

CHÖÔNG V



BAÛO VEÄ DÖÖ LIEÄU

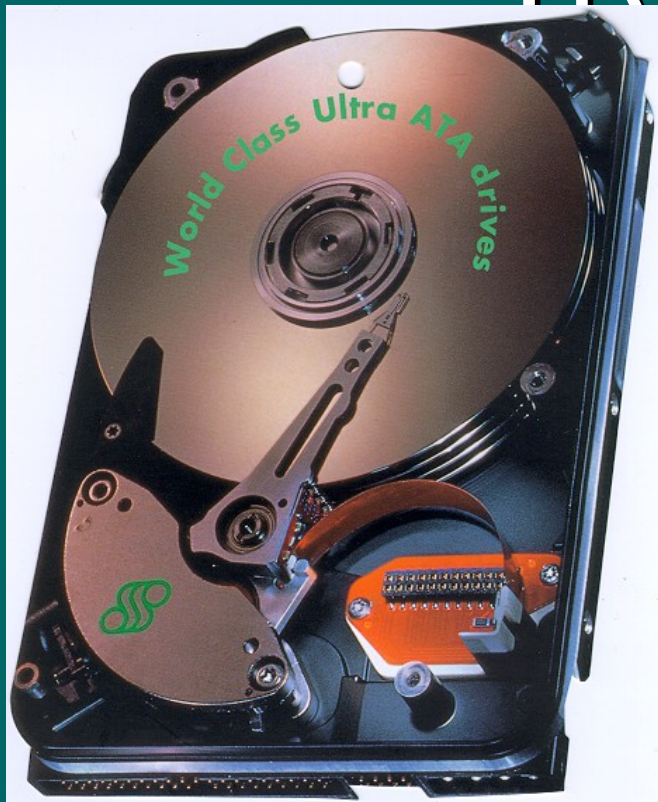




MỞ ĐẦU

DỔ LIỆU CỦA NGƯỜI DƯƠNG LAO TẠO

NGUYỄN QUỲ NHẬT TRONG MÀU



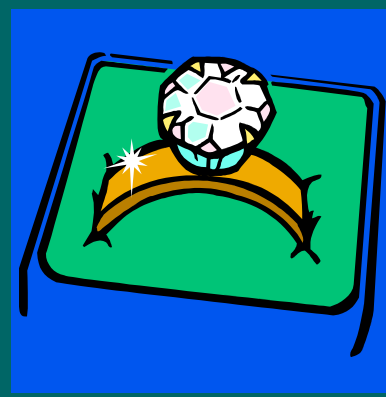
- CAÙC FILE VAÊN BAÙN
.DOC
- CAÙC FILE BAÙNG TÍNH
.XLS
- CAÙC FILE DỔ LIỆU
.DBF
- CAÙC FILE CHÖÔNG TRÌNH



- Phaàn meàm maùy tính laø linh hoàn cuûa maùy, laø taøi nguyêân quyù giaù. Trong maùy, caùc phaàn meàm heä thoáng, phaàn meàm công cuï laø taøi saün ñaét giaù. Ñaéc bieät, nhöõng chöông trình vaø döõ lieäu quan troïng maø ngöôøi söû duïng maùy taïo ra laø taøi saün quyù nhaát, raát caàn ñöôïc baôu veä, vì noù laø taøi saün rieâng cuûa ngöôøi duøng maùy, khoâng theå mua ñöôïc. 4



Data = Golden + Diamon

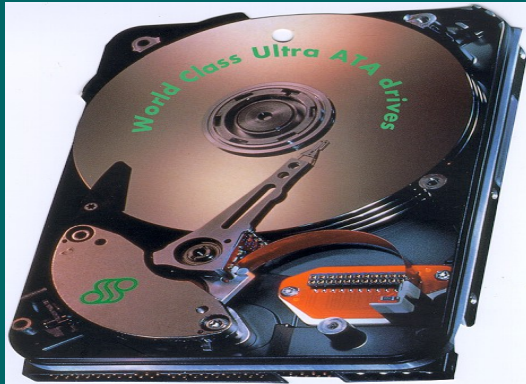


CAÙC NGUYEÂN NHAÂN LAØM MAÁT DÖÖ LIỆÄU

VIRUS

HARD DISK

HACKER



5.1 BẢO VỆ Ổ ĐĨA



BẢO VỆ Ổ ĐĨA

- Nón cùng hiện nay chất lượng rất tốt, giá rẻ, dung lượng rất lớn, rất tiện với chức GB. Hầu hết công trình và đồ liệu nên lưu trữ trên nón cùng.
- Tuổi thọ trung bình của ổ cùng vào khoảng 10.000 giờ sử dụng.
- Do nên kiện và yù thối của ổ ngoài sử dụng, thời gian hoạt động của ổ cùng có thể tăng lên hay giảm đi, có thể trực tiếp, hoặc hỏng bất ngờ.
- Nếu máy tính bỏ ổ cùng thì không phải chæ mất các tệp tin do ổ ngoài sử dụng tạo ra mà là mất tất cả.

BẢO VỆ Ổ ĐĨA

- Nắm bắt nhiều kiến thức đúng nhất : có bản gốc, bỏ lỗi nhiều
- Không để rơi bắt máy tính từ thời
- Tránh hình dạng nóng cùng nhiều lần
- Chú ý tuổi thọ của ổ đĩa cùng. Nếu sử dụng liên tục

5.2 VIRUS TIN HOÏC



REUTERS

CÁC KHÁI NIỆM CƠ BẢN


Thuật ngữ Virus tin học dùng để chỉ các chương trình máy tính do con người tạo ra.

