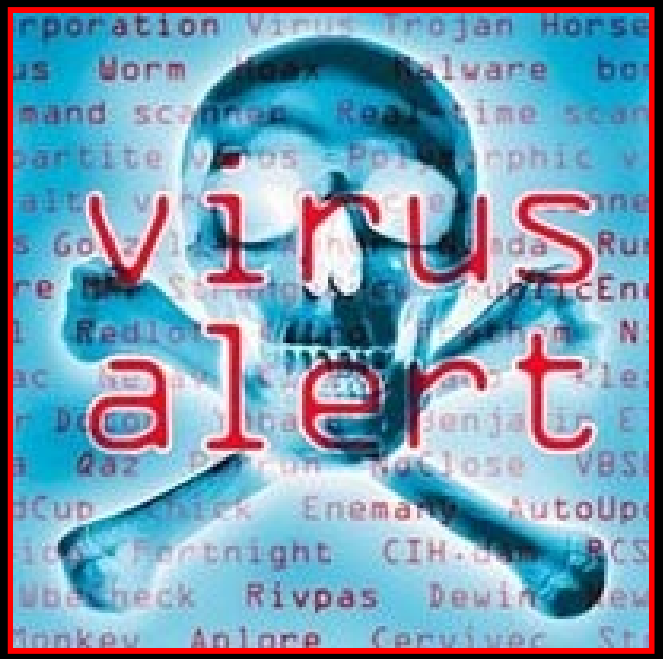
ICT TALK - Siri 9/2011
6 September 2011



Jenis-jenis Virus Komputer dan Implikasinya kepada Pengguna PC

TOPIK

1. Definisi
2. Jenis-jenis virus dan ciri-cirinya
3. Tanda-tanda/*Symptom* jangkitan virus
4. Cara untuk mengesan serangan virus
5. Nama virus dan cara serangannya

TOPIK

6. Tindakan bila menerima emel yang dijangkiti virus
7. Memilih perisian antivirus
8. Mengawal PC daripada dijangkiti virus
9. Kenapa orang mencipta virus ?

DEFINISI

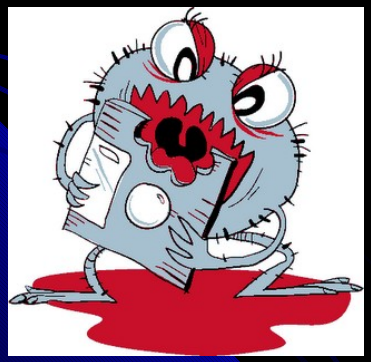
- Merupakan sebuah atur cara berparasit yang ditulis dengan tujuan untuk memasuki komputer tanpa pengetahuan atau kebenaran penggunanya.
- Virus akan bercantum kepada fail atau sektor *boot* dan menggandakan dirinya (replikasi) untuk merebakkan jangkitannya.
- Sebuah perisian aturcara yang bercantum dengan aturcara lain dalam memori komputer atau cakera, dan merebak daripada satu aturcara kepada aturcara yang lain.

JENIS-JENIS VIRUS

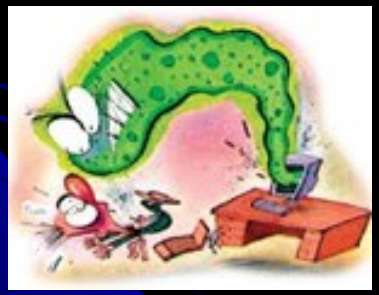
Virus pertama ditemui pada tahun 1986. Terdapat 7 jenis virus :

