JURNAL ILMIAH **Vol. XIX, No.1, Maret 2023**

INFOKAM

INFORMASI KOMPUTER AKUNTANSI DAN MANAJEMEN

ISSN 1829 - 7458
E-ISSN 2798 - 4753

SK DIREKTUR AMIK "JTC" SEMARANG
NO. 6856/AMIK-JTC/DIR/XII/2022

Jurnal Ilmiah INFOKAM terbit minimal setiap 6 bulan sekali (2 X dalam setahun, bulan Maret & September) oleh AMIK "JTC" Semarang dengan maksud sebagai media informasi tentang Komputer, Akuntansi dan Manajemen bagi Sivitas Akademika pada khususnya dan masyarakat pada umumnya.

Alamat Redaksi / Penerbit :

Badan Penerbit Pusat Penelitian dan Pengabdian Masyarakat (BP-P3M)
AKADEMI MANAJEMEN INFORMATIKA DAN KOMPUTER
"JAKARTA TEKNOLOGI CIPTA"
Jl. Kelud Raya No. 19 Telp. 024 – 8310002 Semarang
www.amikjtc.com/jurnal, email : infokam.amikjtc@gmail.com

JURNAL ILMIAH **Vol. XIX, No. 1, Maret 2023**

INFOKAM

INFORMASI KOMPUTER AKUNTANSI DAN MANAJEMEN

ISSN 1829 - 7458
E-ISSN 2798 - 4753

DAFTAR ISI

Mengenal Lebih Dalam Tentang Virus-Virus Komputer dan Perilakunya

Sugeng Murdowo
Sugengmurdowo0298@gmail.com
Komputerisasi Akuntansi - AMIK JTC Semarang

Abstrak

Virus komputer pada umumnya menginfeksi menginfeksi *file* sistem operasi yang terus menyebar ke dalam sistem yang berakibat sistem operasi yang terpasang menjadi rusak dan ada kemungkinan kita kehilangan data yang sangat penting. Banyaknya jenis virus dengan perilaku yang berbeda serta menghasilkan dampak yang berbeda pula sangat merepotkan dan mengganggu hampir semua pengguna komputer. Untuk itu perlu menyiapkan *software* anti virus yang baik dan handal serta selalu melakukan update *database* virus di personal komputer ataupun laptop agar dapat mendeteksi virus dengan baik dan sempurna.

Kata Kunci : Virus, Deteksi Virus, Perilaku Virus

Abstrack

Computer viruses generally infect operating system files which continue to spread throughout the system resulting in the installed operating system being damaged and there is a possibility that we may lose very important data. The many types of viruses with different behavior and produce different impacts are very inconvenient and disturbing for almost all computer users. For this reason, it is necessary to prepare good and reliable anti-virus software and always update the virus database on a personal computer or laptop so that it can detect viruses properly and perfectly.

***Keyword** : Virus, Virus Detection, Virus Behavior*

1. Pendahuluan

Pesatnya perkembangan komputer sebagai alat bantu manusia di bidang informasi, bisnis, dan pendidikan menunjukkan semakin besar peranannya dalam kehidupan manusia. Semakin banyak pula jenis *software* yang digunakan untuk membantu dalam menyelesaikan pekerjaan, yang berakibat banyak celah yang bisa ditembus dari sisi keamanan sistemnya. Keamanan komputer juga mencakup tentang keamanan data dari serangan virus komputer. Para pengguna yang komputernya diserang oleh virus komputer merasa tidak nyaman dan bisa jadi memperlambat kinerja atau bahkan menghilangkan beberapa data yang ada dikomputer.

Virus komputer pada umumnya menginfeksi *file* sistem operasi yang terus menyebar ke dalam sistem yang berakibat sistem operasi yang terpasang menjadi rusak. Semakin pesatnya perkembangan virus sehingga meskipun komputernya sudah dipasang anti virus kadangkala tetap bisa terinfeksi virus hal tersebut biasanya disebabkan pengguna tidak mengupdate data anti virus dengan versi terbaru.

Virus komputer merupakan penyakit umum dalam dunia teknologi modern, virus dapat menyebar dengan cepat melalui jaringan komputer yang terbuka seperti Internet yang berakibat kerugian hingga milyaran dolar dalam waktu singkat.

2. Kerangka Teori

a. **Pengertian Virus**

"A program that can infect other programs by modifying them to includea slighty altered copy of itself. A virus can spread throughout a computer system or network using the authorization of every user using it toinfect their programs. Every programs that gets infected can also act asa virus that infection grows "(Fred Cohen) Pertama kali istilah "virus" digunakan oleh Fred Cohen pada tahun 1984 di Amerika Serikat (Cohen, 1984)

Virus komputer dinamakan "Virus" karena memiliki beberapa persamaan mendasar dengan virus pada istilah kedokteran (*biological viruses*). Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya, yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya. Ada yang perlu dicatat disini,

virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, disinilah perbedaannya dengan "*worm*".

Pada dasarnya virus komputer dapat diklasifikasi menjadi dua tipe. Tipe virus komputer yang pertama dibuat untuk tujuan penelitian dan studi, dan tidak dipublikasikan. Sedangkan tipe kedua yang merupakan kebalikan dari tipe pertama, merupakan virus komputer yang membahayakan sistem komputer pada umumnya, sering kali disebut dengan istilah virus '*in the wild*'.

b. **Sejarah Virus**

Berikut adalah sekilas sejarah mengenai virus komputer (Ludwig, 1984) :

1981 Virus '*in the wild*' pertama ditemukan. Virus yang bernama Elk Cloner ini menyebar melalui *floppy disk* pada komputer Apple II.

