LAPORAN SURVEY MALWARE

PERIODE
JANUARI-MEI
2015

DIDUKUNG OLEH

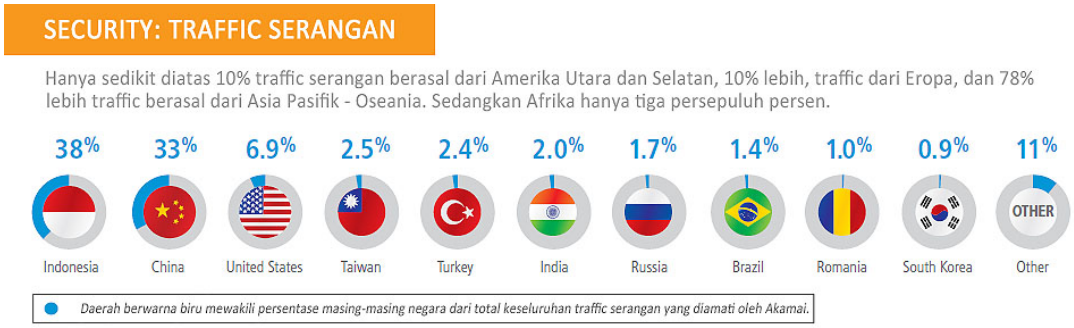
KEMKOMINFO

Daftar Isi

Bab 1

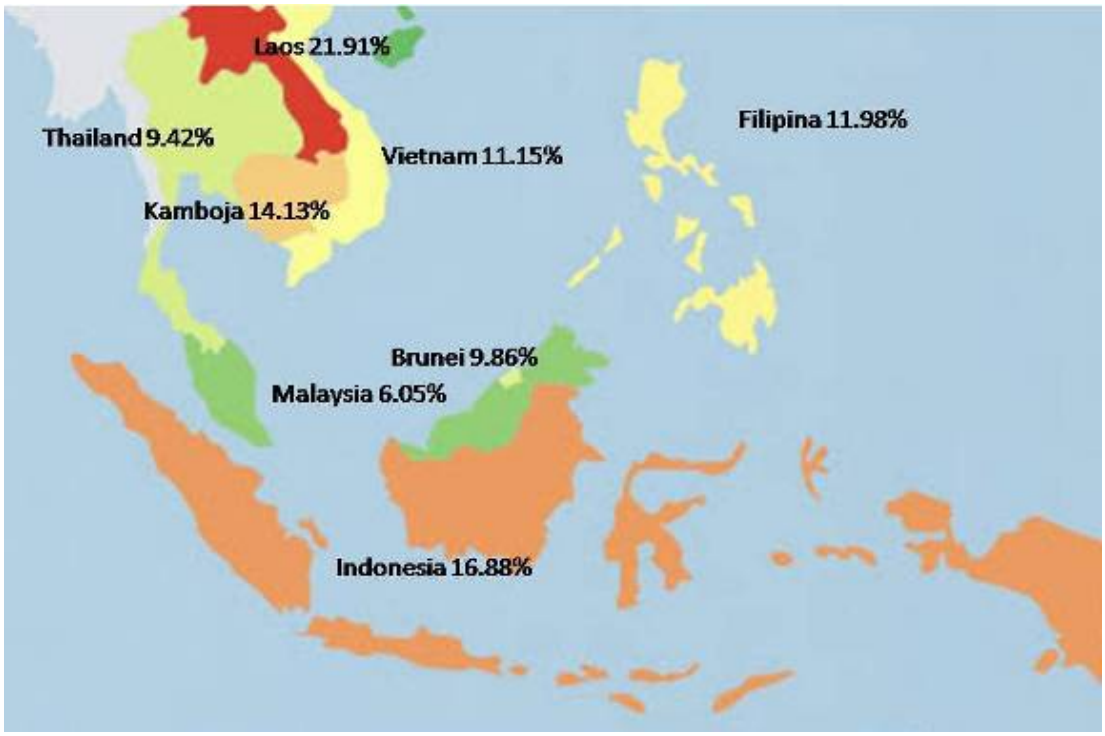
Pendahuluan

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]

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 Postfix [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 akhir bulan Mei 2015. 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.