1. BOOT SECTOR
2. PARTITION TABLE
3. FILE VIRUS
4. MULTIPARTITE VIRUS
5. MACRO VIRUS
6. TROJAN HORSE
7. WORMS

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI
BOOT SECTOR 	Mendiami sebahagian daripada bahagian cakera keras atau disket pada bahagian rekod *boot* utama. Ia akan mendiamkan dirinya sehingga ia dihidupkan oleh aturcara tersebut.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI
PARTITION TABLE 	Ia menyerang *partition table* cakera keras (ruang simpan maklumat cakera keras) dengan menggerakkan ia ke sektor yang baru dan menggantikan sektor yang ada dengan kod yang dijangkiti virus. Virus akan disebarkan daripada *partition table* ke *boot sector* disket jika disket digunakan.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI
FILE VIRUS	Biasa didapati pada fail-fail. Ia akan mencantumkan dirinya kepada fail '.exe' dan akan menghalang fail itu daripada berfungsi. Ia juga mampu mengubahsuai dan merosakkan fail itu bagi memudahkan ia disebarkan sebelum ia dikesan.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI (CHARACTER)
MULTIPARTITE VIRUS	Ia bercantum kepada fail dan mengubahsuai rekod *boot* cakera keras. Jarang didapati tetapi mampu melakukan tindakan yang boleh membinasakan PC.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI
MACRO VIRUS	Muncul pada Julai 1995 dalam MS WORD. Semua fail yang menggunakan aplikasi *Word, Excel* dan aplikasi lain yang menggunakan fungsi makro. Ia boleh menghasilkan jaringan arahan di dalam sebuah fail yang menjalankan arahan setiap kali sesuatu kombinasi kekunci itu ditekan.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI (CHARACTER)
TROJAN HORSE	Sering dimuatkan dalam program yang baru kerana ia kerap digunakan oleh pengguna. Apabila ia dihidupkan, ia akan memaparkan mesej, menukar data atau memusnahkan banyak fail.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI (CHARACTER)
WORMS 	Ia mereplikasikan dirinya dengan cepat. Setiap kali ia mengeluarkan salinan, setiap kali itulah *worm* dihasilkan dalam masa yang singkat dan memakan ruang cakera keras. Ia merebak menerusi rangkaian atau emel dan memenuhi ruang storan rangkaian atau simpanan emel.

JENIS-JENIS VIRUS DAN CIRI-CIRINYA

JENIS VIRUS	CIRI-CIRI (CHARACTER)
TIME BOMB 	Ia tidak mereplikasikan dirinya, sebaliknya ia bertindak mengikut tarikh tertentu. Dilakukan oleh pengaturcara yang tidak berpuas hati dengan majikannya atau untuk tujuan pemusnahan. **Time Bomb** akan dimasukkan ke dalam komputer dan apabila tiba pada tarikh tertentu (biasanya pada tarikh ini, pengaturcara tersebut sudah berhenti dari syarikat itu), ia akan memadam kesemua fail di dalam komputer tersebut.

TANDA/*SYMPTOM* JANGKITAN VIRUS

1. Perubahan dalam saiz fail.
2. Perubahan pada tarikh fail walaupun fail itu tidak diubahsuai.
3. Program mengambil masa yang lama daripada biasa untuk dijalankan.
4. Operasi sistem (Windows) yang perlahan.

TANDA/*SYMPTOM* JANGKITAN VIRUS

5. Pengurangan ruang cakera keras dan memori secara mendadak dan tidak dapat dikesan puncanya.
6. Sektor rosak pada disket/storan yang lain.
7. Paparan mesej kerosakan yang ganjil.
8. Aktiviti skrin yang ganjil.

TANDA/*SYMPTOM* JANGKITAN VIRUS

9. Aturcara/Perisian tidak dapat dijalankan.
10. Sistem *boot* gagal semasa sistem bermula atau semasa mem*boot* daripada pemacu.
11. Terdapat aktiviti pencapaian cakera keras walaupun tiada aktiviti sedang berjalan.
12. Perkakasan seperti *monitor*, papan kekunci dan tetikus dirosakkan dengan mengganggu ROM.

