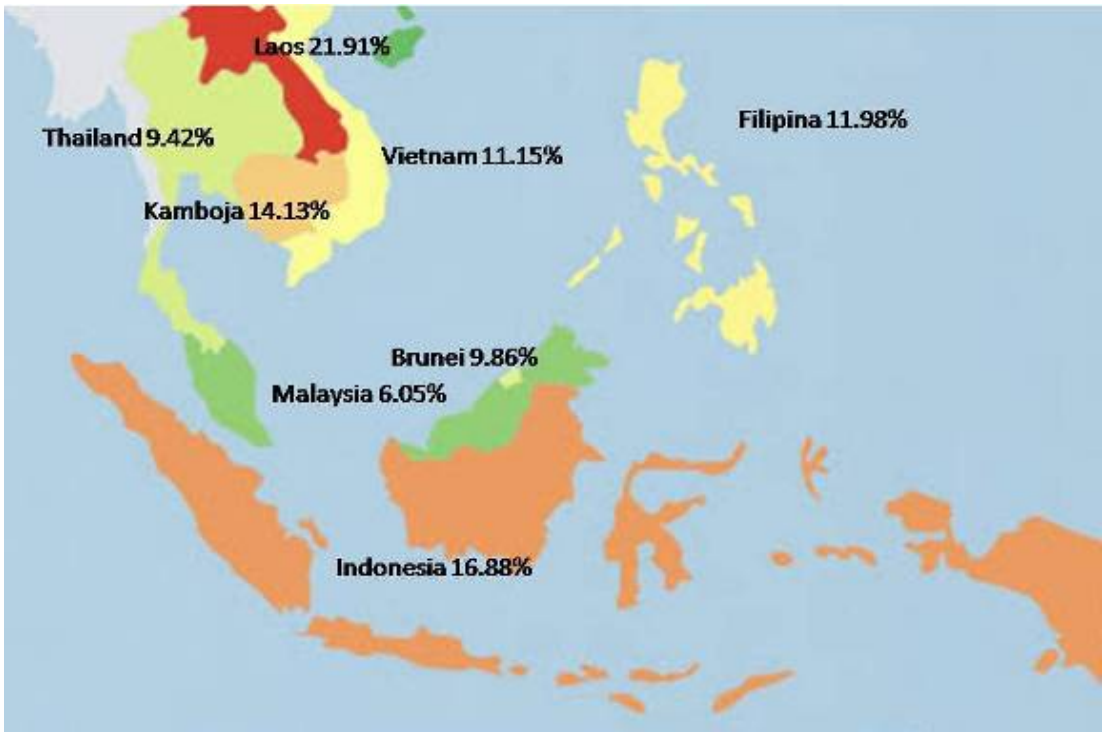
Pendahuluan

Pada tahun 2013 Akamai melaporkan Indonesia menjadi negara nomor 1 sumber serangan Internet (malicious traffic) [Akamai, 2013]. Trafik serangan dari IP Indonesia berkisar 38% dari seluruh serangan di Internet dibandingkan trafik dari sekitar 175 negara yang diteliti. Trafik serangan ini meningkat hampir dua kali lipat dibandingkan data sebelumnya yaitu sekitar 21%. Akamai dalam laporan tersebut menyatakan bahwa IP yang terdeteksi sebagai sumber serangan bisa jadi tidak mencerminkan lokasi penyerang. Karena bisa saja seorang penyerang dari Amerika Serikat melancarkan serangan dari IP Indonesia melalui jaringan botnet atau komputer yang terinfeksi malware. Grafik laporan serangan dapat terlihat pada gambar 1.1.



Gambar 1.1: Trafik Serangan Akamai [Akamai, 2013][Akamai, 2013]

Selain itu ESET Indonesia pada bulan Mei 2013 melaporkan tingkat prevelansi malware Indonesia di ASEAN cukup tinggi yaitu sebesar 16,88% [Eset, 2013]. dari laporan tersebut malware yang banyak beredar di Indonesia diantaranya adalah Ramnit, Sality dll [Radar, 2013]. Peta laporan prevalensi malware dapat dilihat pada gambar 1.2.



Gambar 1.2: Prevalensi Malware ASEAN[Eset, 2013]

Kedua laporan diatas mengindikasikan tingginya tingkat penyebaran malware di Indonesia. Sayangnya belum ada penelitian yang dapat memetakan bagaimana sesungguhnya penyebaran malware di Indonesia. Data penyebaran malware ini dapat digunakan untuk mempelajari aktifitas malware di Indonesia serta langkah-langkah penanganan yang dapat diambil.