1983 Fred Cohen dalam paper-nya yang berjudul '*Computer Viruses – Theory and Experiments*' memberikan definisi pertama mengenai virus komputer dan memaparkan eksperimen yang telah dilakukannya untuk membuktikan konsep dari sebuah virus komputer. Bersama dengan Len Adelman, ia menciptakan sebuah contoh virus pada komputer VAX 11/750 dengan sistem operasi Unix.

1986 Sepasang kakak adik dari Pakistan, Basit dan Amjad, menciptakan sebuah *boot sector virus* pertama yang diberi nama Brain. Brain sering kali disebut sebagai virus komputer pertama di dunia. *PC-based* Trojan pertama diciptakan dalam bentuk program *shareware* yang diberi nama *PC-Write*. Dalam beberapa laporan disebutkan bahwa *file virus* pertama, Virdem, juga ditemukan pada tahun yang sama. Virdem diciptakan oleh Ralf Burger.

1987 Virus-virus *file infector* seperti *Leigh* mulai bermunculan, kebanyakan menyerang file COM seperti COMMAND.COM. Pada tahun yang sama muncul virus penyerang file-file EXE pertama, Suriv 01 dan 02 serta Jerusalem. *Mainframe* IBM mengalami serangan worm IBM Christmas Worm dengan kecepatan replikasi setengah juta kopi per jam.

1988 Virus pertama yang menyerang komputer Macintosh, MacMag dan Scores, muncul. Pada tahun yang sama didirikan CERT (*Computer Emergency Response Team*) oleh DARPA dengan tujuan awalnya untuk mengatasi serangan Morris Worm yang diciptakan oleh Robert Morris.

1989 AIDS Trojan muncul sebagai trojan yang menggunakan samaran sebagai AIDS information program. Ketika dijalankan trojan ini akan mengenkripsi *hard drive* dan meminta pembayaran untuk kunci dekripsinya.

1990 *Virus Exchange Factory* (VX) BBS yang merupakan forum diskusi *online* para pencipta virus didirikan di Bulgaria. Mark Ludwig menulis buku "*The Little Black Book of Computer Viruses*" yang berisi cara-cara untuk menciptakan berbagai jenis virus komputer.

1991 Virus polymorphic pertama, Tequila, muncul di Swiss. Virus ini dapat mengubah dirinya untuk menghindari deteksi.

1992 Kehadiran virus Michaelangelo yang menjadi ancaman bagi seluruh dunia, namun demikian kerusakan yang ditimbulkan pada akhirnya tidak terlalu hebat. Kemuculan beberapa *tool* yang dapat digunakan untuk menciptakan virus seperti *Dark Avenger Mutation Engine* (DAME) yang dapat mengubah virus apa pun menjadi virus *polymorphic*, dan *Virus Creation Lab* (VCL) yang merupakan kit pertama yang dapat digunakan untuk menciptakan virus.

1995 Para *hacker* dengan nama '*Internet Liberation Front*' melakukan banyak serangan pada hari *Thanksgiving*. Beberapa badan yang menjadi korban serangan ini adalah Griffith Air Force Base, Korean Atomic Research Institute, NASA, GE, IBM, dll. Virus macro pertama yang menyerang aplikasi Microsoft Word, Concept, dikembangkan.

1996 Kemunculan virus Boza yang didesain khusus untuk menyerang file-file Windows 95, virus Laroux yang merupakan virus penyerang Microsoft Excel pertama, virus

Staog yang merupakan virus Linux pertama. 1998 Kemunculan virus Java pertama, Strange Brew. *Back Orifice* merupakan trojan pertama yang dapat digunakan sebagai *tool* untuk mengambil alih kendali komputer *remote* melalui Internet. Pada tahun ini, virus-virus macro lainnya bermunculan.

1999 Kemunculan virus Melissa yang merupakan kombinasi antara virus macro yang menyerang aplikasi Microsoft Word dan *worm* yang menggunakan *address book* pada aplikasi Microsoft Outlook dan Oulook Express untuk mengirimkan dirinya sendiri melalui *email*. Virus Corner merupakan virus pertama menyerang file-file aplikasi MS Project.

Virus Tristate merupakan virus macro yang bersifat multi-program menyerang aplikasi Microsoft Word, Excel, dan PowerPoint.

Bubbleboy merupakan *worm* pertama yang dapat aktif hanya dengan membuka email melalui aplikasi Microsoft Outlook tanpa memerlukan *attachment*.

2000 Serangan *Distributed Denial of Service* (DDoS) pertama membuat kerusakan pada situs-situs besar seperti Yahoo!, Amazon.com, dan lain-lain.

Love Letter merupakan *worm* dengan kecepatan menyebar tertinggi pada saat itu yang menyebabkan kerusakan pada banyak sistem *email* di seluruh dunia.