CARA UNTUK MENGESAN SERANGAN VIRUS

1. Berhati-hati dengan *pen drive* dan fail yang anda terima daripada orang lain.
2. Elakkan mengguna semula *pen drive* yang telah digunakan di komputer lain.

CARA UNTUK MENGESAN SERANGAN VIRUS

3. Jangan muat turun fail dari laman web yang tidak selamat dan jangan buka *attachment* emel sebelum anda memeriksanya terlebih dahulu. Berhati-hati terhadap mesej dan lampirannya (walaupun dihantar oleh orang yang anda kenali), dengan tajuk kandungan yang meragukan, contohnya, *"Check this out !!!"* atau *"See these pictures !!!"*

CARA UNTUK MENGESAN SERANGAN VIRUS

4. Dapatkan program antivirus untuk lebih selamat berkongsi *pen drive*, memindahturun fail dari Internet dan membuka lampiran emel.
5. Jika sistem anda dijangkiti virus, lawatilah laman web pengeluar perisian pengimbas-virus dan pasang/*install* mana-mana pengesan virus baru yang ada. Perisian ini mungkin tidak dapat menghapuskan virus, tetapi sekurang-kurangnya ia dapat mengenalpasti virus.

CARA UNTUK MENGESAN SERANGAN VIRUS

6. Cari maklumat di Internet berkenaan virus yang telah anda kenalpasti tadi dengan menaip nama virus atau fail yang berkaitan pada ruangan di enjin pencari, diikuti dengan perkataan "virus". Contohnya, "Melissa virus", "BubbleBoy virus" dan sebagainya.

CARA UNTUK MENGESAN SERANGAN VIRUS

7. Pindah turun dan pasang mana-mana perisian pembetulan sementara (patches) atau program-program yang boleh membantu anda menghapuskan virus tersebut, atau ikut mana-mana arahan yang anda temui bagi memadam virus secara manual.
8. Jalankan pengimbas virus lain untuk memastikan virus berkenaan telah "diuruskan" sebagaimana sepatutnya.

CARA UNTUK MENGESAN SERANGAN VIRUS

9. Ambil langkah berjaga-jaga apabila anda menerima kepilan/*attachment* yang biasanya diakhiri dengan .doc, .exe, .com, .xls atau .ppt. Jangan sekali-kali membuka kepilan yang berakhir dengan .vbs atau .js – tiada sebab untuk anda membuka fail-fail ini.

CARA UNTUK MENGESAN SERANGAN VIRUS

10. Selain itu kepilan "anniv.com" telah dikenalpasti menyebarkan virus Melissa, **JANGAN** buka, segera **HAPUSKAN**nya. Jika kepilan atau mana-mana dokumen yang dijangkiti dibuka, ia akan menghantar salinan dirinya sendiri kepada senarai 50 alamat pertama yang tersenarai dalam buku alamat Microsoft Outlook - "mangsa".

NAMA VIRUS DAN CARA SERANGANNYA

NAMA VIRUS	CARA SERANGAN
Worm. ExploreZip	Virus ini dipindahkan dengan menggunakan fail .zip yang dihantar menerusi emel. Ia akan memadamkan fail-fail dokumen perisian-perisian Word, Excel, dan Powerpoint.

NAMA VIRUS DAN CARA SERANGANNYA

NAMA VIRUS	CARA SERANGAN
CIH	Dicipta oleh seorang pelajar Taiwan bernama Chen Ing-Hau berusia 24 tahun. Virus akan memadamkan semua fail dalam cakera keras dan merosakkan komputer.

NAMA VIRUS DAN CARA SERANGANNYA

NAMA VIRUS	CARA SERANGAN
MELISSA	Disebarkan menerusi sebuah fail 'list.doc' yang mengandungi senarai laman web lucah. Jika fail itu dibuka, secara automatik komputer itu akan dijangkiti.