Các chương trình này thường ngắn, tinh vi và có khả năng bám vào các file khác nhờ một vật thể ký sinh.

Chúng có khả năng tự nhân bản, tự sao chép chính nó lên



- Nói tổng quát công cụ chúng ta cần nhớ cùng với nhớ màm chừa dõ lỗi, làm cho các file kiểu .COM, .EXE chạy sai hoặc không chạy; hãy nhớ các file khác trên nhớ.
- Do cách thức hoạt động của chúng giống virus sinh học nên người ta đặt cho chúng cái tên "Virus"

- 
- Döia vaø cauc phöông tieän giao tieáp maùy tính nhö ñóa, maïng, nhaát laø Internet chuùng lan truyeàn vaø coù maët khaép nôï trên theá giöùì vöùì soá lööïng ñoàng khoàng keã xieát. Coù theã noùì raèng nôï naøo coù maùy tính, nôï ñoù coù virus tin hoïc, taàm hoait ñoäng cuûa virus tin hoïc laø phoã bieán voã cuøng.
 - Moãi Virus coù moät teân, nhö

LÝ DO TẠO VIRUS

- Khôùï ñààu laø ñeã vui ñuøa, nghòch ngôim, ñeã chöông toù taøi naêng tin hoïc, ñeã ñöôïc ngöôøi khaùc chuù yù hay ñeã theã hieän moät yù töôùng haùo thaéng, noãi loaïn, baát maõn.
- Keá ñeán, taïo ra Virus ñeã baùn chöông trình trò Virus.
- Duøng Virus ñeã phaù hoaï ñoái thuû caïnh tranh, baùo veã baùn quyeàn phaàn meàm, choáng laïi caùc haønh ñoäng sao cheùp troãm
- Ngaøy nay vöùï söï phaùt trieån mau leï

ĐẶC TÍNH CỦA VIRUS

- Tội nhân lên tốc độ nhanh
- Chiếm dụng tài nguyên của máy, làm chậm hệ thống
- Tồn tồn làm hỏng dữ liệu cùng
- Bí mật mang các file hệ thống và thông tin để mật khẩu máy
- Chương trình Virus gọn, nhẹ, chạy nhanh, tinh vi và hiệu quả

TÁC HẠI CỦA VIRUS

- Cài máy Virus taán công tröïc tiếp laø döõ lieäu trên máy. Song trên Internet thì Virus taán công vào các WebSite, làm tê liệt hoạt ñöäng, ñăc biệt là các hoạt ñöäng kinh tế, thông mại ñiễn tộu, thông tin liên lạc, các kho döõ lieäu,...

- Nhiều Virus khi lây vào máy có khả năng tội ñöäng gôu ñi các file và ñi vào trong máy và

TÁC HẠI CỦA VIRUS

- Năm 2001, Virus Love Bug làm thiệt hại khoảng 9 tỷ USD. Virus Code Red tấn công ngoạn mục chi phí 2 tỷ USD, chưa khác phục xong thì Virus Nimda lại gây một cơn bão mới và cứ liên tục như thế.

- Tác hại của Virus ngày một lớn, ngày một trầm trọng, nhất là trong thời đại Thông tin.

- Thế giới này có nhiều cách

DẤU HIỆU BỊ VIRUS

- Ngoaøi vieäc phaù hoaïi thöïc söi, caùc virus coøn aãn naùu trong maùy chôø thôøi cô, khoâng phaûi luïc naøo cuõng deã daøng phaùt hieän maùy tính ñang bò nhieãm virus

- Trieäu chöùng roõ reät nhaát laø maùy tính laøm vieäc baát bình thöôøng, chaäm laïi; ñó cöùng bò maát döõ lieäu hoaëc khoâng

DẤU HIỆU BỊ VIRUS

- Còn khi gặp những hiện tượng lạ như bọ nhím không tua theo số liệu khiến hoặc thậm chí thoát ra những dòng chữ vô nghĩa, những nhóm màu nhầy nhụa trên màn hình hoặc khi loa của máy lại nhai những tiếng nhai vô nghĩa

- Trạm trong hơn, toàn bộ đã đổ



- Kích thước của các tập tin nhiễm F-Virus bao giờ cũng lớn hơn kích thước ban đầu. Đây chính là dấu hiệu đặc trưng của khuẩn thể nhân dạng sợi toàn thể của F-Virus trên file thí nghiệm

CÁCH LÂY LAN

- Trước đây, Virus lây lan chủ yếu qua sao chép các đĩa mềm từ máy này sang máy khác.
- Ngày nay, ngoài đĩa mềm, Virus còn lây lan rất nhanh thông qua các dịch vụ Internet nhờ những tiện ích E-Mail, World Wide Web, Download File,...

CÁCH LÂY LAN

- Cách thức lây lan ngày càng tinh vi, phức tạp. Virus hoạt động càng có tính tối ưu càng cao.
- Nhiều Virus có khả năng chèn thêm mã độc vào sau đó gửi chính nó tới tất cả các máy chủ e-mail mà nó tìm thấy trên máy này.
- Nhiều Virus còn có khả năng tìm và gửi đi những file văn bản có trên máy mà nó lây nhiễm.