Tabel 3.1: Tabel Relawan

No	Nama	Kota Asal
1	Abdul	Bandung
2	Abdul Rahim	Cirebon
3	Ahmad Khalil Alkazimy	Jakarta
4	Akbar Dwi Prastyo	Banjarbaru
5	Andhika Prasetian	Bandar Lampung
6	Andi Harits	Makasar
7	Andri Trismanto	Magelang
8	Andy Pramurjadi	Cianjur
9	Aries Syamsuddin	Blitar

Tabel 3.1: Tabel Relawan

No	Nama	Kota Asal
10	Cendrayani Rekza Legawati	Sidoarjo
11	David Setiadi	Sumedang
12	Dwiki Nurrahman	Bekasi
13	Fais Al Huda	Malang
14	Fatnan Ahmad Thawsan	Bandung
15	Galih Rizky	Bogor
16	Gilang Fahreza Alfisyahrin	Depok
17	Harits Andi	Makasar
18	Idan Misdani	Bandung
19	Ika Sapto Hadi	Bekasi
20	Ilham Ismail	Padang
21	Indra Ramadhan	Tangerang
22	Irfan Saepulloh	Bandung
23	Ismayana Teguh Pratama	Sukabumi
24	Ketut Artayasa	Bali
25	Laurensius Jeffrey Chandra	Tangerang
26	Lily	Kuningan
27	Meutia Rahmatika	Jakarta
28	Mukti Priagung Wicaksana	Tulungagung
29	Musanni Fauziah	Mandailing Natal
30	Nanik Ramini	Serpong
31	Nurul Anisah	Jakarta
32	Nurwin	Bandung
33	Oktavianus Dudung	Bekasi
34	Onny Rafizan	Jakarta
35	Otong Surotong	Jakarta
36	Rahmatika Putri	Medan
37	Rian Widi Ramdani	Bandung
38	Risnandar	Bandung
39	Rivalda Maulana	Bandung
40	Rizky Ferdiansyah	Bandung
41	Satriyo Adi Negara	Bandung
42	Seni Meilani Putri	Bandung

Tabel 3.1: Tabel Relawan

No	Nama	Kota Asal
43	Sofyan Hadi	Jakarta
44	Syaifudin Amrozi	Surabaya
45	Syarief	Bandung
46	Wisnu Nurdiyanto	Palu
47	Yuddy Mardyana	Cikarang
48	Yudha Tri Putra	Depok
49	Yunizar Muhammad	Jakarta
50	Yusa Inderapermana	Cirebon
51	Yusfa Anugrah Baihaki	Surabaya

Dari daftar relawan terlihat Survey malware ID-CERT diikuti 51 relawan yang berasal dari 27 kota dan 12 propinsi di Indonesia. Relawan paling banyak berasal dari kota Bandung sebanyak 13 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. 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. Sementara daftar sebaran provinsi para relawan survey malware dapat dilihat pada tabel 3.2

Tabel 3.2 Daftar Provinsi

No	Daftar Propinsi
1	Sumatera Utara
2	Sumatera Barat
3	Lampung
4	Jawa Barat
5	Jakarta
6	Banten
7	Jawa Tengah
8	Jawa Timur

No	Provinsi
9	Bali
10	Kalimantan Selatan
11	Sulawesi Selatan
12	Sulawesi Utara

Gambar 3.1: Kota Asal Relawan [Geographic, 2014]

3.2 Daftar Malware

Sementara daftar malware yang berhasil dilaporkan adalah dapat dilihat pada tabel 3.3

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
1	MemScan:Trojan.Generic.3268307(B)	Bandung
2	Trojan.Generic.7320471(B)	Bandung
3	Generic.Malware.SPDVTk.2C83EFBE(B)	Bandung

