

**ANALISIS SERANGAN WORMS KOMPUTER,
TINJAUAN KASUS : EMAIL-WORM.Win32.Brontok.c**

**Laporan Tugas Akhir
Mata Kuliah EC7010
Keamanan Sistem Lanjut**

Oleh

RIZA KURNIAWAN

NIM : 23205338

Program Studi Teknik Elektro



**INSTITUT TEKNOLOGI BANDUNG
2006**

ABSTRAK

Analisis Serangan Worms Komputer, Tinjauan Kasus : Worms Lokal Email-Worms.Win32.Brontok.c

Memahami dan memprediksi ancaman terhadap keamanan sistem informasi, merupakan salah satu kunci sukses dalam memproteksi sistem tersebut di masa depan. Salah satu ancaman yang cukup serius bagi pengguna komputer baik pada tingkat *end user* ataupun pengelola sistem informasi (*administrator*) adalah penyebaran virus komputer. Evolusi virus komputer yang dimulai ketika Fred Cohen pada tahun 1984 mempublikasikan teori tentang “*self replicating program*”^[1], hingga saat ini telah mencapai perkembangan yang menakjubkan seiring dengan peningkatan teknik pemrograman dan cakupan lingkungan penyebarannya. Sehingga pencegahan dan penanggulangan dari dampak negatif virus komputer tersebut mutlak perlu ditingkatkan.

Secara umum bagi pengguna komputer, perlindungan terhadap ancaman virus komputer dianggap telah memadai dengan dipergunakannya *software anti virus*. Namun virus komputer seperti halnya *trojan horse*, *worms*, *spyware* dan sebagainya, yang juga dikategorikan sebagai program yang berbahaya (*malicious software*), memiliki beberapa karakteristik yang berbeda-beda sesuai dengan teknik pemrograman dan tujuan dari si pembuat virus. Sehingga proteksi sistem dengan hanya mengandalkan kemampuan *software anti virus* saja, belum dapat dianggap mencukupi. Untuk itu, masih sangat diperlukan langkah-langkah perlindungan yang menyeluruh, yang didasarkan atas informasi mengenai karakteristik dan dampak negatif dari penyebaran virus komputer tersebut.

Tulisan ini akan mencoba membahas secara ringkas, bagaimana melakukan analisis penanganan sistem terhadap ancaman *worms* komputer. Secara umum akan diuraikan langkah-langkah penanganan yang meliputi tindakan pencegahan, tindakan pada saat sistem telah terjangkit, serta tindakan proteksi sistem agar *worms* komputer tersebut tidak menyebar luas. Untuk melengkapi analisis, disertakan pula tinjauan kasus dari sebuah *worms* lokal Email-Worms.Win32.Brontok.c. Diharapkan dengan melakukan analisis dan metodologi ini, perlindungan sistem akan ancaman dari dampak negatif *worms* komputer dapat lebih ditingkatkan.

Kata kunci : *self replicating program*, *trojan horse*, *worms*, *spyware*, *malicious software*, analisis.

DAFTAR ISI

	Halaman
ABSTRAK	i
DAFTAR ISI	ii
DAFTAR TABEL	iii
DAFTAR GAMBAR	iv
BAB I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	2
1.3 Ruang lingkup	3
1.4 Metodologi.....	3
BAB II. TINJAUAN SINGKAT WORMS.....	4
2.1 Malware.....	5
2.2. Perbedaan virus dan worms	6
2.3 Sejarah dan taksonomi worms	9
2.4 Struktur worms	10
2.5 Tipe-tipe worms	11
2.6 Pola lalu lintas penyebaran worms	11
BAB III. ANALISIS WORMS Email-Worm.Win32.Brontok.c	13
3.1 Tinjauan umum	13
3.2 Alat dan bahan	15
3.3 Proses analisis	15
3.4 Hasil analisis	18
BAB III. CARA PENANGGULANGAN WORMS Email- Worm.Win32.Brontok.c	23
DAFTAR PUSTAKA	

DAFTAR TABEL

	Halaman
Tabel 3.1 Tabel Perangkat lunak analisis	15

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Klasifikasi malware	4
Gambar 2.2 Cara penyebaran virus surat masal ^[3]	6
Gambar 2.3 Cara penyebaran <i>worms</i> ^[3]	6
Gambar 2.4 Kronologis <i>worms</i> ^[2]	7
Gambar 2.5 Gambaran proses umum komponen <i>worms</i> ^[2]	10
Gambar 2.6 Gambar 2.6 Contoh grafik prediksi pertumbuhan <i>worms</i> ^[2]	12
Gambar 3.1 Tampilan PE-ID saat mengidentifikasi file terinfeksi	16
Gambar 3.2 Tampilan IDA-Pro saat mengidentifikasi file terinfeksi	16
Gambar 3.3 Tampilan IDA Pro sebelum melakukan <i>debugging</i>	17
Gambar 3.4 Tampilan Aplikasi Msconfig terinfeksi	19
Gambar 3.5 Tampilan Aplikasi Regedit terinfeksi pada <i>Command prompt</i>	20
Gambar 3.6 Tampilan Windows Explorer terinfeksi	20

BAB I

PENDAHULUAN

1.1 Latar belakang

Selama lebih dari tiga dekade yang lalu, virus komputer telah berkembang dari sekedar riset akademis menjadi masalah yang umum bagi para pengguna komputer di dunia. Masalah terbesar dari virus ini berasal dari penanggulangan efek kerugian yang ditimbulkan oleh penyebarannya. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia. Berdasarkan hasil survei CSI/FBI^[4] sejak tahun 1999-2006 pada sekitar 300-an responden dari berbagai organisasi di Amerika Serikat, tentang kejahatan komputer dan keamanannya, menyebutkan bahwa virus menempati urutan pertama sebagai kejahatan komputer yang paling merugikan. Masih dari hasil survey tersebut, dinyatakan kerugian rata-rata yang diderita organisasi-organisasi itu akibat virus komputer ditaksir mencapai sekitar 38 juta dolar amerika per tahun.

Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya. Salah satu bentuk evolusi tersebut dikenal dengan *Worms* komputer. *Worms* yang mula-mula diciptakan oleh Robert T. Morris tahun 1984^[1] ini, dikategorikan sebagai program yang berbahaya (*malicious software/malware*) yang mirip dengan virus dan menyebar melalui jaringan komputer. Keunggulan worms ini jika dibandingkan dengan virus adalah kecepatannya yang tinggi dalam menginfeksi komputer dalam jaringan (*internet*). Sebagai contoh, *Worms* Code Red II mampu menyebar pada 360.000 *host* pada 2000 sistem komputer dalam satu hari^[2].

Perkembangan penyebaran *worms* di Indonesia, pada awalnya lebih banyak didominasi oleh *worms* yang berasal dari luar negeri. Namun pada bulan Oktober 2005, dominasi ini mulai runtuh dengan menyebarnya *worms* Rontokbro (Email-Worm.Win32.Brontok.a^[7]). Menurut Vaksin.com, worms tersebut selama bulan November 2005 sampai dengan Agustus 2005, menempati urutan pertama sebagai

worms yang paling banyak menyebar di Indonesia^[7]. Tidak hanya itu, Rontokbro tersebut juga telah menyebar pada beberapa negara seperti Amerika, Polandia, Spanyol, Jepang, Vietnam, Belanda, Hungaria, Swedia, Peru, Rusia dan Israel^[7]. Selain itu Aksi worms ini juga telah melumpuhkan situs www.kaskus.com dan menyerang situs 17tahun.com, <http://israel.gov.il> dan sebuah situs pribadi www.fajarweb.com^[4]. Karena dampak dan eksistensinya, maka worms ini dan beberapa variannya juga masuk dalam daftar *PC Viruses In-the-Wild* dari bulan November 2005 sampai Agustus 2006^[x].