PHÂN LOẠI VIRUS

Dựa vào cách lây lan, tái chia virus thành 3 nhóm chính:

- ***B-virus*** (Boot virus)
- ***F-virus*** (File virus)
- ***Macro-virus***




B-virus (Boot virus)

- B-Virus taán công vào Master Boot, Boot Sector của ổ đĩa, bảng FAT (File Allocation Table), bảng Thở mục (Root directory)
- B-Virus chæ còu theỏ ñöôic kích hoạt khi khôi ñoäng máy tính bằng ổ đĩa nhieãm. Lúc naøy heã thoáng chõa ñöôic moăt heã ñieàu haønh naøo kieãm soaùt. Nhõ ñaëc ñieãm naøy maø noù còu khaù naêng laây trên



F-virus (File virus)

- F-virus gắn liền vào file .COM và .EXE một lần mỗi lần file này thực hiện, mỗi lần sẽ tiếp kích hoạt, thông thường trong vòng một, khoảng thời gian truy xuất file, tìm kiếm file thì hành sách khác nữa thì gắn liền vào.
- F-virus dễ dàng tiếp kích hoạt do ta cần truy xuất các file .COM, .EXE của hệ thống rất cao. ²⁵ Tiếp



➤ F-virus có thể lây vào vòng nhòu, tạo xung ãoạt về tính nhất quãn của vòng nhòu, khai thác vòng nhòu một cách không thích hõip, làm rối loạn các trìn ãiều khiến thiết bò hiện haønh...

➤ F-virus có thể phá hoại dữ liệu bằng cách dùng những chõu nâng về file ãể thay ãoại ãoại dung các tập tin vền bản,

Macro Virus

- Virus choin ngoan ngoo macro cua Microsoft Word lam phong tien lay lan tren moi troong Winword. Toø vaen baun nhieãm, Macro Virus seõ ñooc ñoa vaø NORMAL.DOT, roai toø ñây chuùng toi cheøn vaø cauc vaen baun saich khac
- Daing thòu hai cua Macro Virus laø lay vaø baung tinh cua Microsoft Excel
- Macro Virus chæ phaù hoai döõ lieäu

9 HƯỚNG DẪN VỀ ĐỀ PHÒNG VIRUS



1. HÃN CHEÁ DUØNG CHUNG MAÙY
2. DUØNG PHAÀN MEÀM COÙ BAÛN QUYỀÀN
3. KIEẢM TRA ÑÓA LAÏ TRÖÖÙC KHI SÖÙ DUÏNG
4. THÖÖØNG XUYỀÂN DUØNG CAÙC CHÖÖØNG TRÌNH PHAÙT HIEẢN-PHOØNG-DIEÄT VIRUS MÔÙI NHAÁT

5-THẬN TRỌNG KHI NHẬN E-MAIL
HOẶC DOWNLOAD FILE

6-THƯỜNG XUYÊÂN SAO LÖU
CAÙC DÖÖ LIÊÄU QUAN TRÖÖNG
RA CAÙC THIÊÁT BÒ LÖU TRÖÖ



7-ÑEÀ PHOØNG B-virus

ÑÖÖNG KHÔÛI ÑOÄNG MAÙY TÖÖ
ÑÓA MEÀM. NEÁU BUOÄC PHAÛI
KHÔÛI ÑOÄNG, HAÛY CHAÉC RAÈNG
ÑÓA MEÀM NAØY SAÏCH

8-ÑEÀ PHOØNG F-VIRUS

KHOÂNG ÑÖÖIC CHAÏY CAÙC
CHÖÔNG TRÌNH KHOÂNG ROÛ
NGUOÀN GOÁC.

NEÁU NGHI NGÔØ, SÖÛ DUÏNG
MOÄT PHAÀN MEÀM CHOÁNG VIRUS



9-ÑÈÀ PHOØNG MACRO VIRUS

KHI NHAÄN MÖÄT FILE **.DOC** HAY **.XL?** HAÕY NHÒU KIEÄM TRA VIRUS TRÖÖUC KHI MÔU

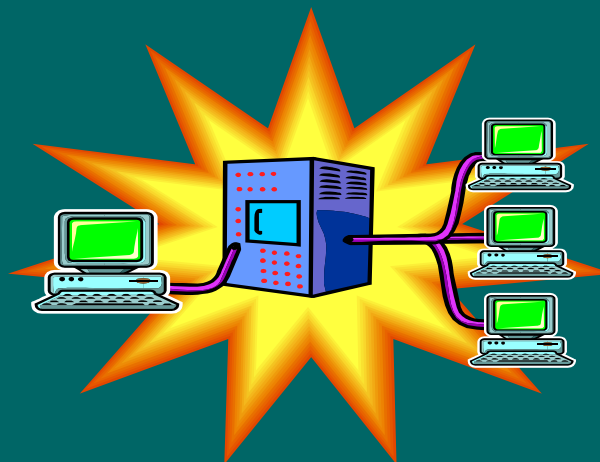
KHI MÔU TAÄP TIN, CHOÏN MENU **TOOL/MACRO** CUÛA WINWORD ÑÈÄ TÌM MACRO LAÏ. NEÁU COÙ, XOAÙ NGAY. SAU ÑÒU THOAÙT KHOÛI WINWORD, XOAÙ LUOÂN TAÄP TIN **NORMAL.DOT.**