Untuk itulah ID-CERT (*Indonesia Computer Emergency Response Team*) menggagas survey malware [ID-CERT, 2014]. Diharapkan dari penelitian ini dapat diperoleh data-data real tentang penyebaran malware di Indonesia.

Bab 2

Survey Malware ID-CERT

Survey Malware ID-CERT bertujuan untuk mendapatkan data tentang penyebaran malware di Indonesia. Survey dilakukan dengan menyebarkan Flash-Disk berisikan aplikasi pemindai malware (*antivirus*) kepada para relawan. Relawan diharuskan mendaftar terlebih dahulu dengan mengirimkan email berisi identitas dan kota asal. Kemudian relawan diminta melakukan pendeteksian malware (*scanning*) pada komputer atau laptop yang dimiliki dengan aplikasi tersebut. Setelah pendeteksian malware selesai, relawan diminta mengirimkan hasil scanning (*report*) ke email ID-CERT. ID-CERT kemudian mengumpulkan hasil report dan melakukan analisa. Hasil analisa yang didapatkan adalah data tentang penyebaran malware di Indonesia.

Aplikasi antivirus yang digunakan adalah Emsisoft [EmsiSoft, 2014]. Selain itu dikembangkan juga aplikasi untuk melakukan parsing email report ke database. Database yang digunakan adalah MySQL [MySQL, 2014]. Mail Server yang digunakan adalah Squirrelmail [Squirrelmail, 2014].

2.1 Anggota Tim

Berikut kami laporkan anggota tim Survey Malware ID-CERT.

Ketua	: Budi Rahardjo	- ID-CERT
Anggota	: Ahmad Alkazimy	- ID-CERT
	: Abdul Rahim	- Pemkot Cirebon
	: Aries Syamsuddin	- Pemda Blitar
	: Samuel Cahyawijaya	- ITB
	: Arya Dhanang	- ITB
	: Hadi Rasyid Sono	- ITB
	: Setia Juli Irzal Ismail	- Telkom University

Bab 3

Laporan Kegiatan

Pada bab ini kami laporkan hasil kegiatan survey malware ID-CERT sampai bulan Juni 2014. Kegiatan survey malware telah dimulai sejak bulan Januari 2014. Pengembangan aplikasi dilakukan sejak Januari 2014. Pengujian telah dilakukan pada bulan Februari 2014. Penyebaran USB dan aplikasi kepada para relawan telah dimulai sejak bulan Maret 2014.

3.1 Daftar Relawan

Daftar relawan yang telah mendaftar dapat dilihat pada tabel 3.1.

Dari daftar relawan terlihat Survey malware ID-CERT diikuti 37 relawan yang berasal dari 23 kota dan 9 propinsi di Indonesia. Relawan paling banyak berasal dari kota Bandung sebanyak 10 orang. Sebaran kota asal relawan adalah sebagaimana pada gambar 3.1. Dari daftar relawan terlihat jumlah relawan masih sedikit dan belum dapat merepresentasikan penyebaran malware di Indonesia. Hal ini dikarenakan survey malware masih pada tahap awal. Pada tahap ini ID-CERT masih berkonsentrasi mengembangkan sistem dan perangkat survey malware yang tepat. Diharapkan ada pihak atau lembaga yang mau berperan serta untuk mensosialisasikan kegiatan ini dan membantu penyebaran Flash-disk survey malware.

Gambar 3.1: Kota Asal Relawan [Geographic, 2014]

3.2 Daftar Malware

Sementara daftar malware yang berhasil dilaporkan adalah dapat dilihat pada tabel 3.2.

Terlihat hanya terdapat data penyebaran malware dari 2 kota yaitu Cirebon dan Bandung. Hal ini dikarenakan belum semua relawan melaporkan hasil scanning. Sedangkan data hasil report dari Jakarta bukanlah malware. EICAR-ANTIVIRUS-TESTFILE merupakan file yang digunakan untuk menguji Antivirus.

3.3 Teknis Pelaksanaan

Scanning malware dilakukan dengan memberikan Flash Disk yang berisi antivirus Emsisoft. Selain itu relawan juga dapat mengunduh file dari link yang diberikan. Petunjuk pelaksanaan Survey Malware yang diberikan kepada para relawan adalah sebagai berikut:

1. kirim email ke daftar@malware.cert.or.id dengan keterangan nama lengkap, kota tinggal dan email anda;

2. unduh aplikasi yang digunakan untuk scan malware, di http://is.gd/idcert atau dari tautan https://www.dropbox.com/sh/n8gwludssk95odx/TrkFpnf49f lalu pilih download as .zip (agar mudah dapat didownload dalam format .zip); setelah selesai didownload, lalu ekstrak file Emsisoft Emergency Kit.zip;
3. jalankan start.exe yang terdapat pada folder Emsisoft Emergency Kit;
4. pilih Emergency Kit Scanner -> Scan PC;
5. pilih metode scan sesuai kebutuhan (Quick Scan, Smart Scan, Deep Scan, Custom Scan);
6. tekan tombol 'Scan'; Tunggu sampai scan selesai;
7. tekan tombol 'View Report' dan folder log akan terbuka;
8. kirimkan melalui email file log tersebut ke lapor@malware.cert.or.id (file report tersimpan pada folder /Run/Report/.....).