Tulisan ini akan membahas, bagaimana melakukan analisis dari teknis penanganan sistem terhadap ancaman worms komputer. Untuk melengkapi analisis, disertakan pula tinjauan kasus dari sebuah worms lokal Email-Worm.Win32.Brontok.c. Diharapkan dengan melakukan analisis ini, perlindungan sistem akan ancaman dari dampak negatif worms komputer dapat lebih ditingkatkan.

1.2 Tujuan

Tujuan dalam pembuatan tulisan ini adalah,

1. Sebagai suatu referensi dalam meningkatkan keamanan sistem informasi.
2. Sebagai referensi dalam mencegah dan menanggulangi serangan worms komputer.

1.3 Ruang Lingkup

Tulisan ini hanya akan membahas,

1. Hal-hal umum seputar terminologi *malware* dan kategorinya;
2. Tinjauan singkat tentang *worms* yang meliputi, sejarah dan taksonomi, struktur, metode penyebaran, metode penanganannya;
3. Analisis singkat *worms* Email-Worm.Win32.Brontok.c yang meliputi, tinjauan umum, alat dan bahan, struktur, strategi penyerangan, serta metode penanganannya.

1.4 Metodologi

Metode yang digunakan pada tulisan ini adalah,

1. studi literatur dari berbagai sumber di internet;
2. analisis teknis worms Email-Worm.Win32.Brontok.c yaitu,
 - mencari *file* sampel yang terinfeksi worms tersebut,
 - mengidentifikasi perilaku worms (*black box analysis* dan *debugging file* sampel),
 - melakukan rekayasa ulang (*reverse engineering*) *file* sampel dan
 - mendokumentasi hasil analisis.

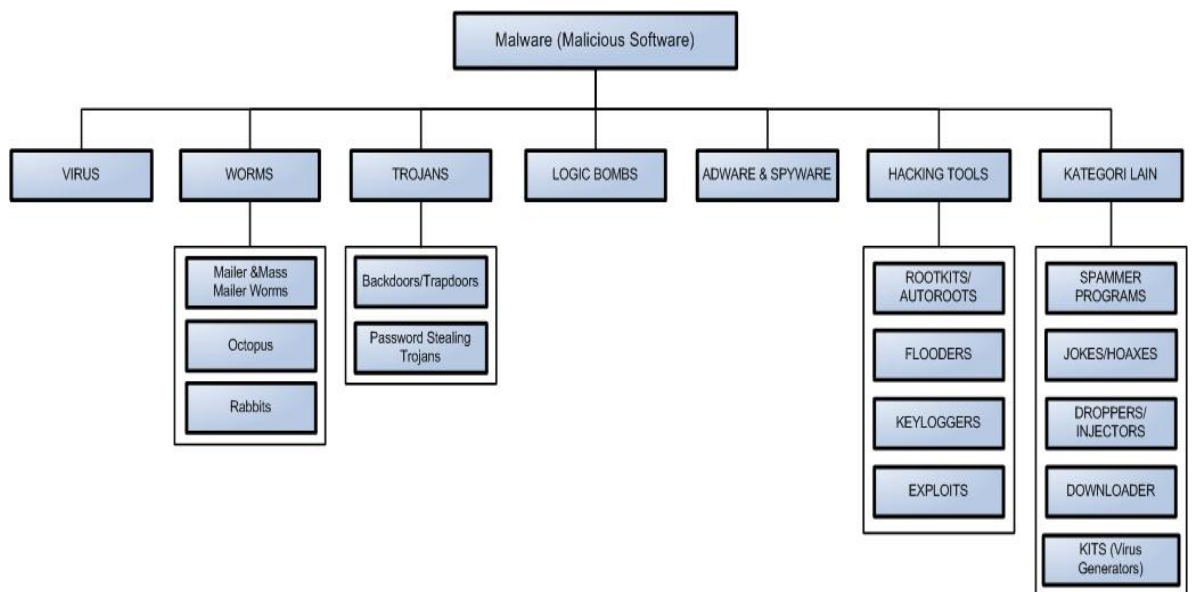
BAB II

TINJAUAN SINGKAT *WORMS*

2.1 Malware

Perkembangan teknologi komputer yang pesat, ternyata tidak hanya membawa manfaat yang besar bagi penggunaannya tetapi juga menimbulkan dampak negatif dengan dibuatnya kode program yang berbahaya. Program-program berbahaya itu sering disebut juga dengan *Malicious Code/Malicious Software (malware)*. Pada dasarnya *malware* didefinisikan dengan *sebuah perangkat lunak yang didesain untuk melakukan infiltrasi atau merusak suatu sistem komputer, tanpa seijin pemiliknya*^[2].

Beberapa usaha untuk membuat pengklasifikasian malware secara tepat tidak mudah dilakukan, tumpang tindih antara spesifikasi teknis tiap kelas dan *sub* kelasnya selalu ditemukan pada klasifikasi tersebut. Namun secara umum, menurut Peter Szor^[1] *malware* dapat diklasifikasikan seperti gambar berikut ini,



Gambar 2.1 Klasifikasi *Malware*

2.2 Perbedaan Virus dan Worms

Dari klasifikasi di atas, karena memiliki aksi yang hampir serupa, terdapat dua tipe *malware* yang agak sulit dibedakan yaitu, virus dan *worms*. Untuk mempermudah melihat perbedaan kedua *malware* tersebut dapat ditinjau dari

a. Definisi

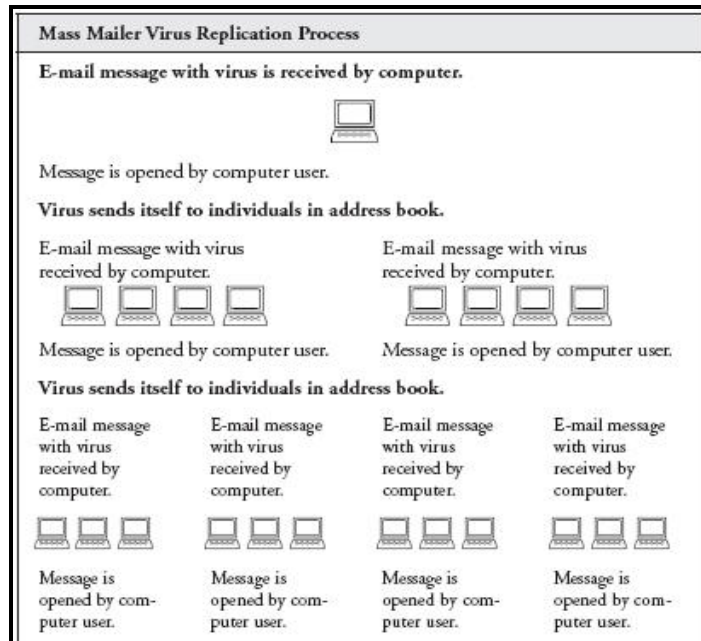
- pada awalnya virus didefinisikan oleh Frederick B. Cohen sebagai *suatu program yang dapat menginfeksi program lain dengan memodifikasinya, termasuk kemungkinan untuk berevolusi dengan menggandakan dirinya sendiri*^[1]. Seiring dengan perkembangan teknik pemrogramannya, terdapat beberapa bentuk virus yang tidak sesuai dengan definisi tersebut. Sebagai contoh, suatu virus yang sering disebut *companion virus* memiliki kemampuan menggandakan diri tanpa mengubah program yang diinfeksinya. Sehingga menurut Peter Szor, definisi yang lebih akurat untuk virus pada saat ini adalah, *suatu program yang secara berulang (recursively) dan dengan tegas (explicitly) menggandakan suatu versi dirinya sebagai kemungkinan untuk berevolusi*^[1].
- Sedangkan definisi formal untuk *worms* menurut Robert T. Morris adalah *suatu program yang berpindah dari satu komputer ke komputer yang lain tanpa mengikatkan dirinya (attach itself) pada sistem operasi komputer yang diinfeksinya*^[2]. Sejalan dengan perkembangannya, definisi *worms* tersebut sudah tidak begitu tepat. Beberapa *worms* sering menggunakan teknik untuk menyembunyikan kehadirannya dengan melakukan instalasi atau memodifikasi sistem. Sehingga definisi yang lebih tepat menurut Jose Nazario adalah *suatu agen penginfeksi yang otonom dan independen dalam bereplikasi, serta memiliki kemampuan dalam menginfeksi sistem host baru melalui fasilitas jaringan*^[2].