Dùng chung màu y



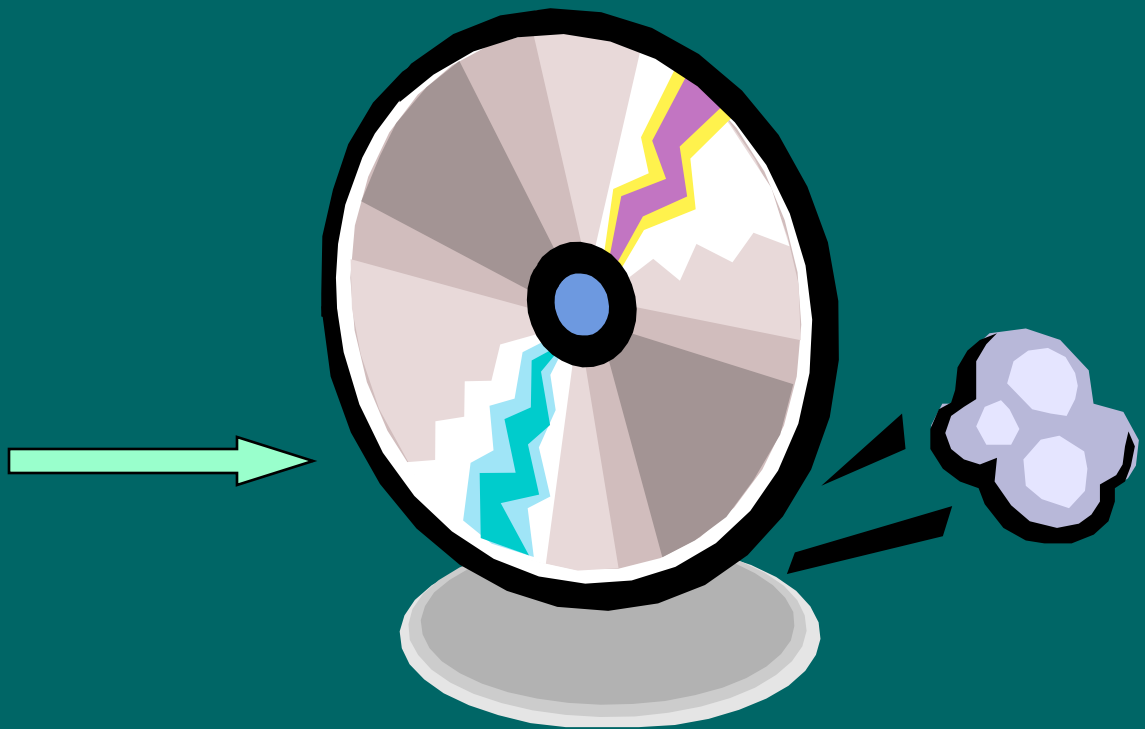
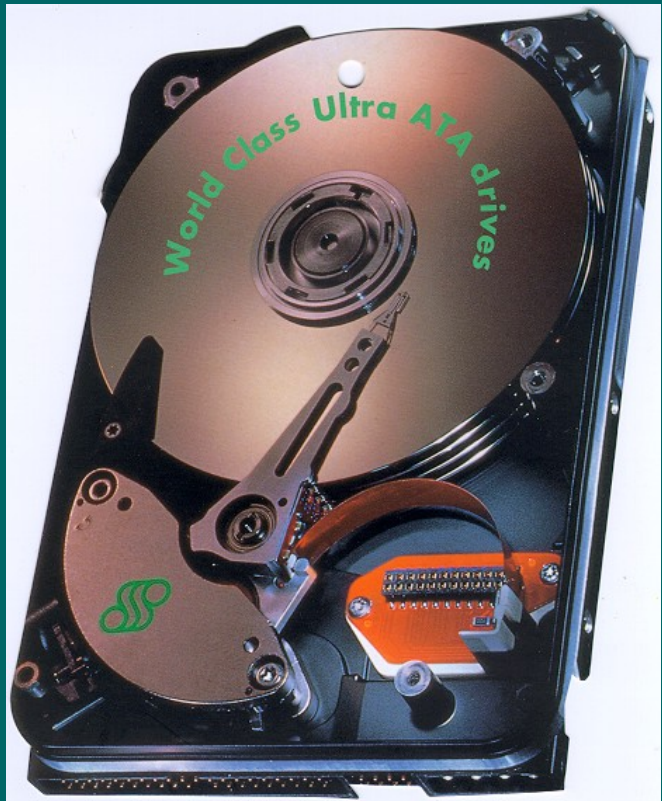
Nhään file keøm E-
Mail lạ



KHÔNG MỞ FILE LẠ ĐÍNH KÈM E-MAIL
KHÔNG XEM MAIL LẠ NGAY CẢ TRONG
CHẾ ĐỘ PREVIEW



SAO LƯU LÀ BIỆN PHÁP QUAN TRỌNG NHẤT



SAO LÖU THÖÖNG XUYEÂN HOAËC ÑÒNH KYØ DỮ LIỆU RA :