Scanning dilakukan hanya pada komputer dengan OS Windows. Bila ada pertanyaan bisa hubungi email berikut support@malware.cert.or.id atau ahmad@cert.or.id via email.

Tabel 3.1: Daftar Relawan

No	Nama	Kota Asal
1	Abdul Rahim	Cirebon
2	Abdul	Bandung
3	Akbar Dwi Prastyo	Banjarbaru
4	Andhika Prasetian	Bandar Lampung
5	Andri Trismanto	Magelang
6	Andy Pramurjadi	Cianjur
7	Aries Syamsuddin	Bandung
8	Cendrayani Rekza Legawati	Sidoarjo
9	Fais Al Huda	Malang
10	Galih Rizky	Bogor
11	Gilang Fahreza Alfisyahrin	Depok
12	Harits Andi	Makassar
13	Andi Harits	Bandung
14	Idan Misdani	Bandung
15	Ika Sapto Hadi	Bekasi
16	Indra Ramadhan	Tangerang
17	Ismayana Teguh Pratama	Sukabumi
18	Ketut Artayasa	Bali
19	Laurensius Jeffrey Chandra	Bandung
20	Lily	Kuningan
21	Mukti Priagung Wicaksana	Tulungagung
22	Musanni Fauziah	Mandailing Natal
23	Nurul Anisah	Jakarta
24	Nurwin	Bandung
25	Oktavianus Dudung	Bekasi
26	Onny Rafizan	Jakarta
27	Rahmatika putri	Medan
28	Rian Widi Ramdani	Bandung
29	Risnandar	Bandung
30	Seni Meilani Putri	Bandung
31	Sofyan Hadi	Jakarta
32	Syaifudin Amrozi	Surabaya
33	Syarief	Bandung
34	Wisnu Nurdiyanto	Palu
35	Yuddy Mardyana	Cikarang
36	Yusa Inderapermana	Cirebon
37	Yusfa Anugrah Baihaki	Surabaya

Tabel 3.2: Daftar Malware

No	Nama Malware	Kota Asal
1	MemScan:Trojan.Generic.3268307(B)	Cirebon
2	Trojan.Generic.7320471(B)	Cirebon
3	Generic.Malware.SPDVTk.2C83EFBE(B)	Cirebon
4	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Cirebon
5	Trojan.Generic.7320471(B)	Cirebon
6	Generic.Malware.SPDVTk.2C83EFBE(B)	Cirebon
7	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Cirebon
8	Trojan.Generic.7890946(B)	Cirebon
9	Gen:Variant.Application.MediaFinder.1(B)	Cirebon
10	Gen:Variant.Application.MediaFinder.1(B)	Cirebon
11	Gen:Variant.Application.MediaFinder.1(B)	Cirebon
12	Gen:Variant.Application.MediaFinder.1(B)	Cirebon
13	Gen:Variant.Application.MediaFinder.1(B)	Cirebon
14	Trojan.Generic.6265065(B)	Cirebon
15	MemScan:Trojan.Generic.3268307(B)	Bandung
16	Trojan.Generic.7320471(B)	Bandung
17	Generic.Malware.SPDVTk.2C83EFBE(B)	Bandung
18	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Bandung
19	Trojan.Generic.7320471(B)	Bandung
20	Generic.Malware.SPDVTk.2C83EFBE(B)	Bandung
21	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Bandung
22	Trojan.Generic.7890946(B)	Bandung
23	Gen:Variant.Application.MediaFinder.1(B)	Bandung
24	Gen:Variant.Application.MediaFinder.1(B)	Bandung
25	Gen:Variant.Application.MediaFinder.1(B)	Bandung
26	Gen:Variant.Application.MediaFinder.1(B)	Bandung
27	Trojan.Generic.6265065(B)	Bandung
28	EICAR-ANTIVIRUS-TESTFILE!E2	Jakarta
29	EICAR-ANTIVIRUS-TESTFILE!E2	Jakarta
30	EICAR-ANTIVIRUS-TESTFILE!E5	Jakarta
31	EICAR-ANTIVIRUS-TESTFILE!E8	Jakarta
32	EICAR-ANTIVIRUS-TESTFILE!E9	Jakarta

Bab 4

Evaluasi

Pada bab ini kami laporkan hasil evaluasi tim terhadap jalannya survey malware sampai bulan Juni 2014.