Liberty Crack yang merupakan *worm* pertama untuk peralatan PDA. 2001 Gnuman (Mandragore) merupakan *worm* pertama yang menyerang jaringan komunikasi *peer to peer*. *Worm* ini menyamarkan diri dalam bentuk *file* MP3 yang dapat di *download*. Kemunculan virus yang didesain untuk menyerang baik sistem operasi Windows maupun Linux, seperti Winux atau Lindose. Virus LogoLogic-A menyebar melalui aplikasi MIRC dan e-mail.

2002 Virus LFM-926 merupakan virus pertama yang menyerang *file-file* aplikasi *Shockwave Flash*. Donut merupakan *worm* pertama yang menyerang .NET *services*.

SQLSpider merupakan *worm* yang menyerang aplikasi yang menggunakan teknologi Microsoft SQL Server

2003 SQL SLAMMER Pada dasarnya adalah paket jaringan replikasi diri, *worm* ini mengeksploitasi kerentanan di Microsoft SQL Server dan menyebar dengan cepat, menginfeksi sebagian besar korban hanya dalam waktu sepuluh menit. Internet menjadi sangat lambat hari itu.

2004 MYDOOM *Worm mailer* massal yang menyebar selama dekade pertama abad ke-21. Versi asli tercatat karena penyebarannya yang cepat, tetapi paling diingat karena melakukan serangan DDoS (*Distributed Denial of Service*) pada SCO Group dan Microsoft, yang keduanya kemudian menawarkan $250.000 untuk informasi yang mengarah pada penangkapan pengembang *malware*.

2005 COMMWARRIOR Virus ponsel pertama yang dapat menyebar melalui pesan MMS dan *Bluetooth*, Commwarrior menargetkan *smartphone* Symbian Series 60. Dampaknya kecil, tetapi implikasinya terhadap para ahli AV sangat besar.

2005 BRONTOX Virus indonesia yang menyebar ke seluruh dunia, dan saat itu sulit dikenali oleh sebagian produsen besar *antivirus*.

2006 VB.NEI Juga dikenal sebagai Nyxem, Blacmal atau Mywife, dia menerima banyak perhatian karena menggunakan penghitung yang memungkinkan peneliti untuk melacak jumlah *host* yang terinfeksi. VB.NEI juga terkenal karena menghapus *file*, mengingatkan pada hari-hari awal virus penghancur data yang sekarang telah langka.

2007 STORM Dideteksi oleh ESET sebagai Nuwar, *worm Storm* terkenal menginfeksi komputer di seluruh Eropa dan Amerika Serikat, disebarkan melalui *email* yang mengabarkan mengenai bencana akibat cuaca buruk dan kemudian terdeteksi dalam *email* palsu dengan subjek mulai dari Saddam Husein hingga Fidel Castro. Komputer yang terinfeksi menjadi bagian dari botnet.

2008 CONFICKER Pernahkah botnet menyebar begitu luas, begitu lama, dan menarik begitu banyak perhatian media, tanpa benar-benar melakukan banyak hal? Meski begitu, penggunaannya algoritma *fluxing* untuk menghambat pelacakan menjadi indikasi pengembangan *malware* di masa depan.

2009 TDL3 *Rootkit* TDL3 yang inovatif, adaptif, dan penerusnya (TDL3+, TDL4) telah terbukti sangat menjengkelkan dalam hal persistensi. Ini juga memperkenalkan tipuan baru dari ide-ide lama seperti jaringan P2P dan menyembunyikan *malware*, sama seperti *malware* sebelumnya telah menggunakan *bad sector*, ruang kosong, atau aliran, TDL telah menggunakan sistem *file* tersembunyi secara efektif.

2010 STUXNET *Worm* kelas militer pertama yang menjadi berita besar yang mempengaruhi *low volume sistem*, *Worm* ini menargetkan *Industrial Control System* (ICS) dan digunakan untuk menyerang fasilitas nuklir Iran.

2011 KELIHOS Suksesor *worm Storm*, botnet ini terutama digunakan untuk menjalankan kampanye *spam* dan mencuri informasi.

2012 MEDRE Ditemukan oleh tim ESET mencuri informasi dokumen AUTOCAD Sebuah virus pencuri informasi yang mengincar dokumen AutoCAD mengancam perusahaan besar dan banyak terjadi di Peru.

2013 HESPERBOT virus ini kaategori trojan canggih yang bertujuan pada pengguna perbankan *online* dengan operasi *phising* terhadap organisasi besar. Pelaku memperoleh kredensial masuk dengan memikat korbannya untuk menjalankan *malware*.

2014 WINDIGO *malware* setiap hari mengirimpan jutaan *email spam* bertujuan membajak *server*, menginfeksi dan mencuri informasi.

2015 BLACKENERGY *Malware* menempel di ICS/SCADA. *Supervisory Control And Data Acquisition* (SCADA) adalah sebuah *Industrial Control System* (ICS) yang biasanya digunakan pada pabrik, industri, infrastruktur dan sistem layanan.