b. Cara penyebaran

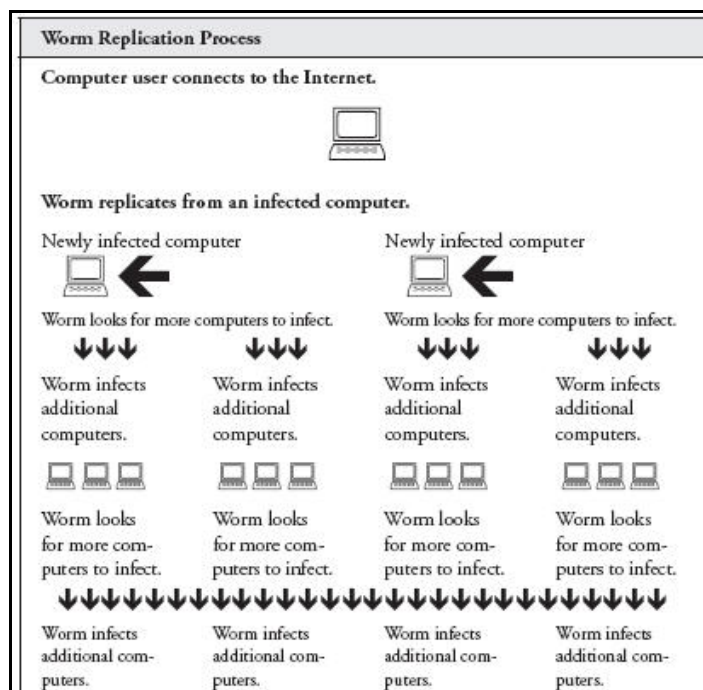
- Virus memerlukan campur tangan pengguna dalam penyebarannya, misalnya dalam proses *download*, klik ganda pada *file* yang terinfeksi, dan lain-lain.
- Sedangkan *worms* dapat secara otomatis menyebar dengan tanpa atau sedikit campur tangan dari penggunannya. Misalnya dengan satu kali klik pada file

lampiran e-mail yang terinfeksi *worms*, maka satu atau beberapa sistem yang terkoneksi melalui e-mail tersebut akan segera terinfeksi.

Untuk lebih jelas, dapat dilihat dari dua contoh gambar berikut,



Gambar 2.2 Cara penyebaran virus surat masal^[3]

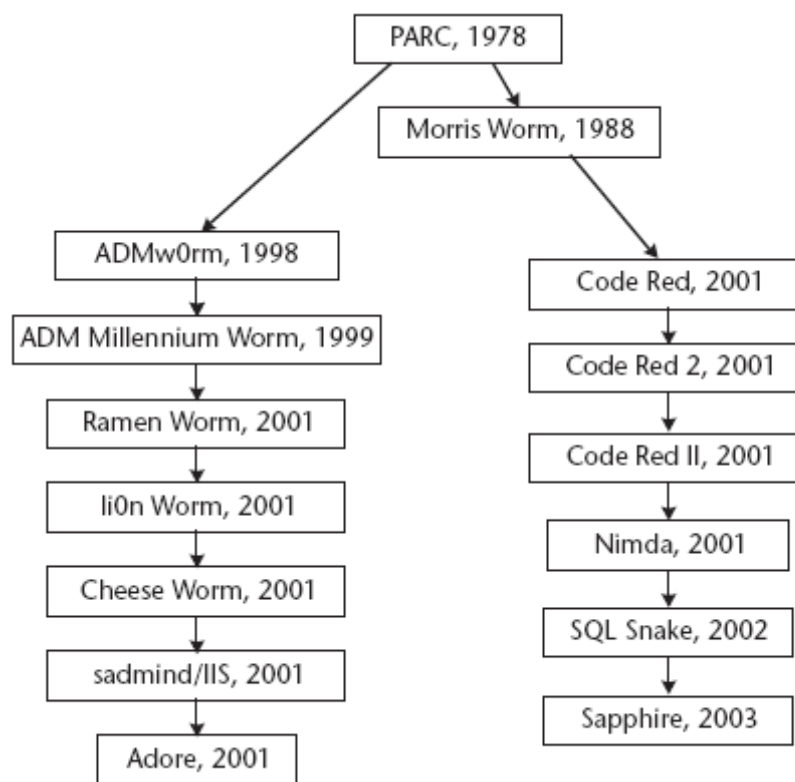


Gambar 2.3 Cara penyebaran *worms*^[3]

2.3 Sejarah Singkat dan Taksonomi Worms

Sejarah *Worms* mulai ada dan dikenal sejak awal internet mulai dipublikasikan. Dimana saat itu para ahli berusaha mengumpulkan informasi dari seluruh jaringan internet yang belum memiliki semacam mesin pencari (*search engine*).

Untuk mengenal sejarah awal keberadaan *worms* ini, secara umum dapat dilihat pada gambar kronologis kemunculan *worms* di bawah ini,



Gambar 2.4 Kronologis worms^[2]

Dari gambar tersebut, secara singkat dapat diketahui bahwa sejak awal penciptaan *worms* di Palo Alto Research Center (PARC) oleh Robert T. Morris, berdasarkan lingkungan sistem operasinya *worms* berkembang dua kategori yaitu, *worms* yang berjalan dengan target sistem operasi UNIX dan *Worms* yang pada sistem operasi Microsoft Windows. *Worms* pada sistem UNIX dan variannya terdiri dari ADMW0rm, ADM Millenium, Ramen, li0n, Cheese, sadmind/IIS, dan Adore.

Sedangkan *worms* yang berjalan pada sistem Microsoft Windows terdiri dari Code Red 1, Code Red 2, Code Red II, Nimda, SQL Snake dan Sapphire.

Beberapa catatan yang dari kronologis *worms* tersebut adalah tentang,

1. Morris *worms*^[2]

Worms ini diciptakan oleh Robert Tappan Morris pada tahun 1988 sebagai proyek riset pada saat menyelesaikan program doktoralnya di Cornell University. Dengan memanfaatkan kelemahan (*vulnerability*) pada *Sendmail Server* dan *Finger Daemon* pada sistem Unix, *worms* ini menyebar dengan setelah menyebabkan keadaan *zero argumenth* pada sistem yang diinfeksi. Teknik penyebaran *worms* ini, masih dipakai hingga saat ini. Efek penyebaran *worms* yang sangat luas ini, menyebabkan pembentukan tim Computer Emergency Response Team (CERT/CERT-CC) oleh Amerika.