NAMA VIRUS DAN CARA SERANGANNYA

NAMA VIRUS	CARA SERANGAN
BACK DOOR-G	Aturcara yang dihantar melalui Internet menerusi emel dan dipindahkan dalam format *screensaver*. Jika program ini dijalankan, maka komputer itu boleh dicapai dan dicerobohi oleh pengguna yang tidak dibenarkan.

NAMA VIRUS DAN CARA SERANGANNYA

NAMA VIRUS	CARA SERANGAN
PRETTY PARK	Disebarkan menerusi emel di mana virus akan mencuri maklumat seperti nombor telefon, kata laluan dan maklumat penting yang lain mengenai komputer pengguna itu dan dihantarkan kepada sebuah tapak *chatting* Internet.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
BRAIN (1986)	Virus ini tidak terlalu merosakkan komputer. Setelah munculnya virus ini, ia menjadi perangsang kepada 100,000 pencipta virus bagi abad seterusnya.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
MICHAEL ANGELO (1991)	Virus ini merupakan virus MS-DOS yang paling teruk sekali kerana ia menyerang apa saja yang masuk ke komputer seperti disket dan *pendrive*. Setelah menyebarkan virus selama berbulan – bulan secara senyap, virus ini diaktifkan dan merosakkan data-data yang tersimpan di dalam komputer.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
MELISSA (1999)	Virus Melissa diambil bersempena nama seorang penari bogel. Virus ini akan disebarkan melalui emel dan dihantar kepada beribu-ribu orang. Pencipta virus ini telah dikenakan penjara selama 20 bulan.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
ILOVEYOU (2000)	Virus pertama yang menggunakan tipu helah untuk menyuruh anda membuka sesuatu fail yang telah dijangkiti virus. Fail tersebut dibuat dalam skrip VBS kononnya merupakan surat cinta dan anda diminta anda membacanya.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
CODE RED (2001)	Virus ini menyerang melalui *server web* dan merosakkan laman web melalui serangan ke atas satu hos IP.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
NIMDA (2001)	Virus ini dibuat berdasarkan virus *Code Red* dan melancarkan serangan melalui laman web, emel dan sambungan Internet seperti *Yahoo Messenger* dan sebagainya.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
KLEZ (2001)	Virus ini akan menghantar maklumat melalui emel dan mendakwa Bill Gates hendak memberi wang percuma kepada pembaca emel tersebut. Pembaca yang teruja akan klik dan virus tersebut secara automatiknya akan tersebar.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
SLAMMER (2003)	Virus yang amat pantas sekali tersebar. Ini kerana ia boleh menjangkiti kira – kira 75,000 PC dalam masa 1 minit. Kesannya ialah ia akan melembabkan Internet dan merosakkan laman web.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
MYDOOM (2004)	Virus ini merupakan yang paling cepat sekali dalam sejarah disebarkan melalui emel. Ia akan berterusan menghantar emel ke komputer anda dalam dalam kuantiti yang banyak.

10 VIRUS PALING MERBAHAYA

NAMA VIRUS	KESAN VIRUS
STORM (2007)	Virus ini disebarkan melalui emel *spam* dan telah menjangkiti lebih 10 juta buah komputer.

TINDAKAN BILA MENERIMA EMEL YANG DIJANGKITI VIRUS

1. Catat alamat emel orang yang menghantar emel tersebut.
2. Padam/buang emel tersebut dan fail kepilannya (attachment).
3. Jalankan/*Run* pengimbas virus di komputer anda.
4. Hantar emel kepada orang yang menghantar virus, beri peringatan bahawa komputernya telah dijangkiti virus.

MEMILIH PERISIAN ANTI VIRUS

1. Beli salah satu daripada program anti virus yang utama, seperti *Symantec's, Norton Anti-Virus, McAfee VirusScan, Quarterdeck ViruSweep atau Dr. Solomon's Anti-Virus*. Pengeluar-pengeluar utama ini boleh diharapkan untuk mengeluarkan program kemaskini yang bersesuaian dengan virus terbaru, mengikut jangka masa tertentu yang telah ditetapkan.