Tabel 3.3: Tabel Malware

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

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
37	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Kuningan
38	Trojan.Generic.7320471(B)	Kuningan
39	Generic.Malware.SPDVTk.2C83EFBE(B)	Kuningan
40	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Kuningan
41	Trojan.Generic.7890946(B)	Kuningan
42	Gen:Variant.Application.MediaFinder.1(B)	Kuningan
43	Gen:Variant.Application.MediaFinder.1(B)	Kuningan
44	Gen:Variant.Application.MediaFinder.1(B)	Kuningan
45	Gen:Variant.Application.MediaFinder.1(B)	Kuningan
46	Gen:Variant.Application.MediaFinder.1(B)	Kuningan
47	Trojan.Generic.6265065(B)	Kuningan
48	Trace.File.Bejeweled2Deluxe1.0(A)	Cirebon
49	Trace.File.FeedingFrenzy2(A)	Cirebon
50	Trace.Registry.FeedingFrenzy2(A)	Cirebon
51	Trace.File.Bejeweled2Deluxe1.0(A)	Cirebon
52	Trace.File.FeedingFrenzy2(A)	Cirebon
53	Trace.Registry.FeedingFrenzy2(A)	Cirebon
54	Trace.Registry.BaiduBar(A)	Cirebon
55	Trace.Registry.PCTuneUp(A)	Makasar
56	Trace.Registry.PCTuneUp(A)	Makasar
57	Trace.Registry.BaiduBar(A)	Makasar
58	Gen:Trojan.Heur.GM.000C040880(B)	Malang
59	Backdoor.Perl.IRCBot.AM(B)	Malang
60	Trojan.Hacktool.Linux.Prochider.A(B)	Malang
61	Trojan.Exploit.Linux.Small.F(B)	Malang
62	Gen:Trojan.Heur.GZ.OGZ@buhJ80ni(B)	Malang
63	Trojan.Generic.8834573(B)	Malang
64	Application.Win32.WebApp(A)	Malang
65	Application.InstallExpress(A)	Malang
66	Application.WebSearch(A)	Malang
67	Application.AppInstall(A)	Malang
68	Application.AppInstall(A)	Malang
69	Application.AdGenie(A)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
70	Application.AdGenie(A)	Malang
71	Application.AdGenie(A)	Malang
72	Application.AdGenie(A)	Malang
73	Application.AdGenie(A)	Malang
74	Application.AdReg(A)	Malang
75	Application.AdGenie(A)	Malang
76	Application.AdReg(A)	Malang
77	Application.AdGenie(A)	Malang
78	Application.AdGenie(A)	Malang
79	Application.AdGenie(A)	Malang
80	Application.AdStart(A)	Malang
81	Application.AppInstall(A)	Malang
82	Application.AppInstall(A)	Malang
83	Application.AppInstall(A)	Malang
84	Application.AppInstall(A)	Malang
85	Application.AppInstall(A)	Malang
86	Application.AppInstall(A)	Malang
87	Application.AppInstall(A)	Malang
88	Application.AppInstall(A)	Malang
89	Application.AppInstall(A)	Malang
90	Application.SearchPlug(A)	Malang
91	Application.SearchPlug(A)	Malang
92	Application.SearchPlug(A)	Malang
93	Application.AdReg(A)	Malang
94	Application.AdReg(A)	Malang
95	Application.AdReg(A)	Malang
96	Application.AdReg(A)	Malang
97	Application.AdReg(A)	Malang
98	Application.AdReg(A)	Malang
99	Application.AdReg(A)	Malang
100	Application.AdReg(A)	Malang
101	Application.AdReg(A)	Malang
102	Application.AdReg(A)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
103	Application.AdReg(A)	Malang
104	Application.AdReg(A)	Malang
105	Application.AdReg(A)	Malang
106	Application.AdReg(A)	Malang
107	Application.AdReg(A)	Malang
108	Application.AdReg(A)	Malang
109	Application.AdReg(A)	Malang
110	Application.AdReg(A)	Malang
111	Application.AdReg(A)	Malang
112	Application.AdReg(A)	Malang
113	Application.AdServ(A)	Malang
114	Application.BHO(A)	Malang
115	Application.InstallAd(A)	Malang
116	Application.InstallAd(A)	Malang
117	Application.InstallAd(A)	Malang
118	Application.InstallAd(A)	Malang
119	Application.InstallAd(A)	Malang
120	Application.InstallAd(A)	Malang
121	Application.InstallAd(A)	Malang