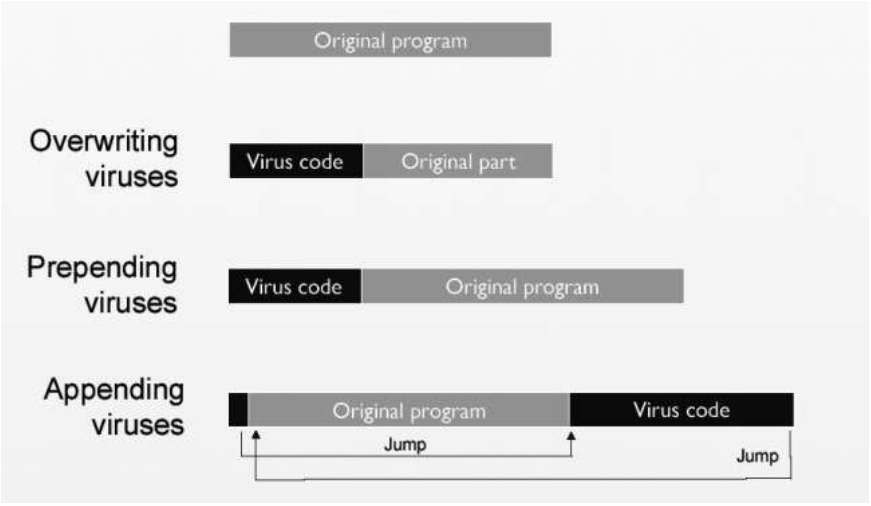
2016 INDUSTROYER *Industrial Control System* akan diekploitasi oleh *Malware* modern ini dan *malware* ini mengakibtkan terjadinya pemadaman listrik kedua di Kiev ibu kota Ukraina.

2017 TELEBOTS merupakan evolusi dari BlackEnergy, wabah NotPetya disebarkan oleh *virus malware*, *malware* akan menghapus *disk* sehingga mengganggu operasi bisnis global berakibat kerugian miliaran dolar.

2018 GREYENERGY merupakan *malware* yang ditemukan ESET dirancang untuk mengeksploitasi ICS/SCADA dan memiliki berbagai modul. *Malware* ini bertujuan untuk spionase dan pengintaian, dikategorikan sebagai mencuri *file*, *backdoor*, *keylogging*, mengambil *screenshot*, kata sandi, pencurian kredensial, dan banyak lagi.

c. **Cara Kerja Virus Komputer**

Proses replikasi sebuah virus dengan cara memodifikasi program lain sehingga virus tersebut menjadi bagian dari program tersebut. Sehingga setiap kali program tersebut dieksekusi, virus akan dieksekusi pula dan menyerang program lain.



Gambar 1 : Gambaran Fisik Virus Komputer

Tampak pada gambaran fisik di atas 3 jenis virus komputer yaitu (Chen, 2003) :

1) ***Overwriting viruses***: virus ini menjadi bagian dari program *host* dengan 'menimpa' (menggantikan) bagian awal dari program tersebut, sehingga program *host* tidak akan mengalami perubahan ukuran, namun mengalami kerusakan dan tidak dapat berfungsi sebagaimana mestinya.
2) ***Prepending viruses***: virus bereplikasi dengan menjadi bagian awal dari program *host* sehingga ketika program *host* dieksekusi, sebelum program *host* virus akan terlebih dahulu dieksekusi. Keberadaan virus tidak menyebabkan kerusakan fungsional pada program *host* namun akan memperbesar ukuran program *host*.
3) ***Appending viruses***: virus bereplikasi dengan menjadi bagian akhir dari program *host* tanpa merubah isi dari program *host*. Namun pada bagian awal program yang telah terinfeksi diberikan mekanisme agar ketika program dieksekusi, virus akan dieksekusi terlebih dahulu.

d. **Cara Kerja/Perilaku Berbagai Jenis Virus Komputer :**

File infector virus: memiliki kemampuan untuk melekatkan diri (*attach*) pada sebuah *file*, yang biasanya merupakan *file executable*. Pada umumnya virus jenis ini tidak menyerang *file* data. Namun dewasa ini, sebuah *file* data atau dokumen lainnya dapat mengandung kode *executable* seperti *macro*, yang dapat dieksploitasi oleh pencipta virus komputer, *worms* atau *trojan horse*.

Boot sector virus: memodifikasi program yang berada di dalam *boot sector* pada DOS-*formatted disk*. Pada umumnya, sebuah *boot sector* virus akan terlebih dahulu mengeksekusi dirinya sendiri sebelum proses *bootup* pada PC, sehingga seluruh *floppy* disk yang digunakan pada PC tersebut akan terjangkiti pula.

Multipartite virus: memiliki fitur dari kedua jenis virus di atas (baik sebagai *file infector* mau pun sebagai *boot/system* sector virus). Ketika sebuah *file* yang terinfeksi oleh virus jenis ini dieksekusi, maka virus akan menjangkiti *boot sector* dari *hard disk* atau *partition sector* dari komputer tersebut, dan sebaliknya.

Macro virus: menjangkiti program macro dari sebuah *file* data atau dokumen (yang biasanya digunakan untuk *global setting* seperti *template* Microsoft Word), sehingga dokumen berikutnya yang diedit oleh program aplikasi tersebut akan terinfeksi pula oleh *macro* yang telah terinfeksi sebelumnya.

Stealth virus: virus ini bekerja secara residensial (menetap) di dalam memori dan menyembunyikan perubahan yang telah dilakukannya terhadap file yang dijangkiti. Hal ini dilakukan dengan mengambil alih fungsi sistem jika terjadi proses pembacaan. Jika program lain meminta informasi dari bagian sistem yang telah dijangkiti virus *stealth*, maka virus akan

memberikan informasi yang sesuai dengan keadaan sebelum terjangkiti virus, sehingga seolah-olah sistem berfungsi dalam keadaan baik tanpa gangguan dari virus komputer.