-ÑÓA MEÂM

-ÑÓA CÖÜNG THÖÙ 2

-FLASH ROM

-ÑÓA CD

-BAÊNG TÖØ



CHỌN THIẾT BỊ SAO LƯU

Sao lưu nhỏ : dưới 2 GB

- ổ đĩa quang từ usb 1gb
- ổ đĩa iomega zip usb 250 mg
- ổ cd-rw *

Sao lưu trung bình : 2 GB đến 20 GB

- ổ cứng cầm tay 20 gb
- ổ dvd-rw *

Sao lưu đầy đủ : trên 20 GB

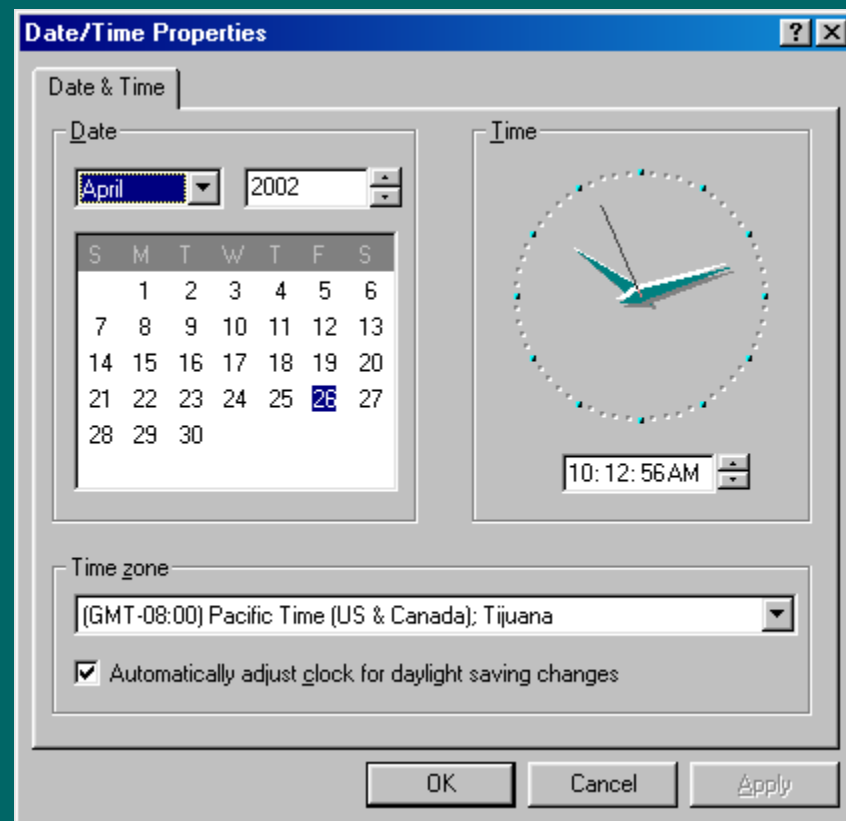
- ổ gắn ngoài 80 gb có tích hợp phần mềm sao lưu hệ thống *
- ổ băng từ dung lượng rất cao, rất tốt

8 LƯU Ý VỀ SAO LƯU

- Lập danh sách các tập tin cần sao lưu
- Quyết định mức độ sao lưu thường xuyên
- Duyệt lại dữ liệu sau sao lưu
- Tạo nhiều bản và cất nhiều nơi
- Bảo vệ, bảo quản tốt bản sao
- Không dùng một công nghệ duy nhất
- Dùng chương trình sao lưu với nhiều tính năng chứ đừng chỉ kéo thả
- Hãy chạy thử phần sao lưu

ĐỊNH NGÀY THÁNG GIÁ

**START/SETTINGS/
CONTROL PANEL**



**VIRUS CIH
CHERNOBYL 26-4**

ĐĨA MỀM CỨU HỘ

- Là đĩa mềm sạch có chứa các file sạch cần thiết để dự phòng
- Sử dụng khi Windows hư hay cài đặt lại Hệ điều hành, format đĩa cứng, khi máy bị Virus
- Nếu mua máy đã cài Windows thì phải kèm theo đĩa khởi động
- Đĩa chứa MS-DOS, với COMMAND.COM và vài file khác

TẠO ĐĨA MỀM CỨU HỘ

- Nhấn nút sách vào ổ A của một máy sách
- Start/Settings/Control Panel/Add/Remove Programs/Startup disk/Create disk
- OK
- Copy phần mềm diệt virus vào ổ A (hoặc vào một ổ sách khác)
- Nhấn các nút choáng ghi cho



CÁC ANTIVIRUS



- Chương trình diệt virus là chương trình nhôic thieát keá ñeå dò tìm caùc ñoaïn maõ virus ñaõ ñôic gaén vaø caùc chương trình khaùc vaø loaïi tröø caùc ñoaïn maõ aáy, phuc hoài laïi chương trình nhô tröôùc khi bò lây nhiễm.
- Caùc Anti-Virus ngoaïi thöông phaåm nhô SCAN của McAfee, Norton Anti-virus của Symantec, Toolkit
- Caùc Anti-Virus noãi free nhô D2 vaø

Hạn chế của Antivirus

- Các phần mềm Anti-Virus ñóng vai trò tích cực nhất trong việc chống Virus song :
- Chæ còu taüc ñưng trên các loại virus ñã biết
- Chæ laø moät chöông trình kiểm tra vào phức hoài các tập tin chöông trình ñã bò lây nhiễm virus
- Không nên ñặt niềm tin vào moät chöông trình Anti-Virus nào ñó
- Không còu taüc ñưng với các virus

CÁC LƯU Ý

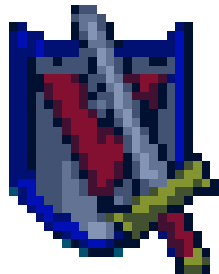
- Phaûi chaiÿ Anti-Virus saïch trong tình traïng boã nhôu saïch
- Raø queùt 1 laàn; khôûi ñoãng laïï maùy vaø raø queùt laàn 2
- Neân söû duïng caû Anti-Virus ngoaïï nhaäp vaø noãi ñò
- Duøng phoái hôïp ñoàng thôøi caùc Antivirus
- Chaiÿ ñònh kyø chòu khoâng chôø khi bò nhieãm
- Duøng AntiVirus môùi phaát