122	Application.InstallTool(A)	Malang
123	Application.InstallTool(A)	Malang
124	Application.WebExt(A)	Malang
125	Application.WebExt(A)	Malang
126	Application.WebExt(A)	Malang
127	Application.WebExt(A)	Malang
128	Application.AdTool(A)	Malang
129	Application.AdTool(A)	Malang
130	Trojan.Win32.Agent(A)	Malang
131	Application.AppInstall(A)	Malang
132	Application.InstallAd(A)	Malang
133	Application.InstallAd(A)	Malang
134	Application.InstallAd(A)	Malang
135	Application.InstallAd(A)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
136	Application.InstallAd(A)	Malang
137	Application.InstallAd(A)	Malang
138	Application.InstallAd(A)	Malang
139	Application.InstallAd(A)	Malang
140	Application.InstallAd(A)	Malang
141	Application.InstallAd(A)	Malang
142	Application.InstallAd(A)	Malang
143	Application.InstallAd(A)	Malang
144	Application.InstallDeal(A)	Malang
145	Application.InstallTool(A)	Malang
146	Application.InstallTool(A)	Malang
147	Application.InstallTool(A)	Malang
148	Application.Win32.WSearch(A)	Malang
149	Application.Win32.WSearch(A)	Malang
150	Application.Win32.WSearch(A)	Malang
151	Application.Win32.WSearch(A)	Malang
152	Application.Win32.WSearch(A)	Malang
153	Application.AdReg(A)	Malang
154	Application.AdReg(A)	Malang
155	Application.AdReg(A)	Malang
156	Application.AdReg(A)	Malang
157	Application.AdReg(A)	Malang
158	Application.Win32.InstallExt(A)	Malang
159	Application.Win32.InstallExt(A)	Malang
160	Application.Win32.InstallExt(A)	Malang
161	Application.Win32.InstallExt(A)	Malang
162	Application.Win32.InstallExt(A)	Malang
163	Application.Win32.InstallExt(A)	Malang
164	Application.Win32.WebToolbar(A)	Malang
165	Adware.Win32.Agent(A)	Malang
166	Application.Win32.InstallTool(A)	Malang
167	Gen:Application.Bundler.DefaultTab.1(B)	Malang
168	Worm.VBS.AO(B)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
169	Application.Bundler.Somoto.I(B)	Malang
170	Worm.VBS.AO(B)	Malang
171	Gen:Variant.Zusy.76367(B)	Malang
172	Application.Bundler.Somoto.I(B)	Malang
173	Trojan.LNK.Gen(B)	Malang
174	Trojan.LNK.Gen(B)	Malang
175	Application.Bundler.Somoto.I(B)	Malang
176	Gen:Variant.Application.Bundler.DomaIQ.3(B)	Malang
177	Worm.VBS.AO(B)	Malang
178	Win32.Ramnit.L(B)	Malang
179	Gen:Application.Bundler.DefaultTab.1(B)	Malang
180	Application.Bundler.Somoto.I(B)	Malang
181	Worm.VBS.AO(B)	Malang
182	Worm.VBS.AO(B)	Malang
183	Gen:Application.Bundler.DefaultTab.1(B)	Malang
184	Application.Bundler.Somoto.I(B)	Malang
185	Trojan.AutorunINF.Gen(B)	Malang
186	Application.Bundler.Somoto.I(B)	Malang
187	Trojan.Generic.5145126(B)	Malang
188	Worm.VBS.AO(B)	Malang
189	Trojan.Generic.10494008(B)	Malang
190	Application.BitCoinMiner.EG(B)	Malang
191	Dropped:Trojan.GenericKD.1583276(B)	Malang
192	Trojan.LNK.Gen(B)	Malang
193	Dropped:Trojan.AgentWDCR.BM(B)	Malang
194	Trojan.Generic.5145126(B)	Malang
195	Worm.VBS.AO(B)	Malang
196	Win32.Madangel.I(B)	Malang
197	Application.Bundler.Somoto.C(B)	Malang
198	Trojan.Generic.11106456(B)	Malang
199	Gen:Variant.Kazy.339345(B)	Malang
200	Trojan.AgentWDCR.BM(B)	Malang
201	Worm.VBS.AO(B)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
202	Application.Bundler.Somoto.C(B)	Malang
203	Worm.VBS.AO(B)	Malang
204	Application.BitCoinMiner.BK(B)	Malang
205	Application.Bundler.Somoto.I(B)	Malang
206	Gen:Variant.Kazy.197178(B)	Malang
207	Trojan.GenericKD.1582891(B)	Malang
208	Gen:Variant.Application.Bundler.DomaIQ.3(B)	Malang
209	Application.Bundler.Somoto.I(B)	Malang
210	Worm.VBS.AO(B)	Malang