Polymorphic virus: virus yang cenderung melakukan perubahan di dalam kodenya setiap kali mengalami proses replikasi sehingga sulit untuk dideteksi oleh anti-virus *software*.

Companion virus: adalah virus yang bekerja dengan berpura-pura menggantikan *file* yang hendak diakses oleh pengguna. Sebagai contoh dalam sistem operasi DOS, *file* A.EXE dapat diinfeksi dengan membuat sebuah *file* dengan nama A.COM. DOS akan terlebih dahulu akan mencari *file* berekstensi COM sebelum file dengan ekstensi EXE. Setelah A.COM telah dieksekusi, kemudian A.EXE akan dieksekusi pula sehingga *file* tersebut terinfeksi pula. Cara lain adalah dengan menempatkan sebuah file dengan nama yang persis sama pada cabang lain dari *file tree*, sehingga bila *file* palsu ini ditempatkan secara tepat dan terjadi kesalahan dengan tidak menuliskan *path* yang lengkap dalam menjalankan sebuah program, akan berakibat tereksekusinya *file* palsu tersebut.

Tunneling virus: virus ini mencoba untuk mengambil alih *interrupt handlers* pada DOS dan BIOS, kemudian meng-install dirinya sehingga berada 'di bawah' program-program lainnya.

Dengan ini virus dapat menghindari hadangan dari program anti virus sejenis *monitors*.

Fast Infectors Virus: Virus jenis ini tidak hanya menyerang ketika program target dieksekusi, melainkan juga ketika diakses. Hal ini bertujuan untuk menumpangi perangkat anti virus sebagai media penyebaran ketika melakukan pengecekan terhadap *file-file* di dalam komputer.

Slow Infectors Virus: merupakan kebalikan dari *fast infectors*, di mana virus hanya akan menyebar ketika *file-file* target diciptakan atau dimodifikasi. Hal ini bertujuan untuk memperdaya anti virus sejenis *integrity checkers* dengan menumpangi proses yang 'sah' untuk mengubah sebuah *file*.

Armoured virus: merupakan virus yang dibuat sedemikian rupa sehingga sulit untuk peneliti anti-virus dalam mempelajari cara mereka bekerja.

e. **Cara Penyebaran Dan Jenis Virus**

Berikut adalah gambaran umum cara penyebaran berbagai jenis virus komputer yang umum pada saat ini (Li, 2003), (Yudanto dkk, 2010), (Suliyanto, 2010).

Boot Sector Virus, Sebuah PC terinfeksi oleh *boot sector* virus jika PC tersebut di-*boot* atau di-*re-boot* dari *floppy disk* yang telah terinfeksi oleh virus jenis ini. *Boot sector* virus cenderung tidak menyebar melalui jaringan komputer, dan biasanya menyebar akibat ketidaksengajaan penggunaan *floppy disk* yang telah terinfeksi.

Dalam menggandakan dirinya akan memindahkan atau menggantikan *boot sector* asli dengan program *booting virus*. Sehingga saat terjadi *booting* maka virus akan diload ke memori dan selanjutnya virus akan mempunyai kemampuan mengendalikan *hardware* standar (misalnya: monitor, printer, dll) dan dari memori ini virus akan menyebar ke seluruh *drive* yang ada dan terhubung ke komputer.

Persembunyian : Virus ini bersembunyi di dalam memori hingga DOS mengakses floppy disk, Dan ke manapun data yang *boot* akses, virus menginfeksi itu.

Contoh virus:

1) Variant virus wyx, misalnya wyx.C (B) menginfeksi *boot record* dan *floppy*. Panjang: 520 bytes. Karakteristik: *memory resident* dan terenkripsi.
2) Variant V-Sign, menginfeksi *Master Boot Record*. Panjang: 520 bytes. Karakteristik: menetap di memori (*memory resident*) , terenkripsi, dan *polymorphic*.
3) *Stoned*. june 4 /bloody!, menginfeksi *Master Boot Record* dan *floppy*. Panjang: 520 bytes. Karakteristik: menetap di memori, terenkripsi dan menampilkan pesan Bloody!june 4 th 1989 set elah komputer melakukan booting sebanyak 128 kali.
4) Polyboot.B, AntiEXE

Proteksi : Cara terbaik untuk menghindari virus *boot sector* adalah untuk memastikan *floppy disk* di *write protect*.

File Virus, Virus jenis ini menginfeksi *file* lain ketika program yang telah terinfeksi olehnya dieksekusi. Oleh sebab itu virus jenis ini dapat menyebar melalui jaringan komputer dengan sangat cepat. Virus ini menginfeksi *file-file* yang dapat dieksekusi langsung dari sistem operasi, baik itu file *application* (*.EXE) , maupun *.COM biasanya juga hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran *file* yang diserangnya.

Contoh Virus : The Yerusalem, Cascade

Stealth Virus, Virus ini akan menguasai tabel-tabel *interrupt* pada DOS yang sering kita kenal dengan *Interrupt interceptor*. Virus ini berkemampuan untuk mengendalikan instruksi-instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya baik secara penuh ataupun ukurannya.