2. Ramen *Worms*^[2]

Merupakan *worms* pertama yang berhasil menyebar pada lingkungan Linux. Ia pertama kali di identifikasikan menyerang Red Hat versi 6.1, 6.2, 6.3 dan 7.0., *worms* ini menyebar dengan bantuan *shell scripts exploits* dan *scanner* yang telah dikompilasi (*packed*) menjadi *file binary*. Setelah berhasil menginfeksi dan menjalankan aksinya (*payload*), ia kemudian mencari *host* lain secara acak pada jaringan kelas B.

3. Sadmind/IIS^[2]

Worms ini mampu menyerang *web server* IIS (*Internet Information Service*) Microsoft Windows, melalui kelemahan sistem pada Sun Solaris. Dengan mencari akses *root* pada Sun Solaris yang terhubung dengan sistem Unix, *worms* ini berevolusi dengan mengubah tampilan (*deface*) situs-situs yang menggunakan IIS.

4. Melissa^[2]

Worms ini bukan yang pertama kali menggunakan teknik penyebaran melalui e-mail, tetapi kecepatan penyebaran yang hebat membuat *worms* membuat seluruh pengguna internet/e-mail di dunia menjadi sangat menderita. Rahasia dibalik kesuksesan *worms* ini terletak pada implementasi rekayasa sosial pada

file attachment e-mail yang telah terinfeksi *worms* tersebut. teknik ini sampai sekarang masih efektif dan digunakan oleh *worms-worms* lainnya.

5. Code Red (Code Red 1)^[2]

Begitu *worms* ini beraksi, ia langsung menjadi sebuah standar *worms* lain dalam melakukan infeksi. Teknik yang digunakan adalah melakukan *exploits* pada lubang keamanan sistem yang baru diumumkan oleh vendornya. Waktu yang dibutuhkan *worms* ini dalam usaha untuk mengeksploitasi lubang keamanan suatu sistem, melebihi kecepatan vendor dalam menyediakan *patch* untuk kelemahan sistem tersebut.

6. Code Red II^[2]

Worms ini menggunakan landasan eksploitasi pada pendahulunya yaitu Code Red 1 dan Code Red 2. Dengan Teknik *Island hopping* *worms* ini membuat kecepatan penyebarannya meningkat tiga sampai empat kali lebih cepat dari versi pendahulunya. Teknik ini membuat probabilitas serangan acak pada alamat *Internet Protocol* jaringan kelas A dan B menjadi lebih tinggi, sehingga lebih mudah dan cepat dalam menginfeksi sistem lain.

7. Nimda^[2]

Meskipun diidentifikasi dibuat bukan oleh pembuat Code Red, *worms* ini kemungkinan memiliki tujuan untuk melanjutkan hasil serangan dari Code Red II. Dengan menggunakan teknik yang sama dengan Code Red II, *worms* ini berbeda dalam proses *scanning* alamat IP pada jaringan. Dengan teknik tersebut *worms* ini menyebabkan aktivitas besar-besaran yang menguras sumber daya dalam jaringan.

2.4 Struktur Worms

Lima komponen yang umum dimiliki oleh *worms*^[2] adalah sebagai berikut,

1. *Reconnaissance*.

Komponen *Worms* ini bertugas untuk merintis jalannya penyebaran pada jaringan. Komponen ini memastikan titik-titik (*node*) mana saja pada jaringan yang dapat diinfeksi olehnya.

2. *Attack* .

Komponen ini bertugas untuk melancarkan serangan pada target *node* yang telah teridentifikasi. Bentuk serangan dapat berupa tradisional *buffer* atau *heap overflow*, *string format*, dan sebagainya.

3. *Communications*

Komponen ini membuat tiap *node* yang terinfeksi pada jaringan dapat saling berkomunikasi. Komponen memberikan semacam antar muka (*interface*) agar tiap worm pada jaringan dapat saling mengirim pesan.

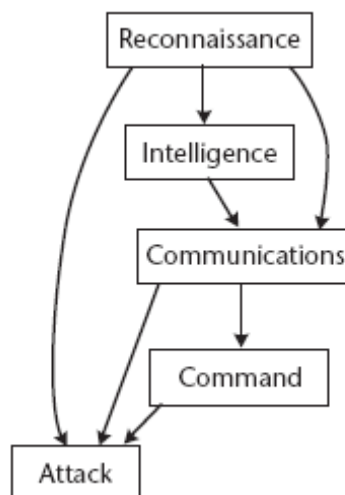
4. *Command*

Komponen ini menjadi semacam pemicu apabila target sudah teridentifikasi. Komponen ini merupakan suatu antar muka agar setiap *worms* dapat mengeluarkan perintah (*command*) pada *worms* di titik lain lain.

5. *Intelligent*

Komponen ini merupakan komponen cerdas yang mampu memberikan informasi bagaimana karakteristik keadaan *worms* di titik lain pada jaringan.

Berikut ini adalah bagaimana proses dari tiap komponen tersebut bekerjasama dalam melakukan suatu serangan



Gambar 2.5 Gambaran proses umum komponen *worms*^[2]

2.5 Tipe-tipe worms

Berdasarkan media penyebarannya worms^[2], dapat digolongkan menjadi,

1. *Email Worms*
2. *Instant Messaging Worms*
3. *Internet Relay Chat (IRC) Worms*
4. *File Sharing Networks Worms*
5. *Internet Worms*

2.6 Pola Lalulintas penyebaran worms^[2]

Secara umum aktivikasi pola penyebaran worms dapat diketahui dengan beberapa cara, antara lain :

1. Prediksi pola penyebaran

Pola penyebaran worms dapat diprediksi dengan formula *Logistic Growth*

Model sebagai berikut,

$$Nda = (Na)K(1 - a)dt$$

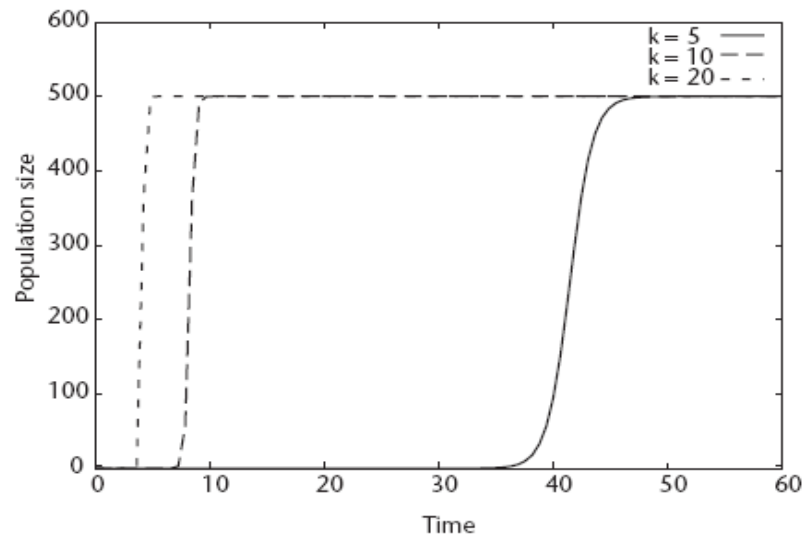
dengan

$$a = \frac{e^{K(t-T)}}{1 + e^{K(t-T)}}$$

Keterangan :

- a : proporsi kelemahan (*vulnerability*) sistem
- t : waktu
- T : waktu konstan pada saat pertumbuhan worms dimulai
- K : skala dari awal *vulnerability* mulai diketahui

Berikut ini adalah contoh grafik dari formula tersebut,



Gambar 2.6 Contoh grafik prediksi pertumbuhan *worms*^[2]