211	Gen:Variant.Kazy.325894(B)	Malang
212	Win32.Ramnit.L(B)	Malang
213	Worm.VBS.AO(B)	Malang
214	Application.Bundler.Somoto.C(B)	Malang
215	Trojan.GenericKD.1474810(B)	Malang
216	Application.Bundler.Somoto.I(B)	Malang
217	Win32.Ramnit.L(B)	Malang
218	Application.Bundler.InstallBrain.A(B)	Malang
219	Application.Bundler.Somoto.I(B)	Malang
220	Trojan.Generic.10229435(B)	Malang
221	Application.Bundler.Somoto.C(B)	Malang
222	Worm.VBS.AO(B)	Malang
223	Worm.VBS.AO(B)	Malang
224	Application.Bundler.Somoto.I(B)	Malang
225	Worm.VBS.AO(B)	Malang
226	Gen:Trojan.Heur.AutoIT.6(B)	Malang
227	Trojan.Generic.5145126(B)	Malang
228	Application.Bundler.Somoto.I(B)	Malang
229	Worm.VBS.AO(B)	Malang
230	Trojan.LNK.Gen(B)	Malang
231	Application.Bundler.Somoto.I(B)	Malang
232	Trojan.LNK.Gen(B)	Malang
233	Worm.VBS.AO(B)	Malang
234	Gen:Variant.Graftor.126775(B)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
235	Adware.NewNextMe.A(B)	Malang
236	Application.Malware.NOV(B)	Malang
237	Worm.VBS.AO(B)	Malang
238	Gen:Variant.Graftor.119203(B)	Malang
239	Gen:Variant.Symmi.37373(B)	Malang
240	Worm.VBS.AO(B)	Malang
241	Application.Bundler.Somoto.I(B)	Malang
242	Worm.VBS.AO(B)	Malang
243	Win32.Worm.Downadup.Gen(B)	Malang
244	Application.Bundler.Somoto.I(B)	Malang
245	Trojan.Generic.8834573(B)	Malang
246	Gen:Adware.MPlug.1(B)	Malang
247	Application.Win32.InstallAd(A)	Malang
248	Application.Win32.InstallTool(A)	Malang
249	Adware.Win32.Agent(A)	Malang
250	Adware.NewNextMe.A(B)	Malang
251	Application.Bundler.Somoto.I(B)	Malang
252	Application.Bundler.Somoto.I(B)	Malang
253	Application.Bundler.Somoto.I(B)	Malang
254	Application.InstallAd(A)	Malang
255	Application.Bundler.Somoto.I(B)	Malang
256	Application.Bundler.Somoto.I(B)	Malang
257	Application.Bundler.Somoto.I(B)	Malang
258	Application.Bundler.Somoto.J(B)	Malang
259	Application.Bundler.Somoto.I(B)	Malang
260	Application.InstallAd(A)	Malang
261	Application.InstallAd(A)	Malang
262	Application.Bundler.Somoto.I(B)	Malang
263	Application.InstallAd(A)	Malang
264	Application.Bundler.Somoto.I(B)	Malang
265	Application.Bundler.Somoto.I(B)	Malang
266	Application.InstallAd(A)	Malang
267	Application.Bundler.Somoto.I(B)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
268	Application.InstallAd(A)	Malang
269	Application.Bundler.Somoto.I(B)	Malang
270	Application.InstallAd(A)	Malang
271	Application.InstallAd(A)	Malang
272	Application.Bundler.Somoto.J(B)	Malang
273	Application.Bundler.Somoto.J(B)	Malang
274	Application.InstallAd(A)	Malang
275	Application.Bundler.Somoto.I(B)	Malang
276	Application.Bundler.Somoto.I(B)	Malang
277	Application.Bundler.Somoto.J(B)	Malang
278	Application.Bundler.Somoto.I(B)	Malang
279	Application.Bundler.Somoto.J(B)	Malang
280	Application.Bundler.Somoto.I(B)	Malang
281	Application.InstallAd(A)	Malang
282	Application.Bundler.Somoto.I(B)	Malang
283	Application.InstallAd(A)	Malang
284	Application.Bundler.Somoto.I(B)	Malang
285	Application.InstallAd(A)	Malang
286	Application.Bundler.Somoto.I(B)	Malang
287	Application.InstallAd(A)	Malang
288	Application.InstallAd(A)	Malang
289	Application.Bundler.Somoto.I(B)	Malang
290	Application.InstallAd(A)	Malang
291	Application.Bundler.Somoto.I(B)	Malang
292	Application.InstallAd(A)	Malang
293	Application.InstallAd(A)	Malang
294	Application.InstallAd(A)	Malang
295	Application.InstallAd(A)	Malang
296	Application.InstallAd(A)	Malang
297	Application.Bundler.Somoto.I(B)	Malang