Contoh virus:

1) Yankee.XPEH.4928, menginfeksi file *.COM dan *.EXE. Panjangnya: 4298 bytes. Karakteristik: menetap di memori, ukuran tersembunyi, memiliki pemicu.
2) WXYC (termasuk juga dalam kategori *boot record*) , menginfeksi *floppy* dan *Master Boot Record*. Panjang: 520 *bytes*. Menetap di memori, ukuran dan virus tersembunyi.
3) Vmem (s) , menginfeksi file-file *.EXE, *.SYS, dan *.COM Panjang file 3275 bytes. Karakteristik: menetap di memori, ukuran tersembunyi dan dienkripsi.

Multiparte virus, Virus ini merupakan gabungan dari *virus boot sector* dan *virus file*: artinya pekerjaan yang dilakukan mengakibatkan dua hal, yaitu: dapat menginfeksi file-file *.EXE dan juga dapat menginfeksi *boot sector*.

Persembunyian: Pada tahap awal, virus ini cenderung bersembunyi di dalam memori kemudian menginfeksi *hard disk*.

Contoh : Invader, Flip dan Tequila

Proteksi : Bersihkan sektor *boot* dan juga *disk* untuk menyingkirkan virus, dan kemudian kembalikan semua data di dalamnya. Namun, pastikan bahwa data bersih.

Macro virus, Macro adalah perintah yang berisi perintah program otomatis. Saat ini, banyak aplikasi umum yang menggunakan macro. Jika seorang pengguna mengakses sebuah dokumen yang mengandung macro yang telah terinfeksi oleh virus jenis ini dan secara tidak sengaja mengeksekusinya, maka virus ini dapat mengcopy dirinya ke dalam *file startup* dari aplikasi tersebut. Sehingga komputer tersebut menjadi terinfeksi dan sebuah *copy* dari macro virus tersebut akan tinggal di dalamnya.

Dokumen lain di dalam komputer tersebut yang menggunakan aplikasi yang sama akan terinfeksi pula. Dan jika komputer tersebut berada di dalam sebuah jaringan, maka kemungkinan besar virus ini dapat menyebar dengan cepat ke komputer lain yang berada di dalam jaringan tempat komputer tersebut berada. Bahkan jika dokumen yang telah terinfeksi dikirimkan kepada orang lain, misalnya melalui *floppy disk* ataupun *email*, maka virus akan menjangkiti komputer penerima pula. Proses ini akan berakhir hanya apabila jika virus ini telah diketahui dan seluruh macro yang terinfeksi dibasmi. Macro virus merupakan salah satu jenis virus yang paling umum saat ini. Aplikasi seperti Microsoft Word dan Microsoft Excel tergolong sangat rentan terhadap virus jenis ini. Satu hal yang membuat penyebaran virus ini menjadi sangat 'sukses' adalah karena aplikasi jenis ini kini lebih umum dipertukarkan pengguna dibandingkan *file-file* program, dan juga merupakan dampak langsung maraknya penggunaan aplikasi *email* dan *web* dewasa ini.

Persembunyian: Bersembunyi dalam dokumen yang dibagi melalui *e-mail* atau jaringan. Contoh virus:

1). Variant W97M, misalnya W97M.Panther. Panjang 1234 bytes, dan akan menginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka.
2). WM.Twno.A;TW, Panjangnya 41984 bytes, dan akan menginfeksi dokumen Ms. Word yang menggunakan bahasa makro, biasanya berekstensi *.DOT dan *.DOC.

Contoh : Relax, Melissa.A, Bablas, O97M/Y2K

Proteksi : Teknik perlindungan terbaik adalah menghindari membuka *e-mail* dari pengirim yang tidak dikenal. Juga, menonaktifkan macro dapat membantu melindungi data.

Polymorphic Virus, Virus ini dirancang untuk mengalihkan perhatian program *antivirus*, artinya virus ini selalu berusaha agar tidak dikenali oleh *antivirus* dengan cara selalu merubah-ubah strukturnya setiap kali selesai menginfeksi *file* atau program lain.

Contoh virus:

1). Necropolis A/B, menginfeksi file *.EXE dan *.COM. Panjang filenya: 1963 bytes. Karakteristik: menetap di memori, ukuran dan virus tersembunyi, terenkripsi dan dapat berubah-ubah struktur.
2). Nightfall, menginfeksi file *.EXE. Panjang file: 4554 bytes. Karakteristik: menetap di memori, ukuran dan virus tersembunyi, memiliki pemicu, terenkripsi dan dapat berubah-ubah struktur.
3). Elkern, Marburg, Setan Bug, dan Tuareg

Proteksi : Instal antivirus *high-end*.

Metamorphic Virus, menulis ulang dirinya setelah proses penularan selesai. Metode yang digunakan virus ini menggunakan *metamorphic engine*, sehingga berukuran besar dan rumit. Virus ini sulit dideteksi dengan program anti virus.

Contoh : Win95,Zmis,A

Email worm, Sebagian besar penyebab penyebaran virus saat ini adalah a*ttacment email* yang telah terinfeksi. Kemudahan pengguna untuk mendownload *attachment email* tersebut dan mengeksekusinya. Hal ini dikarenakan sering kali isi *email* yang bersangkutan bersifat 'mengundang', misalnya saja untuk kasus *worm ILoveYou* yang menyebar dengan nama file LOVE-LETTER-FOR-YOU.TXT.vbs disertai dengan pesan yang berbunyi: "*kindly check the attached LOVELETTER coming from me*". Selain melalui *email*, *worm* juga dapat menyebar melalui *newsgroup posting*.