4.1 Proses Pendaftaran

Relawan diharuskan untuk mendaftarkan diri terlebih dahulu dengan mengirimkan email yang berisi, nama, kota asal dan alamat email. Pendaftaran dimaksudkan agar diketahui identitas dan kota asal dari para relawan. Proses pendaftaran dilakukan dengan mengirimkan email ke daftar@malware.cert.or.id. Hasil evaluasi dari proses pendaftaran adalah disarankan agar proses pendaftaran dipermudah. Sehingga diusulkan proses pendaftaran dilakukan otomatis ketika user membuka antivirus. Untuk itu sedang dikembangkan aplikasi yang mengintegrasikan proses registrasi dengan antivirus.

4.2 Aplikasi Antivirus

Survey malware saat ini menggunakan aplikasi antivirus Emsisoft. Alasan penggunaan antivirus ini adalah antivirus tidak perlu proses instalasi terlebih dahulu. Hasil evaluasi dari para relawan terhadap antivirus ini adalah sebagai berikut:

1. proses scanning lama;

2. antivirus ini dinilai memiliki kemampuan deteksi malware yang kurang baik.

Untuk mengatasi masalah ini sedang dikembangkan aplikasi baru yang menggunakan antivirus ClamAV [ClamAV, 2014].

4.3 Proses Pelaporan

Setelah relawan melakukan pemindaian malware (*scanning*), relawan diminta untuk mengirimkan hasil *scanning (report)* ke email lapor@malware.cert.or.id. Hasil yang dikirimkan adalah file log yang terdapat pada folder /Run/Report. Hal ini dianggap menyulitkan relawan. Untuk itu disarankan proses pelaporan diintegrasikan dengan aplikasi, sehingga pelaporan dijalankan secara otomatis.

4.4 Parsing Email

Setelah relawan melaporkan hasil scanning dengan mengirimkan email ke alamat diatas, maka sistem akan melakukan proses parsing email ke database. Proses *parsing* dimaksudkan untuk memindahkan hasil scanning ke database secara otomatis. Aplikasi *parsing* telah dikembangkan. Hanya saja dari hasil evaluasi, proses parsing ini belum berjalan dengan baik. Masih ada beberapa email yang belum berhasil dipindahkan ke database. Kemudian masih ada beberapa email yang masuk ke folder *spam*. Untuk itu sedang dilakukan proses perbaikan dan *debugging* aplikasi parsing ini. Database yang digunakan adalah MySQL. Email server yang digunakan adalah Postfix.

4.5 Partisipasi Relawan

Sampai bulan Juni 2014, relawan yang mengikuti kegiatan ini hanya berjumlah 37 orang dari 23 kota dan 9 propinsi di Indonesia. Jumlah ini belum dapat merepresentasikan sebaran malware di Indonesia. Hal ini dikarenakan penelitian masih dalam tahap awal. Dimana ID-CERT masih fokus mengembangkan sistem yang stabil dan handal yang dapat digunakan untuk survey malware ini. ID-CERT mengharapkan ada pihak maupun instansi yang mau berperan serta untuk mensosialisasikan kegiatan ini.

Daftar Pustaka

Akamai. Akamai second quarter 2013 'state of the internet' report, Oktober 2013. URL http://www.akamai.com/html/about/press/releases/2013/press_101613.html.

ClamAV. Clam anti virus, Juni 2014. URL http://www.clamav.net/lang/en/.

EmsiSoft. Emsisoft anti malware, Juni 2014. URL http://www.emsisoft.de/en/.

Eset. Prevalensi malware di indonesia dan asean 2013, Juni 2013. URL http://blog.eset.co.id/index.php/jagatmaya-indonesia-mei-2013-backdoor-apache-malware-android-dan-terkotor-kedua-se-asean/.

National Geographic. National geographic interactive map, Juni 2014. URL http://education.nationalgeographic.com/education/mapping/interactive-map/?ar_a=1.

ID-CERT. Indonesia computer emergency response team, Juni 2014. URL http://www.cert.or.id/.

MySQL. Mysql the world's most popular open source database, Juni 2014. URL http://www.mysql.com/.

Virus Radar. Prevalensi malware indonesia, Mei 2013. URL http://virusradar.com/en/reports.

Squirrelmail. Squirrelmail, webmail for nuts, Juni 2014. URL http://squirrelmail.org/.