2. Kekacauan yang ditimbulkan pada *Backbone* Internet

Beberapa indikator untuk mengetahui prediksi pertumbuhan *worms* dapat dilakukan dengan mengevaluasi komponen-komponen pada *Backbone* Internet, komponen tersebut adalah,

- a. Data yang dilalukan pada *router* (data routing)
- b. Alamat-alamat *multicast* pada *backbone*
- c. Kondisi pada infrastruktur server yang diserang

3. Hasil observasi

Prediksi pertumbuhan *worms* dapat juga diketahui dengan melakukan observasi pada data aktual dari lalulintas jaringan. Untuk tujuan tersebut terdapat tiga kategori komponen, yaitu,

- a. melalui jaringan besar dari sistem yang diserang
- b. melauli *black hole monitor*
- c. melalui *individual host*

BAB III

ANALISIS WORMS Email-Worm.Win32.Brontok.c

2.1 Tinjauan umum

Perkembangan worms Email-Worm.Win32.Brontok.c yang merupakan varian dari versi awal Email-Worms.Win32.Brontok.a memang tidak secepat versi awalnya. Namun dari efek penyebarannya yang cukup luas yang sempat tercatat pada *wildlist* pada www.wildlist.org pada bulan Maret 2006^[6], membuat *worms* ini cukup berbahaya. Worms ini secara umum memiliki cara kerja yang sama dengan pendahulunya. Berikut ini adalah beberapa data worms Email-Worms.Win32.Brontok.a ,

a. Nama lain (*aliases*)^[7]

Email-Worm.Win32.Brontok.a (KasperskyLab),
W32/Rontokbro.gen@MM (McAfee), W32.Rontokbro@mm (Symantec),
BackDoor.Generic.1138 (Doctor Web), W32/Korbo-B (Sophos),
Worm/Brontok.a (H+BEDV), Win32.Brontok.A@mm (SOFTWIN),
Worm.MytoB.GH (ClamAV), W32/Brontok.C.worm (Panda),
Win32/Brontok.E (Eset)

b. Varian dan Waktu terdeteksi^[7]

Email-Worm.Win32.Brontok.a
Terdeteksi : Oct 12 2005 13:16 GMT

Email-Worm.Win32.Brontok.b
Terdeteksi : Oct 12 2005 15:43 GMT

Email-Worm.Win32.Brontok.c
Terdeteksi : Oct 16 2005 10:03 GMT

Email-Worm.Win32.Brontok.d
Terdeteksi : Jan 21 2006

Email-Worm.Win32.Brontok.e
Terdeteksi : Feb 17 2006 07:56 GMT

Email-Worm.Win32.Brontok.f
Terdeteksi : Feb 20 2006 08:35 GMT

Email-Worm.Win32.Brontok.g
Terdeteksi : Mar 03 2006 20:03 GMT

Email-Worm.Win32.Brontok.h
Terdeteksi : Mar 07 2006 01:56 GMT

Email-Worm.Win32.Brontok.i
Terdeteksi : Mar 08 2006 03:28 GMT

Email-Worm.Win32.Brontok.K
Terdeteksi : Mar 13 2006 03:20 GMT

Email-Worm.Win32.Brontok.l
Terdeteksi : Mar 17 2006 10:40 GMT

Email-Worm.Win32.Brontok.m
Terdeteksi : Mar 20 2006 03:43 GMT

Email-Worm.Win32.Brontok.n
Terdeteksi : Mar 21 2006 06:07 GMT

Email-Worm.Win32.Brontok.o
Terdeteksi : Mar 21 2006 07:33 GMT

Email-Worm.Win32.Brontok.p
Terdeteksi : Apr 06 2006 01:19 GMT

Email-Worm.Win32.Brontok.q
Terdeteksi : May 15 2006 15:08 GMT

Email-Worm.Win32.Brontok.r
Terdeteksi : Jun 12 2006 10:08 GMT

Email-Worm.Win32.Brontok.s
Terdeteksi : Jun 24 2006 07:58 GMT

c. Kategori *level* ^[7]

- *Wild Level*: Rendah
- Jumlah infeksi : 0 - 49
- Jumlah situs terinfeksi : 0 - 2
- Distribusi geografis : Rendah
- Penanggulangan : Menengah

- Tingkat kerusakan : Menengah
- E-mailing: mengirim *mass e-mail* dirinya sendiri.

2.2 Alat dan Bahan

Menurut Yohanes Nugroho^[4] Beberapa alat dan bahan yang diperlukan untuk melakukan analisis kode worms antara lain adalah :

a. Perangkat lunak

Tabel 3.1 Perangkat lunak analisis

No.	Nama	Developer
1.	PE ID 0.9	Sneaker, http://peid.has.it
2.	UnMew 1.12	Northfox, http://northfox.uw.hu
3.	Hexplorer 2.6	Marcindudek, http://sourceforge.net
4.	IDA Pro Advanced 5.0	www.datarescue.com
5.	Norton GoBack 4.0	Symantec Corp., www.symantec.com

b. Perangkat keras

Sebagai lingkungan analisis, digunakan sebuah komputer (PC) dengan spesifikasi :

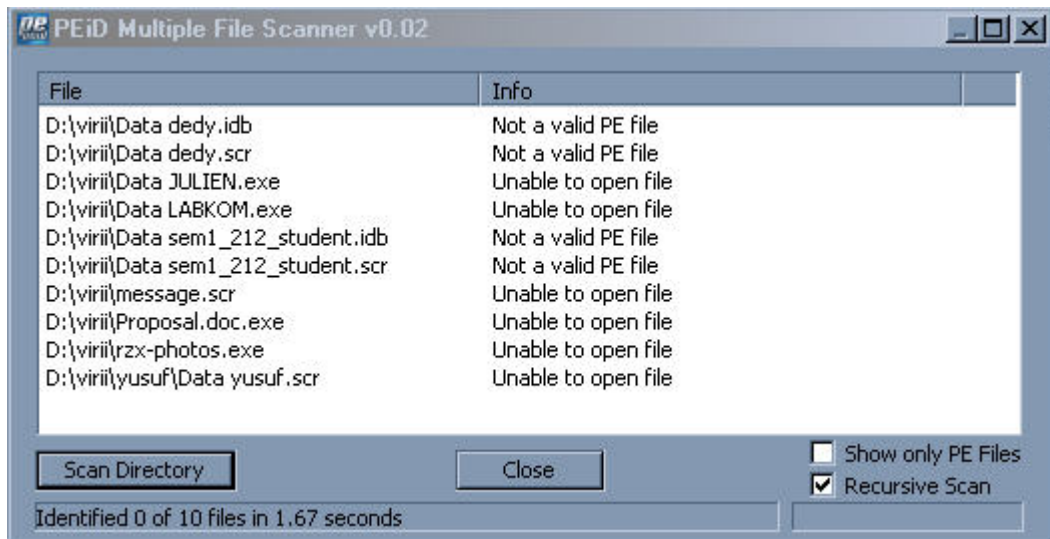
- PC Pentium III 866 Mhz
- Ram 256 Mb
- Hardisk Samsung 40 Gb
- Yang telah berisi sistem operasi Windows XP SP 2, Ms. office 2003, perangkat lunak untuk analisis seperti pada tabel di atas