298	Application.InstallAd(A)	Malang
299	Application.InstallAd(A)	Malang
300	Application.Bundler.Somoto.I(B)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
301	Application.Bundler.Somoto.J(B)	Malang
302	Application.InstallAd(A)	Malang
303	Application.Bundler.Somoto.I(B)	Malang
304	Application.Bundler.Somoto.I(B)	Malang
305	Application.Bundler.Somoto.J(B)	Malang
306	Application.InstallAd(A)	Malang
307	Application.Bundler.Somoto.I(B)	Malang
308	Application.InstallAd(A)	Malang
309	Application.Bundler.Somoto.I(B)	Malang
310	Application.Bundler.Somoto.I(B)	Malang
311	Application.Bundler.Somoto.I(B)	Malang
312	Application.Bundler.Somoto.I(B)	Malang
313	Application.InstallAd(A)	Malang
314	Application.InstallAd(A)	Malang
315	Application.InstallAd(A)	Malang
316	Application.InstallAd(A)	Malang
317	Application.InstallAd(A)	Malang
318	Application.InstallAd(A)	Malang
319	Application.Bundler.Somoto.J(B)	Malang
320	Application.Bundler.Somoto.J(B)	Malang
321	Application.InstallAd(A)	Malang
322	Gen:Variant.Kazy.339345(B)	Malang
323	Trojan.Generic.11106456(B)	Malang
324	Trojan.Generic.11398511(B)	Malang
325	Riskware.Win32.CrackTool(A)	Malang
326	Application.Keygen.ET(B)	Malang
327	Application.Keygen.ET(B)	Malang
328	Trojan.Generic.1938807(B)	Malang
329	Riskware.Win32.HackTool.Patcher(A)	Malang
330	Application.InstallAd(A)	Malang
331	Application.Bundler.Somoto.I(B)	Malang
332	Application.Win32.InstallAd(A)	Malang
333	Application.Win32.InstallAd(A)	Malang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
334	DeepScan:Generic.Zlob.B80B8DE5(B)	Magelang
335	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
336	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
337	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
338	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
339	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
340	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
341	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
342	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
343	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
344	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
345	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
346	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
347	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
348	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
349	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
350	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
351	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
352	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
353	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
354	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
355	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
356	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
357	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
358	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
359	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
360	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
361	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
362	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
363	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
364	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
365	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
366	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang

Tabel 3.3: Tabel Malware

No	Nama Malware	Kota Asal
367	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
368	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
369	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
370	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
371	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
372	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
373	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
374	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
375	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
376	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
377	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
378	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
379	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
380	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
381	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
382	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
383	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
384	Trace.Registry.AdvancedArchivePasswordRecovery4.1(A)	Magelang
385	Trace.File.BaiduBar(A)	Padang
386	Trace.File.SuperPopandDrop(A)	Padang
387	Trace.File.GameFiesta5CardSlingoDeluxe(A)	Padang
388	Trace.Registry.BaiduBar(A)	Padang
389	Trace.Registry.BaiduBar(A)	Padang
390	Trace.Registry.BaiduBar(A)	Padang

Sampai akhir bulan Maret, total jumlah malware yang terdeteksi adalah 390 malware. Kota Malang menjadi kota yang paling banyak melaporkan malware yaitu sebanyak 276 malware. Selanjutnya diikuti oleh Magelang yang melaporkan 51 malware. Klasifikasi malware yang telah dilaporkan dapat dilihat pada tabel 3.4 berikut:

Tabel 3.4: Klasifikasi Malware

No	Daftar Malware	Jenis	Jumlah

Tabel 3.4: Klasifikasi Malware

No	Daftar Malware	Jenis	Jumlah
1	Adware.NewNextMe.A(B)	Adware	2
2	Adware.Win32.Agent(A)	Adware	2
3	Application.AdGenie(A)	Adware	9
4	Application.AdReg(A)	Adware	27
5	Application.AdServ(A)	Adware	1
6	Application.AdStart(A)	Adware	1
7	Application.AdTool(A)	Adware	2
8	Application.AppInstall(A)	Rootkit	12
9	Application.BHO(A)	Trojan	1
10	Application.BitCoinMiner.BK(B)	Trojan	1
11	Application.BitCoinMiner.EG(B)	Trojan	1
12	Application.Bundler.InstallBrain.A(B)	Adware	1
13	Application.Bundler.Somoto.C(B)	Adware	4
14	Application.Bundler.Somoto.I(B)	Adware	46
15	Application.Bundler.Somoto.J(B)	Adware	9
16	Application.InstallAd(A)	Adware	52
17	Application.InstallDeal(A)	Adware	1
18	Application.InstallExpress(A)	Adware	1
19	Application.InstallTool(A)	Adware	5
20	Application.Keygen.ET(B)	Keygen	2
21	Application.Malware.NOV(B)	Trojan	1
22	Application.SearchPlug(A)	Trojan	3
23	Application.WebExt(A)	Adware	4
24	Application.WebSearch(A)	Browser hijacker	1
25	Application.Win32.InstallAd(A)	Adware	3
26	Application.Win32.InstallExt(A)	Adware	6
27	Application.Win32.InstallTool(A)	Adware	2
28	Application.Win32.WebApp(A)	Adware	1
29	Application.Win32.WebToolbar(A)	Adware	1
30	Application.Win32.WSearch(A)	Adware	5
31	Backdoor.Perl.IRCBot.AM(B)	Backdoor	1
32	DeepScan:Generic.Zlob.B80B8DE5(B)	Trojan	1
33	Dropped:Trojan.AgentWDCR.BM(B)	Trojan	1

Tabel 3.4: Klasifikasi Malware

No	Daftar Malware	Jenis	Jumlah
34	Dropped:Trojan.GenericKD.1583276(B)	Trojan	1
35	EICAR-ANTIVIRUS-TESTFILE!E2	Virus test	1
36	EICAR-ANTIVIRUS-TESTFILE!E5	Virus test	1
37	EICAR-ANTIVIRUS-TESTFILE!E8	Virus Test	1
38	EICAR-ANTIVIRUS-TESTFILE!E9	Virus test	1
39	Gen:Adware.MPlug.1(B)	Adware	1
40	Gen:Application.Bundler.DefaultTab.1(B)	Trojan	3
41	Gen:Trojan.Heur.AutoIT.6(B)	Trojan	1
42	Gen:Trojan.Heur.GM.000C040880(B)	Trojan	1
43	Gen:Trojan.Heur.GZ.OGZ@buhJ80ni(B)	Trojan	1
44	Gen:Trojan.Heur.smGfrbXY@VoiC(B)	Trojan	6
45	Gen:Variant.Application.Bundler.DomaIQ.3(B)	Adware	2
46	Gen:Variant.Application.MediaFinder.1(B)	Adware	15
47	Gen:Variant.Graftor.119203(B)	Trojan	1
48	Gen:Variant.Graftor.126775(B)	Trojan	1
49	Gen:Variant.Kazy.197178(B)	Trojan	1
50	Gen:Variant.Kazy.325894(B)	Trojan	1
51	Gen:Variant.Kazy.339345(B)	Trojan	2
52	Gen:Variant.Symmi.37373(B)	Trojan	1
53	Gen:Variant.Zusy.76367(B)	Trojan	1
54	Generic.Malware.SPDVTk.2C83EFBE(B)	Trojan	6
55	MemScan:Trojan.Generic.3268307(B)	Trojan	3
56	Riskware.Win32.CrackTool(A)	Trojan	1
57	Riskware.Win32.HackTool.Patcher(A)	Trojan	1
58	Trace.File.Bejeweled2Deluxe1.0(A)	Trojan	2
59	Trace.File.FeedingFrenzy2(A)	Trojan	2
60	Trace.File.BaiduBar(A)	Spyware	1
61	Trace.File.SuperPopandDrop(A)	Trojan	1
62	Trace.File.GameFiesta5CardSlingoDeluxe(A)	Trojan	1
63	Trace.AdvancedArchivePasswordRecovery4.1(A)	Trojan	50
64	Trace.Registry.BaiduBar(A)	Trojan	2
65	Trace.Registry.FeedingFrenzy2(A)	Trojan	2
66	Trace.Registry.PCTuneUp(A)	Trojan	2