- Neáu maùy vaãn khôûi ñoäng ñöôïc töø ñóá cöùng thì duøng chính nhöõng phaàn meàm dieät virus ñaõ caøi treân ñóá cöùng ñeå queùt virus vì caùc phaàn meàm naøy ñaõ coù cô cheá töï baâu veä. Nhöng khi coù thoâng baùo virus xuaát hieän trong boä nhòu, phaûi duøng ñóá meàm cöùu hoä.
- Neáu khoâng khôûi ñoäng ñöôïc töø ñóá cöùng thì phaûi duøng ñóá meàm



PHAÀN MEÀM DIEÄT VIRUS



McAfee



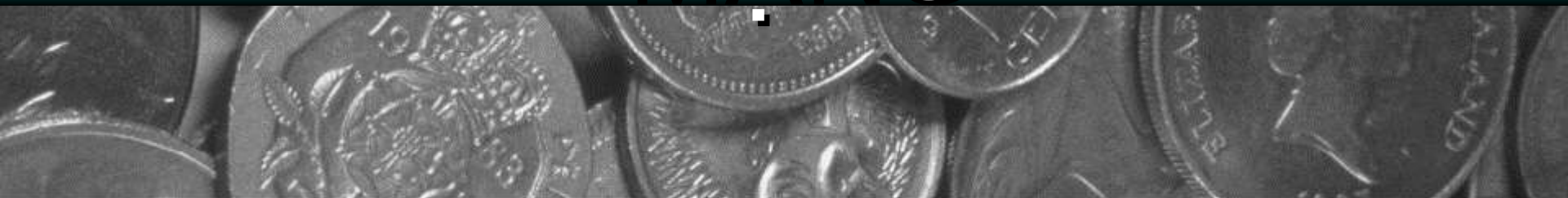
BKAV2002



Shortcut to
D32 Anti-virus



LẤY ANTIVIRUS TRÊN MẠNG



LẤY BKAV TRÊN WEB

<http://www.vnn.vn/vnn1/bkav>



The screenshot shows a Microsoft Internet Explorer browser window with the title "ANTI VIRUS BKAV - Nguyen Tu Quang". The address bar contains the URL "http://www.vnn.vn/vnn1/bkav/". The main content area displays the heading "BKAV DOWNLOAD" in red. Below the heading, there is a blue bullet point: "• Chọn các file bên dưới để download :". This is followed by a list of download links in blue text, each with a red subtitle indicating the update date and specific features:

- [Download BKAV401](#) Cập nhật 25/4/2002
- [Download BKAV2002](#) Cập nhật 1/1/2002
- [Download BKAV2002](#) Cập nhật 30/11. Diệt BadTrans.B
- [Download BKAV2002](#) Phiên bản chính thức
- [Download BKAV2002\[V\]](#) Cập nhật 5/11. Tiêu diệt Nimda.E
- [Download BKAV2002\[Beta2\]](#) Cập nhật virus mới
Phiên bản mới nhất, cập nhật ngày 31/10
- [Download BKAV2002\[Test\]](#)
- [Download BKAV384\[V\]](#)
- [Download BKAV383\[V\]](#)
- [Download BKAV383\[E\]](#)
- [Download BKAV365\[V\]](#)
- [Download BKAV365\[E\]](#)