c. Bahan

Beberapa file yang telah terinfeksi worms Email.Worms.Win32.Brontok.c

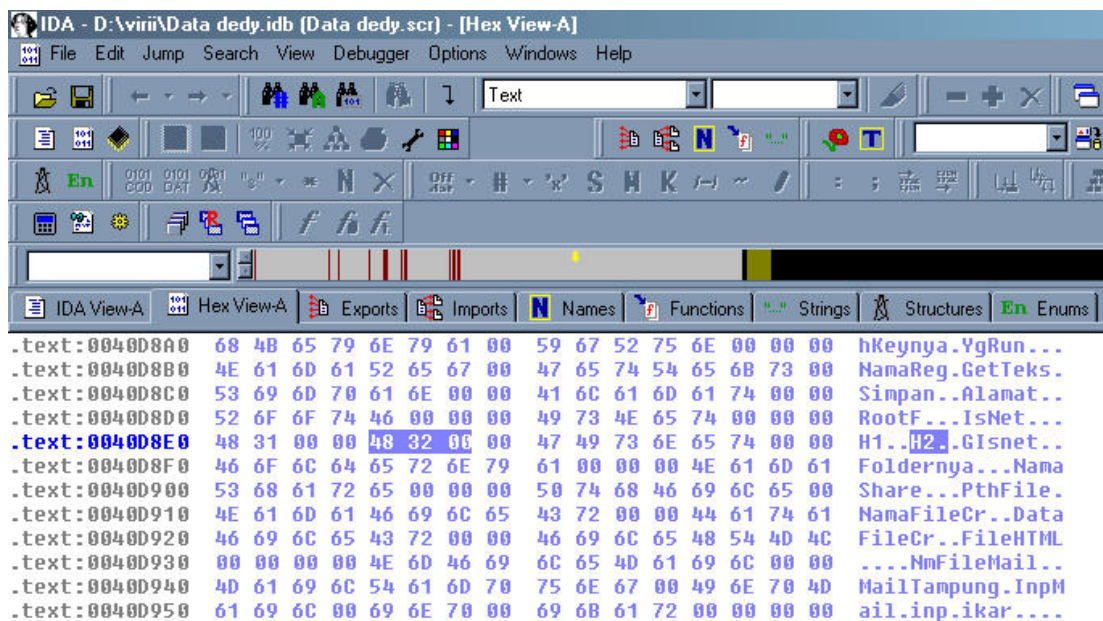
2.3 Proses Analisis

- ### a. Mengidentifikasi perangkat lunak pembuat file *Portable Executable* (PE) dari file terinfeksi. Pada proses ini digunakan perangkat lunak PE-ID yang dapat mengidentifikasi file PE, dengan ekstensi, COM, EXE dan SCR.



Gambar 3.1 Tampilan PE-ID saat mengidentifikasi file terinfeksi

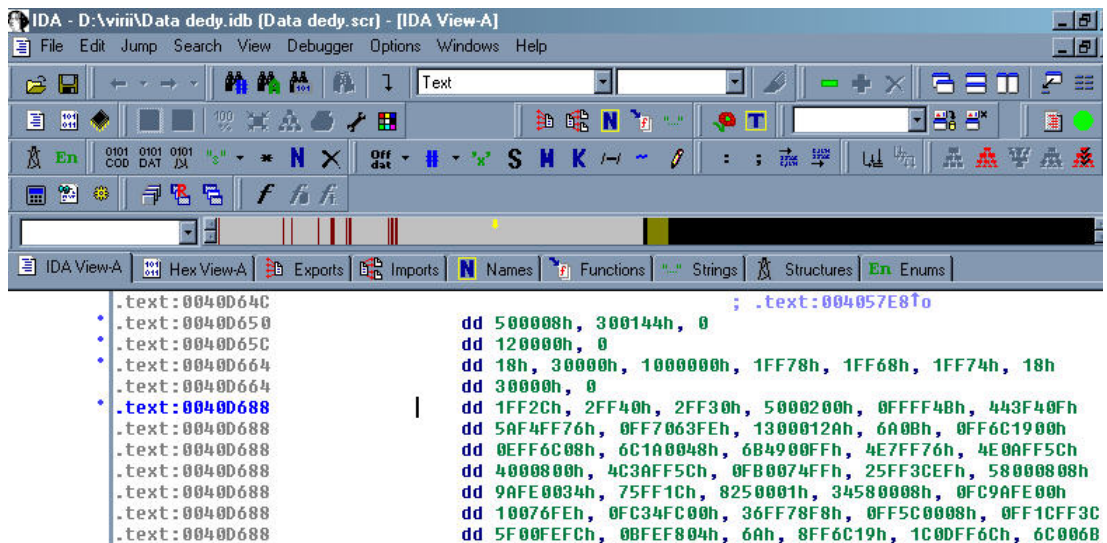
- b. Melakukan *disassembling* file terinfeksi dengan perangkat lunak IDA Pro sehingga diperoleh informasi mengenai potongan-potongan kode program dari worms.



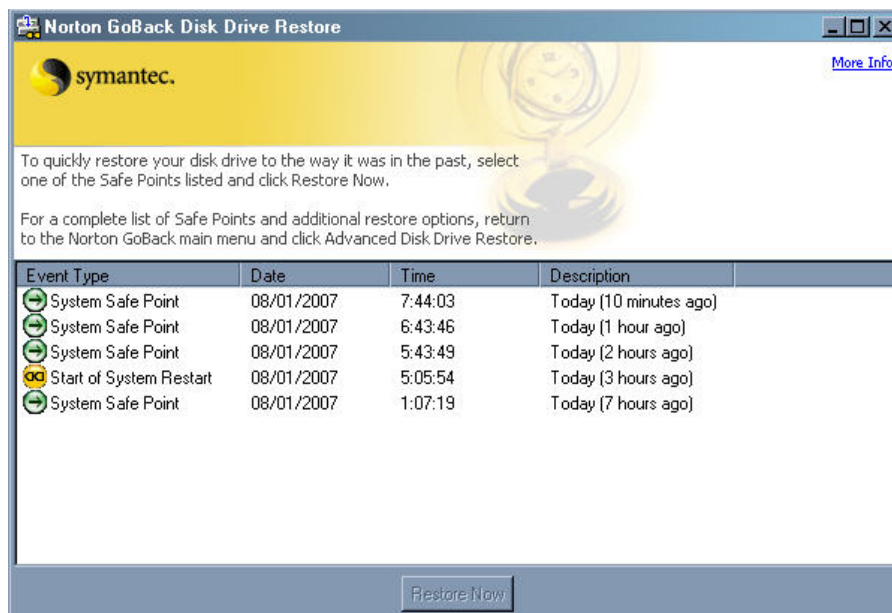
Gambar 3.2 Tampilan IDA Pro saat mengidentifikasi file terinfeksi

c. Melakukan *Debugging* file terinfeksi untuk mengetahui

Proses ini dilakukan dengan tujuan untuk mengetahui “kelakuan” worms pada saat melakukan aksinya. Untuk menandai proses/*state* infeksi digunakan perangkat lunak Norton GoBack agar keadaan sistem operasi dapat dikembalikan pada suatu *state* infeksi.