Tabel 3.4: Klasifikasi Malware

No	Daftar Malware	Jenis	Jumlah
67	Trojan.AgentWDCR.BM(B)	Trojan	1
68	Trojan.AutorunINF.Gen(B)	Trojan	1
69	Trojan.Exploit.Linux.Small.F(B)	Trojan	1
70	Trojan.Generic.10229435(B)	Trojan	1
71	Trojan.Generic.10494008(B)	Trojan	1
72	Trojan.Generic.11106456(B)	Trojan	2
73	Trojan.Generic.11398511(B)	Trojan	1
74	Trojan.Generic.1938807(B)	Trojan	1
75	Trojan.Generic.5145126(B)	Trojan	3
76	Trojan.Generic.6265065(B)	Trojan	3
77	Trojan.Generic.7320471(B)	Trojan	6
78	Trojan.Generic.7890946(B)	Trojan	3
79	Trojan.Generic.8834573(B)	Trojan	2
80	Trojan.GenericKD.1474810(B)	Trojan	1
81	Trojan.GenericKD.1582891(B)	Trojan	1
82	Trojan.Hacktool.Linux.Prochider.A(B)	Trojan	1
83	Trojan.LNK.Gen(B)	Trojan	5
84	Trojan.Win32.Agent(A)	Trojan	1
85	Win32.Madangel.I(B)	Virus	1
86	Win32.Ramnit.L(B)	Virus	3
87	Win32.Worm.Downadup.Gen(B)	Worm	1
88	Worm.VBS.AO(B)	Worm	19

Dari tabel diatas, terlihat trend malware yang terbanyak adalah jenis Adware. Pada penelitian ini ditemukan 203 adware. 52% malware yang dilaporkan adalah Adware. Jenis malware yang banyak ditemukan juga adalah Trojan. Pada penelitian ini ditemukan 138 jenis Trojan. 35% malware yang dilaporkan adalah Trojan. Selain itu ditemukan juga Virus, Worm, Keylogger, Spyware dan backdoor. Varian malware yang paling banyak ditemukan adalah Aplication.InstallAd(A). Malware ini dilaporkan sebanyak 52 kali pada penelitian ini. Malware ini merupakan sebuah tipe Adware. Malware ini tidak terlalu berbahaya, biasanya menginfeksi komputer melalui aplikasi download wrapper. Aplikasi download wrapper ini biasanya didapatkan ketika kita ingin mengunduh file dari sebuah web, kemudian web tersebut meminta kita mengin-

stall sebuah aplikasi Download Manager. Malware ini bekerja dengan memasang iklan pada komputer kita. Selain itu malware ini meninggalkan jejak pada registry komputer.

Malware berikutnya yang banyak ditemukan adalah Trace.AdvancedArchivePassword Recovery4.1(A) sebanyak 50 kali dan Application.Bundler.Somoto.I(B) sebanyak 46 kali. Trace.Advanced Archive PasswordRecovery4.1(A) adalah sebuah Trojan. Biasanya malware ini ditemukan pada aplikasi password recovery untuk membuka file rar dan zip yang dipassword. Sementara malware Application. Bundler. Somoto.I(B) merupakan sebuah Adware. Adware ini memasang iklan, popup dan toolbar pada browser kita. Biasanya malware ini menginfeksi dengan menyisipkan dirinya ketika kita mengunduh aplikasi dari sebuah layanan web.Sebaran malware yang dilaporkan dapat dilihat pada tabel 3.5 berikut:

Tabel 3.5 Sebaran Malware

No	Jenis Malware	Jumlah	Persentasi
1	Adware	203	52%
2	Trojan	138	35%
3	Worm	20	5%
4	Rootkit	12	3%
5	Virus	8	2%
6	Keygen	2	0,5%
7	Spyware	1	0,25%
8	Backdoor	1	0,25%
9	Browser Hijacker	1	0,25%

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://www.cert.or.id/bahan-bacaan/id/konten/24/ atau dari tautan http://www.cert.or.id/media/files/ AplikasiMalware_Scanner_1.zip 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/.....).
9. Scanning dilakukan hanya pada komputer dengan OS Windows. Bila ada pertanyaan hubungi email support@malware.cert.or.id atau ahmad@cert.or.id.

Petunjuk tentang kegiatan ini dapat dilihat pada halaman http://www.cert.or.id/index-berita/id/berita/49/

Bab 4

Evaluasi

Pada bab ini kami laporkan hasil evaluasi tim terhadap jalannya survey malware sampai akhir bulan Mei 2015.

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 akhir bulan Mei 2015, relawan yang mengikuti kegiatan ini hanya berjumlah 51 orang dari 27 kota dan 12 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/press101613.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/.

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/.