LẤY D2 TRÊN WEB

<http://www.vnn.vn/vn1/d2>

CLB TIN HỌC VNN1 VIỆT NAM

Internet TODAY
click here

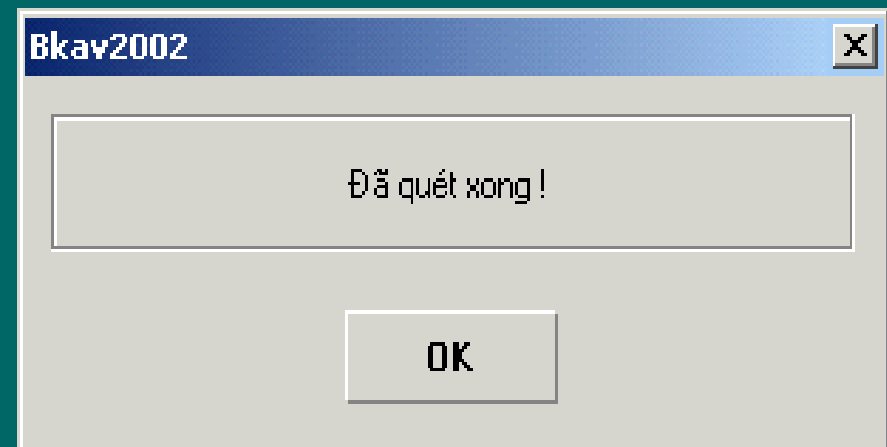
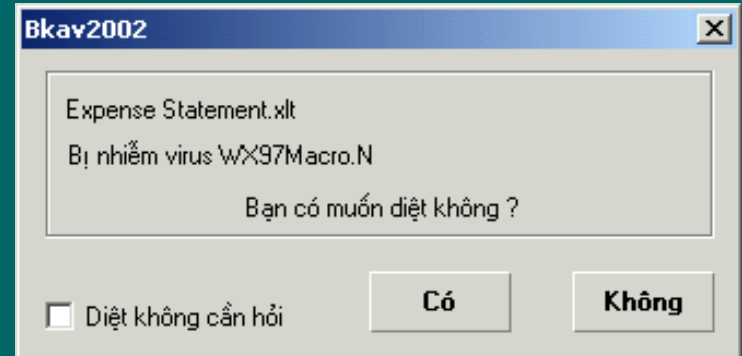
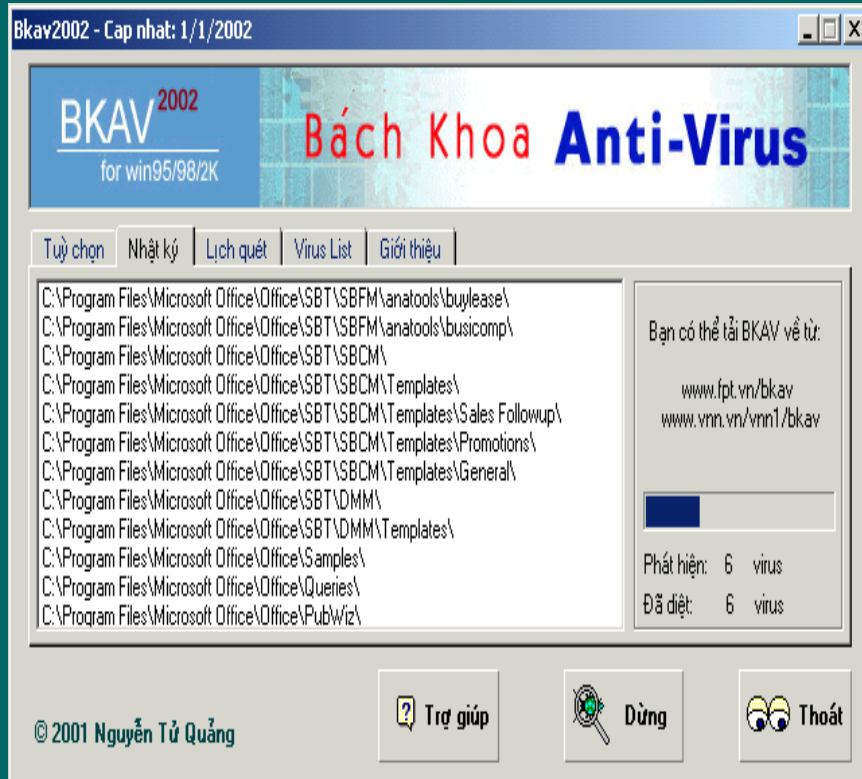
Trao đổi trên VNN1
Hệ thống & mạng Go

D2 ANTI VIRUS

D2 Update 24/9	Phiên bản này cập nhật virus Nimda version 1 và Nimda version 2. Nếu bạn đã cài đặt bản D32 ngày 10/9 thì có thể cài đặt ngay phiên bản này. Nếu chưa thì bạn hãy cài đặt D32 10/9
D2 Update 10/9	Phiên bản này cập nhật các virus DUN (Dial-up Networking) chuyên ăn cắp password, worm SST/VBS, nâng tổng số virus lên 357 con. Ngoài ra còn có thêm một số chức năng mới.
D2 Update 15/8	D32 Update 15/8 cập nhật thêm virus SirCam. Phiên bản này còn bổ sung một số chức năng sau: - Task list: Cho phép xem tất cả các tác vụ ứng dụng đang chạy background hoặc hidden, kể cả các virus đang thường trú. Chức năng này cho phép thể hiện (show), che dấu (hide) hoặc giải phóng (free) các tác vụ ứng dụng trong danh sách - Bổ sung địa chỉ link đến D32 Homepage

CHẠY BKAV





CHẠY D32

D32 [24-9-2001]