Contoh : PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson
Proteksi : Instal antivirus versi terbaru

Trojan atau Trojan Horse adalah kode berbahaya, yang tidak seperti virus, tidak mereproduksi dengan menginfeksi *file* lainnya, juga tidak mereplikasi diri seperti cacing. Program ini menyamar dirinya sebagai program atau aplikasi yang berguna.

Selain itu, ada banyak virus komputer lain yang memiliki potensi untuk menginfeksi data. Oleh karena itu, lindungi komputer kamu dengan menginstal perangkat lunak antivirus yang berkualitas tinggi dan asli. Selain itu jangan mendownload *file* di sebarang situs *download* gratis.

Web Scripting Virus, banyak halaman *web* mengunakan kode yang kompleks dalam rangka menciptakan konten yang menarik dan interaktif. Kode ini sering dimanfaatkan untuk tindakan yang tidak diinginkan.

Persembunyian: Sumber utama *scripting virus web browser* atau halaman *web* yang terinfeksi.

Contoh : JS.Fortnight adalah virus berbahaya yang menyebar melalui e-mail.
Proteksi : Instal aplikasi microsoft tool yang merupakan fitur standar pada Windows 2000, Windows 7 dan Vista. Scan komputer dengan aplikasi ini.

FAT Virus, *File allocation table* (FAT) adalah bagian dari *disk* yang digunakan untuk menyimpan semua informasi mengenai lokasi *file*, ruang yang tersedia, ruang tidak dapat digunakan, dll.

Persembunyian: virus FAT menyerang bagian FAT dan dapat merusak informasi penting. Hal ini bisa sangat berbahaya karena mencegah akses ke bagian tertentu dari disk dimana file penting disimpan. Kerusakan yang disebabkan dapat mengakibatkan hilangnya informasi dari *file* individual atau bahkan seluruh direktori.

Contoh : link Virus

Companion Viruses Persembunyian: umumnya menggunakan nama *file* yang sama dan membuat ekstensi yang berbeda. Sebagai contoh: Jika ada file "Me.exe", virus membuat file lain bernama "Me.com" dan bersembunyi di file baru. Ketika sistem memanggil nama *file*

"*Me*", yang ". Com" file dijalankan (sebagai ". Com" memiliki prioritas lebih tinggi daripada "exe."), Sehingga menginfeksi sistem.

Contoh : Stator, Asimov.1539 dan Terrax.1069

Directory Virus, Direktori virus (juga disebut *Cluster Virus* / *File System Virus*) menginfeksi direktori komputer dengan mengubah jalan yang menunjukkan lokasi *file*. Ketika menjalankan program *file* dengan ekstensi EXE. Atau COM. Yang telah terinfeksi oleh virus, Anda tidak sadar menjalankan program virus, sedangkan *file* asli dan program sebelumnya dipindahkan oleh virus. Setelah terinfeksi, menjadi mustahil untuk menemukan *file* asli.

Persembunyian: Virus ini biasanya terletak dalam satu lokasi *disk*, tetapi menginfeksi seluruh program dalam direktori.

Contoh : virus Dir-2

Memory Resident Virus, Virus ini menetapkan dalam memori komputer dan otomatis aktif setiap kali OS berjalan dan menginfeksi semua *file* yang dibuka.

Persembunyian: Jenis virus ini bersembunyi dalam RAM dan tinggal di sana bahkan setelah kode berbahaya dijalankan. Virus mendapat kontrol atas memori sistem dan mengalokasikan blok memori di mana ia menjalankan kode sendiri, dan mengeksekusi kode ketika fungsi apapun dijalankan.

Target : Dapat merusak *file* dan program yang dibuka, ditutup, disalin, diubah namanya, dll.

Contoh : Randex, CMJ, Meve, dan MrKlunky.

Proteksi : Instal program antivirus

Direct Action Viruses, Tujuan utama virus ini adalah untuk meniru dan bertindak ketika dijalankan. Ketika kondisi tertentu terpenuhi, virus akan beraksi dan menginfeksi *file* dalam direktori atau *folder* yang ditentukan dalam *path* file AUTOEXEC.BAT. *File batch* ini selalu terletak di direktori *root hard disk* dan melakukan operasi tertentu ketika komputer *boot*.

Teknik *FindFirs*t / *FindNext* digunakan di mana kode memilih beberapa *file* sebagai korbannya. Hal ini juga menginfeksi perangkat eksternal seperti *pen drive* atau *hard disk*.

Persembunyian: Virus terus berpindah lokasi ke *file* baru setiap kali kode dijalankan, tapi umumnya ditemukan di direktori *root* pada *hard disk.*

Target : Virus ini dapat merusak file. Pada dasarnya, ini adalah *file virus-infector*.

Contoh : Vienna virus

Proteksi : Instal *scanner* antivirus.

Overwrite Viruses,Virus jenis ini menghapus informasi dalam *file* yang terinfeksi.

Persembunyian: Virus menggantikan isi *file*. Namun, tidak mengubah ukuran file.