Gambar 3.3 Tampilan IDA Pro sebelum melakukan *debugging*



Gambar 3.3 Tampilan Norton GoBack melakukan *restore* sistem operasi

2.4 Hasil Analisis

Setelah dilakukan analisis terhadap file terinfeksi, maka didapatkan beberapa informasi tentang Email-Worms.Win32.Brontok.c. hasil analisis ini dikombinasi dengan beberapa analisis dari beberapa sumber.

a. Proses instalasi (infeksi)

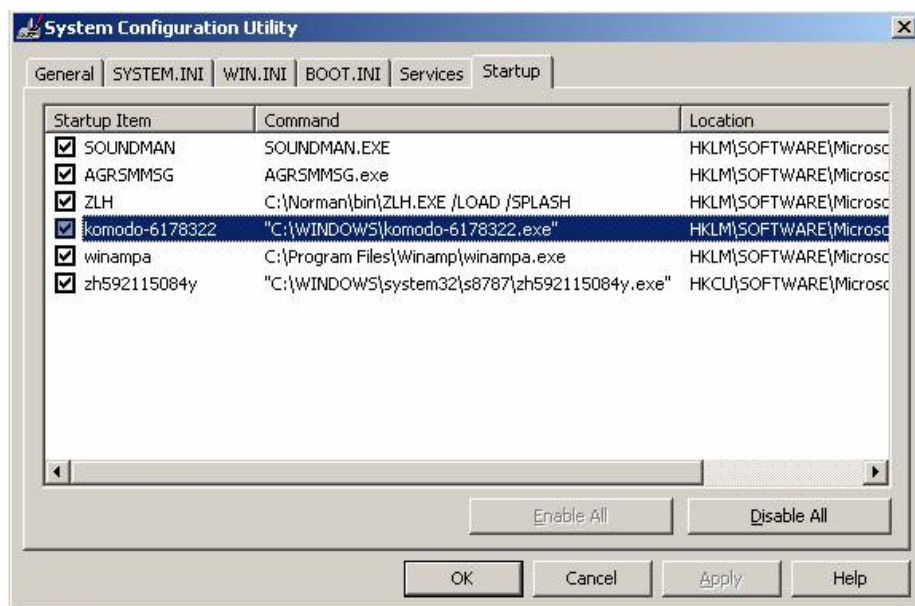
1. Melakukan penambahan beberapa file dan folder pada sistem^[7]

- C:\Windows
_default17832
Cinderawasih-4178327
Komodo-6178322
- C:\Windows\Ad22098
Smss.exe
- C:\Windows\System32\S8787
Csrss.exe
Lsass.exe
Services.exe
Winlogon.exe
Smss.exe
Zh592115084y.exe
C.bron.tok.txt, berisi text Brontok.C, By:Jowobot
- Spread.mail.bro, berisi alamat email yang telah diperoleh dari komputer yang terinfeksi
- Spread.sent.Bro, berisi alamat email yang berhasil dikirimkan
- C:\Documents and Settings\%user%\Local Settings\Application Data
Jalak-932115015-bali.com
Winlogon.exe [berbentuk notepad]
- Dv6211500x, berisi file:
Yesbron.com
- C:\Windows\system32
C_17832k.com
- C:\Documents and Settings\suport\Start Menu\Programs\Startup
Empty.pif
- C:\
Baca Bro !!!.txt
- C:\Windows\System32\n8127
Csrss.exe
Lsass.exe
Services.exe
Winlogon.exe
C.Bron.Tok.txt
- Spread.mail.bro
- Spread.sent.bro
- Sv711917030r.exe
- Smss.exe

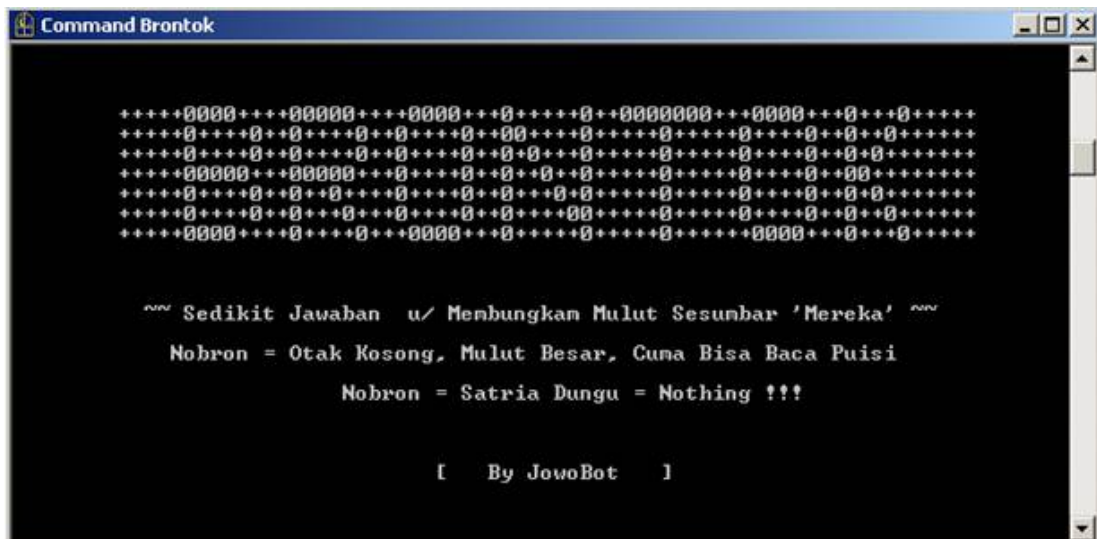
2. Melakukan perubahan *setting registry*^[6]

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
 - Tok-Cirrhatus-3444Admc
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - Bron-Spizaetus-2733VIRM
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - Tok-Cirrhatus-3444Admc
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - Bron-Spizaetus-2733VIRM
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
 - Shell = Explorer.exe "C:\Windows\Cinderawasih-4178327.exe"
 - Userinit = C:\Windows\system32\userinit.exe, C:\Windows\komodo-6178322.exe

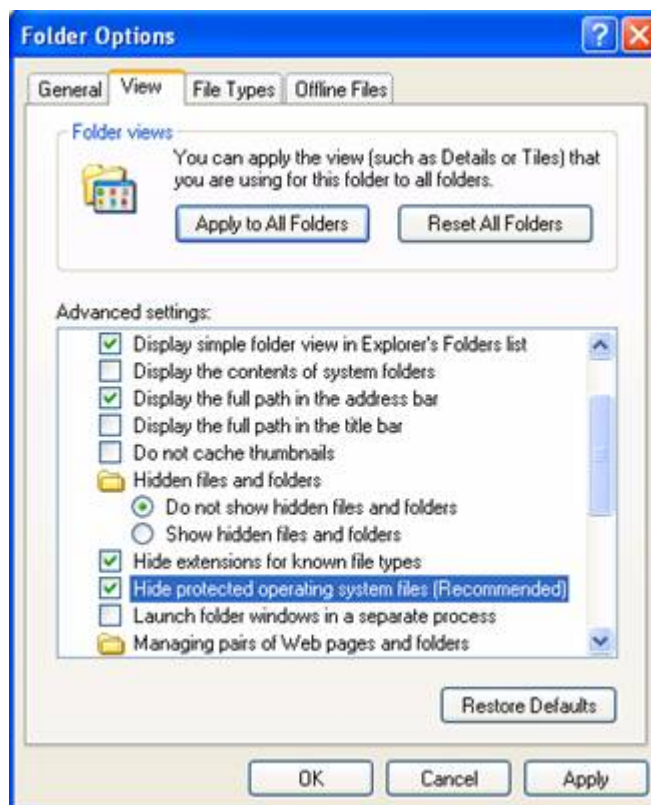
3. Melakukan perubahan konfigurasi sistem pada saat aplikasi Msconfig dan Regedit (pada *command prompt*) dan opsi windows Explorer jalankan,



Gambar 3.4 Tampilan Aplikasi Msconfig terinfeksi



Gambar 3.5 Tampilan Aplikasi Regedit terinfeksi pada *Command prompt*



Gambar 3.6 Opsi Windows Explorer terinfeksi

4. Media Penyebaran^[7],

- Disket/USB/File sharing dengan membuat duplikat berupa file di setiap folder dan sub folder pada media tersebut, dimana file tersebut akan mempunyai ukuran sekitar 48 KB dengan icon Folder.