MEMILIH PERISIAN ANTI VIRUS

2. Lihat ulasan dan *rating* yang telah dibuat di Internet dan dalam majalah-majalah komputer bagi memudahkan anda memilih mengikut keperluan dan keupayaan komputer anda sebelum membuat keputusan untuk membelinya.

MEMILIH PERISIAN ANTI VIRUS

3. Muat turun perisian kongsi (shareware) program anti-virus, jika anda tidak mampu mendapatkan program anti-virus secara komersil.
4. Belanjakan tidak lebih daripada RM200 untuk mendapatkan perisian anti-virus komersil.

MEMILIH PERISIAN ANTI VIRUS

5. Buat penilaian terhadap terma-terma menaik taraf (upgrade) perisian anda sebelum membelinya. Kebanyakan pengeluar menawarkan pakej naik taraf secara percuma yang boleh mengesan virus yang baru dicipta.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Hargai dan Hormati Hakcipta**
  Hindari daripada menggunakan perisian tiruan dalam apa juga keadaan.
- **Pasang Perisian Anti-Virus**
  Pasang perisian anti-virus untuk melindungi PC anda dan pastikan fail tandatangan (signature) yang terkini telah dimasukkan. Anda perlu kemaskini tandatangan virus sekurang-kurangnya sekali dalam setiap hari bekerja.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Kerap Membuat Salinan/ *Backup***

  Selalulah membuat salinan data anda. Membaikpulih menggunakan salinan adalah langkah yang paling selamat bagi mendapatkan kembali fail selepas diserang virus.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Imbas Virus Secara Harian (setiap hari)**
  Jadualkan untuk membuat imbasan setiap hari bagi mengesan virus. Jadual imbasan boleh dilakukan pada waktu bukan puncak, seperti sewaktu rehat tengah hari atau selepas tengah malam.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Periksa Kepilan Email**

  Berwaspada terhadap virus yang datang sebagai kepilan emel daripada punca yang tidak dapat dikenalpasti. Ada virus ulat (worm) yang boleh menyamar sebagai ucapan selamat atau perayaan. Jangan buka sebarang kepilan sehingga anda benar-benar pasti apa isi kandungannya.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Periksa Fail Yang Dimuat turun**

  Periksa *pen drive* dan fail yang dimuat turun dari Internet (terutama dari punca yang tidak diketahui) menggunakan perisian anti-virus sebelum menggunakannya.

MENGAWAL PC DARI DIJANGKITI VIRUS

- **Hentikan Semua Aktiviti Komputer Yang Telah Dijangkiti**

  Jika komputer anda telah dijangkiti oleh virus komputer, semua aktiviti menggunakan komputer tersebut mesti dihentikan – mulakan proses penghapusan virus. Meneruskan penggunaannya akan membantu virus merebak dengan lebih giat.

KENAPA ORANG MENCIPTA VIRUS ?

1. Sebagai projek penyelidikan, usikan serta untuk menyerang produk syarikat-syarikat tertentu, menyebarkan pesanan politik dan memperolehi keuntungan daripada pencurian identiti.

KENAPA ORANG MENCIPTA VIRUS ?

2. Sesetengah penulis virus menganggap ciptaan mereka sebagai seni dan melihat penulisan atur cara virus sebagai suatu hobi yang kreatif.
3. Banyak penulis virus juga menganggap sistem-sistem yang diserang oleh mereka sebagai suatu cabaran intelektual atau satu masalah logik untuk diselesaikan.

SUMBER RUJUKAN

- http://google.com/
- http://ms.wikipedia.org/
- http://www.pesima.net/
- http://myblog.1adscenter.net/bagaimana-hendak-mengesan-virus/
- http://bizniz87.wordpress.com/virus-komputer/
- http://berita-harian-online.com/10-virus-komputer-paling-merbahaya/