Contoh : Way, Trj.Reboot, Trivial.88.D

Proteksi : Satu-satunya cara untuk membersihkan *file* yang terinfeksi oleh virus *Overwrite* adalah dengan menghapus *file* yang terinfeksi.

3. Pembahasan

a. **Cara Penyebaran Virus**

1). Disket, Media Storage (R/W), media ini merupakan media yang mudah di tumpangi untuk penyebaran virus.

2). Jaringan (LAN dll), karena saling terhubung satu dengan lainnya maka virus berpindah saat pertukaran data.

3). www/Internet, sangat dimungkinkan menularkan virus karerna web tersebut ditanam *virus*.

4). *Software* Gratis, *Shareware* Asli maupun bajakan, banyak sekali didalamnya ditanamkan virus.

5). *Attachment File* dan *Transfer File*, biasanya di kirim bareng dengan *email* dengan gambar yang menonjol.

b. **Gejala Yang Mungkin Terjadi Komputer Terinfeksi Virus**

1). Windows tidak berjalan walaupun anda tidak membuat perubahan pada yang sudah terinstalasi sebelumnya..
2). Windows tidak berjalan karena berkas sistem penting tertentu hilang. Selain lagi, muncul pesan kesalahan yang mendaftar berkas-berkas yang hilang.
3). Komputer terkadang memulai sesuai yang diharapkan. Namun, terkadang komputer berhenti merespons sebelum ikon *desktop* dan *taskbar* muncul.
4). Komputer berjalan sangat lambat. Lagi pula, komputer memerlukan waktu yang lebih lama daripada yang diharapkan untuk memulai ulang.
5). Anda menerima pesan tentang memori tidak cukup walaupun komputer memiliki RAM yang cukup.
6). Program baru diinstal secara tidak benar.
7). Windows secara spontan memulai ulang dengan tiba-tiba.
8). Program yang digunakan untuk menjalankan Windows seringkali berhenti merespons. Bahkan ketika Anda menghapus dan menginstal kembali program, permasalahan mulai muncul.
9). Komputer selalu berhenti merespons saat Anda mencoba untuk menggunakan produk Microsoft Office.
10). Perangkat lunak *antivirus* menunjukkan adanya *virus* komputer.

c. **Pencegahan Terkena Virus Komputer.**

1). Gunakan perangkat anti virus
2). Lakukan Scan keseluruhan komputer secara rutin.
3). Lakukan *Update Data* Anti Virus secara teratur minimal satu minggu sekali.
4). Lakukan *backup* secara teratur terhadap *file* penting anda.
5). Lakukan *scanning* terhadap *file-file* yang disapat dari luar baik dari *flash memory*, CD maupun hasil *download* sebelum digunakan.
6). Jangan membuka *file attachmen* ang berektensi vbs atupun js, karena banyak virus yang ditempelkan di *file* tersebut.
7). Lakukan *disable* pada *autoplay* untuk *autorun* usb, kalau windows dari gpedit.msc.

d. **Langkah-langkah Apabila Telah Terinfeksi**

1). Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut, jika anda terhubung ke jaringan maka sebaiknya anda mengisolasi komputer anda terlebih dahulu (bisa dengan melepas kabel atau men*disable* dari *control panel*).
2). Identifikasi dan klasifikasikan jenis *virus* apa yang menyerang PC anda, dengan cara: Gejala yang timbul, misal: pesan, *file* yang *corrupt* atau hilang, dsb.
3). Scan dengan antivirus anda, jika anda terkena saat *Autoprotect* berjalan berarti *virus definition* di komputer anda tidak memiliki data *virus* ini, Cobalah *update* secara manual atau mendownload virus definitionnya untuk anda *install*. Jika virus tersebut memblok usaha anda untuk mengupdatenya maka, upayakan untuk menggunakan media lain (komputer) dengan *antivirus update*-an terbaru.

4. Kesimpulan

Dengan kemunculan berbagai jenis virus dengan perilaku yang berbeda serta menghasilkan dampak yang berbeda pula sangat merepotkan dan mengganggu hampir semua pengguna komputer. Karena habis terkena virus yang belum terdeteksi, kemudian dilakukan instalasi ulang terhadap sistemnya, tidak berapa lama terkena lagi. Hal tersebut membuat kita kehilangan waktu dan merasa tidak nyaman dan tidak aman terhadap kehilangan data akibat virus. Untuk itu perlu kita menyiapkan perangkat lunak anti virus yang baik dan handal serta selalu melakukan *update database virus* agar dapat mendeteksi dengan baik dan sempurna.

Daftar Pustaka

Chen, Tom (2003). Trends in Viruses and Worms. SMU Engineering.
Cohen, Fred (1984). Computer Viruses – Theory and Experiments

https://www.inews.id/techno/internet/sejarah-virus-komputer-di-dunia-dari-masa-ke-masa diakses 28/5/2023)

Li, Xin (2003). Computer Viruses: The Threat Today and The Expected Future. Linkoping Institue of Technology

Ludwig, Mark (1990). The Little Black Book of Computer Viruses – Electronic Edition. American Eagle Publications, Inc.

Suliyanto, Feri (2010), 101 Masalah Malware Dan Penanganannya, Penerbit Andi, Yogyakartaa

Yudanto,Yudha, Sulistyo Yunus, Dedi Gunawan (2010), Panduan Pintar Komputer, Indonesia Tera, Yogyakarta