- *E-mail & attachment*

melalui email dengan terlebih dahulu akan mengambil semua alamat email yang ada dikomputer yang terinfeksi, email yang dikirim biasanya akan mempunyai ciri-ciri sebagai berikut:

Subject:

My Photo on Paris

Foto Liburanku di Bali

Message

This photo was taken from my vacation on Paris, last week.

Wishing you always remember me.

Halo Sobat,

Ini fotoku saat liburan di Bali.

Semoga kamu jadi ingat aku terus.

Terima kasih,

Attachment

Picture.zip

BAB IV

CARA PENANGGULANGAN

EMAIL-WORM.WIN32.BRONTOK.c

Secara umum worms Email-Worms.Win32.Brontok.c dapat ditanggulangi secara manual dengan mengembalikan beberapa setting atau konfigurasi dari sistem yang diinfeksi, Berikut ini adalah cara-cara penanggulangan worms tersebut pada sistem operasi Ms. Windows XP^[7],

1. Jika Matikan [System Restore] untuk sementara selama proses pembersihan
2. Sebaiknya lakukan pembersihan melalui “safe mode”
3. Matikan proses dari virus W32/mybro, Anda dapat menggunakan tools pengganti Task manager seperti [Security task manager], tools tersebut dapat didownload di website <http://www.neuber.com/taskmanager/> matikan proses berikut [ingat !! cari file yang mempunyai bentuk folder].
 - Winlogon
 - Services
 - Lsass
 - Smss
 - Csrss
4. Hapus registry yang pernah dibuat oleh W32/Mybro, copy script berikut di notepad kemudian simpan menjadi repair.inf, jalankan file tersebut, Klik kanan repair.inf, Klik [install]

```
[Version]
Signature="$Chicago$"
Provider=Vaksincom
[DefaultInstall]
AddReg=UnhookRegKey
DelReg=del
[UnhookRegKey]
HKLM, Software\CLASSES\batfile\shell\open\command,,,"%1" %*
HKLM, Software\CLASSES\comfile\shell\open\command,,,"%1" %*
HKLM, Software\CLASSES\exefile\shell\open\command,,,"%1" %*
```

```

HKLM, Software\CLASSES\piffile\shell\open\command,,,"%1" %*"
HKLM, Software\CLASSES\regfile\shell\open\command,,,"regedit.exe %1"
HKLM, Software\CLASSES\scrfile\shell\open\command,,,"%1" %*"
HKLM, SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, Shell,0,
"Explorer.exe"
HKLM, SYSTEM\ControlSet001\Control\SafeBoot, AlternateShell,0, "cmd.exe"
HKLM, SYSTEM\CurrentControlSet\Control\SafeBoot, AlternateShell,0, "cmd.exe"
[del]
HKCU,
Software\Microsoft\Windows\CurrentVersion\Policies\System,DisableRegistryTools
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\System,DisableCMD
HKCU,
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer,NoFolderOptions
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\System,DisableTaskMgr
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run
HKCU, Software\Microsoft\Windows\CurrentVersion\Run,Tok-Cirrhatus-3444Admc
HKLM, SOFTWARE\Microsoft\Windows\CurrentVersion\Run,Bron-Spizaetus-2733VIRM
HKLM,
SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer,ShowSuperHidden
HKLM, SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\run

```

5. Hapus file *Empty.pif* pada direktori

- C:\Documents and Settings\suport\Start Menu\Programs\Startup

6. Hapus file yang pernah dibuat oleh virus, sebelumnya pastikan anda telah menampilkan semua file yang disembunyikan, jika folder option belum muncul juga coba restart komputer terlebih dahulu kemudian booting ke mode “safe mode”, setelah itu hapus file berikut:

- Pada C:\Windows
 - _default17832
 - Cinderawasih-4178327
 - Komodo-6178322
 - C:\Windows\Ad22098
 - Smsg.exe
- Pada C:\Windows\System32\S8787
 - Csrss.exe
 - Lsass.exe
 - Services.exe
 - Winlogon.exe
 - Smsg.exe

- Zh592115084y.exe
 - C.bron.tok.txt, berisi text
 - **Brontok.C**
 - **By:Jowobot**
 - Spread.mail.bro, berisi alamat email yang telah diperoleh dari komputer yang terinfeksi
 - Spread.sent.Bro, berisi alamat email yang berhasil dikirimkan
 - C:\Documents and Settings\%user%\Local Settings\Application Data
 - Jalak-932115015-bali.com
 - Winlogon.exe [berbentuk notepad]
 - Dv6211500x, berisi file:
 - Yesbron.com
 - C:\Windows\system32
 - C_17832k.com
 - C:\Documents and Settings\suport\Start Menu\Programs\Startup
 - Empty.pif
 - C:\
 - Baca Bro !!!.txt
7. Harus perhatikan juga ukuran file yang terinfeksi tersebut, karena jika file yang terinfeksi [file induk] mempunyai ukuran 51 KB W32/Mybro selain membuat file induk diatas juga akan membuat beberapa file induk tambahan diantaranya:
- C:\Windows\System32\n8127
 - Csrss.exe
 - Lsass.exe
 - Services.exe
 - Winlogon.exe
 - C.Bron.Tok.txt
 - Spread.mail.bro
 - Spread.sent.bro
 - Sv711917030r.exe
 - Smss.exe

- C:\Windows\SY20118
 - Smss.exe
8. Hapus file [task scheduled] yang dibuat oleh W32/Mybro
 9. Klik [start]
 10. Klik [Settings]
 11. Klik [control panel]
 12. Klik 2 kali menu [Scheduled task]
 13. Hapus file AT1 dan AT2
 14. Hapus string [daftar website yang diblok] yang dibuat oleh W32/Mybro pada file HOST yang berada dilokasi
 15. C:\Windows\System32\Drivers\ETC
 16. Ubah kembali file *MSVBVM60.dll.xxx* [dimana xxx menunjukkan angka] menjadi nama file *MSVBVM60.dll* pada direktori C:\Windows\system32
 17. Coba cari dan hapus file duplikat yang dibuat oleh virus, dengan ciri-ciri
 - Ukuran 48 KB atau 51 KB
 - Icon yang digunakan berbentuk FOLDER
 - Ekstensi file EXE
 - Type file “Application”
 18. Catatan:

Dari hasil pengujian virus ini tidak membuat file duplikat pada local disk
Untuk pembersihan optimal dan mencegah infeksi ulang, gunakan antivirus yang sudah dapat mengenali virus ini dengan baik.

DAFTAR PUSTAKA

- [1] Szor, Peter (2005), *The Art of Computer Virus Research and Defense*, Addison Wesley Professional, New Jersey.
- [2] Nazario, Jose, et. al., (2004), *Defense and Detection Strategies Againsts Internet Worms*, Artech House inc., Norwood MA.
- [3] Erbschloe, Michael, et. al., (2005), *Trojan, Worms, and Spyware: A Professional Guides to Mallicious Code*, Elsevier inc. Burlington MA.
- [4] Yohanes Nugroho (2005), *Analisis Lengkap Virus Brontok*, [http://www.compactbyte.com/brontok/Analisis Lengkap Virus Brontok.html](http://www.compactbyte.com/brontok/Analisis%20Lengkap%20Virus%20Brontok.html), 11 September 2006.
- [5] Gordon, A., Lawrence et. al., (2006), *CSI/FBI Computer Crime and Security Survey 2006*, CSI Publication, Washington DC, <http://www.GoCSI.com/>, 1 November 2006.
- [6] _____(2006), *PC Viruses in-the-wild 2005-2006*, Wildlist Organization Internationa, <http://www.wildlist.org/>, 9 Oktober 2006.
- [7] _____(2006), PT Vaksincom, <http://vaksin.com/>, 9 Oktober 2006.