File View Tools About Help

Home Go Browse Extension Virus List Task List SysInfo History Options

Scan in C:\WINDOWS\SYSTEM

Links D32 Home ITVietnam LeHoan PC VISAigon

D32 Anti-virus*

Down

Open Save Expand Collapse Clean Hide

RECYCLED Dc18 _RESTORE TEMP ARCHIVE LOGS SFP EXTRACT WINDOWS COMMAND EBD OPTIONS OOBE CABS PWS SYSTEM

File	In folder	Size	Infected by	Status	
maestro.com	MWCI.DLL	CMPBK32.DLL	DCIMAN32.DLL	DISKCOPY.DLL	IR50_
SYNCENG.DLL	PIFMGR.DLL	CMUTIL.DLL	DDAO35.DLL	DSSSENH.DLL	IR50_
WSOCK32.DLL	USBUI.DLL	CMUTOA.DLL	DMSTYLE.DLL	DXTMSFT.DLL	IR_NI
DINDI.DLL	ACTXPRXY.DLL	CNETCFG.DLL	DMLOADER.DLL	DDRAWEX.DLL	ISIGN
DLCNDI.DLL	ADVPACK.DLL	COMCAT.DLL	DEVENUM.DLL	DXTMSFT3.DLL	MSR?
DSKMAINT.DLL	AUDIO3D.DLL	COMCTL32.DLL	DIGEST.DLL	DXTRANS.DLL	JAVA
ISSETUP.DLL	IPROP.DLL	CRTCTRL.DLL	DIGSIG.DLL	ES.DLL	JAVA
NDSWAN16.DLL	ASYCFILT.DLL	COOL.DLL	DIMM.DLL	HIDCI.DLL	JAVA
NDSWAN32.DLL	ATL.DLL	CORPOL.DLL	DMIME.DLL	MSLOCUSR.DLL	JGAV
NETAPI.DLL	AVICAP32.DLL	CRYPT32.DLL	DMBAND.DLL	FONTEXT.DLL	JGSD
INFRARED.DLL	AVIFIL32.DLL	CRYPTEXT.DLL	DOCPROP.DLL	HUNK.DLL	JGSH
NETOS.DLL	AVIFILE.DLL	DPLAY.DLL	DMCOMPOS.DLL	ICFG95.DLL	JOBE
NWINDS.DLL	BLACKBOX.DLL	DMUSIC32.DLL	DX7VB.DLL	IEPEERS.DLL	JSCR
PPNDI.DLL	BROWSELCD.DLL	DMUSIC16.DLL	DSOUND3D.DLL	SCROBJ.DLL	MSS1
RNASERV.DLL	BROWSEUI.DLL	DMUSIC.DLL	DRMCLIE.DLL	IESETUP.DLL	LMR1
SYSDETMG.DLL	MSNETOBJ.DLL	DMSYNTH.DLL	DPSERIAL.DLL	IMAGEHLP.DLL	MB5L
SETUPX.DLL	DDAO36.DLL	DBMSRPCN.DLL	DPMODEMX.DLL	IMGUTIL.DLL	MCIQ
HOTPLUG.DLL	CDFVIEW.DLL	DBMSADSN.DLL	GCHAND.DLL	INDICDLL.DLL	MF32
ISDNUI.DLL	WEBVW.DLL	DBMSSHRN.DLL	DPLAYX.DLL	INET16.DLL	MF3C
RPCLTC5.DLL	CEWMDM.DLL	DBMSSOCN.DLL	IENPSTUB.DLL	INITPKI.DLL	MEMI
RPCLTCCM.DLL	CHOOUSR.DLL	DBMSSPXN.DLL	DPVACM.DLL	INSENG.DLL	MFCL
RPCLTS5.DLL	CLRVIDDC.DLL	DBMSVINN.DLL	DPWSOCKX.DLL	IR41_QC.DLL	MLAN
SENDMAIL.DLL	CMCFG32.DLL	DBNMPNTW.DLL	DS32GT.DLL	IR41_QCX.DLL	MSRI
FRAMEBUF.DLL	CMDIAL32.DLL	DECVW_32.DLL	DSSBASE.DLL	IR50_32.DLL	MMS'

228 7% 552 2m.0s 0:10

Start Microsoft PowerPoint - [Co... D32 7:03 PM

BẮT VIRUS

Neáu nhiễm virus mồi, cheùp caùc file bò laây nhiễm göúi ñeán caùc ñòa chæAnti-Virus

- Vôùi new **Macro Virus**, cheùp file .DOC, .XL?
- Vôùi new **B-Virus**, ñoïc ñóa baèng leãnh DIR A: ñeã baét noù leãn ñóa
- Vôùi new **F-Virus**, cheùp caùc file taêng kích thồùc cuùa taäp tin .COM, .EXE

Neân ghi nhòu kích thồùc file thoâng ñuïng nhò DOSKEY.COM. Trong môi trồøng nhiễm New F-Virus, chaiy DOSKEY.COM

DỰ BÁO

- Các loại virus sẽ lây nhiễm không phải vào hàng trăm ngàn triệu tính mà là hàng triệu triệu tính
- Các virus của tương lai có thể hoạt động theo những xu hướng như sau:
 - Khai thác các lỗ hổng phần mềm của các phần mềm
 - Lây lan theo những cách thức khác nhau như virus lai tạo, hoặc thậm chí trực tiếp,...
 - Các chương trình con phần mềm của Virus

BIỆN PHÁP

- NGHIÊN CỨU NẾU TẠO LẬP CÁC ANTI-VIRUS CÓ KHẢ NĂNG NHẬN ĐĂNG VIRUS MÀ KHÔNG CẦN CẬP NHẬT THEO CƠ CHẾ MIỄN DÒCH.
- TẠO CÁC PHIÊN BẢN THỬ NGHIỆm HỒI TỒI HỆ CHỐNG TRÌNH CHOÁNG VIRUS THÔNG MINH CÓ KHẢ NĂNG ĐỔI BÀO SƠI XUAÁT HIỆN CỬA CÁC LOẠI VIRUS MÔU



- TÌM VÀ LẮP CÁC LỖ HỔNG TRONG CÁC PHẦN MỀM ĐỂ NGĂN CHẶC HACKER THÂM NHẬP PHÁT TÁN VIRUS
- XÀUC LAÄP VAØ THÖIC THI CAUC ÑIEÀU KHOAÛN TRONG BOÄ LUAÄT HÌNH SÖI VEÀ TOÄI DANH PHAÙ HOAÏI DÖÖ LIEÄU

5.3 HACKER





Hacker lạo những kẻ sâu đuiing
măing maùy tính ñeã phaùt taùn
Virus; laáy caép maät khaâu ñeã
truy nhaäp baát hôiïp phaùp vaøo
măing vaø maùy tính cuûa caùc toã
chöùc, caù nhaân ñeã phaù hoaiï,
gian laän...

6 THỦ ĐOẠN

- Gôûi E-mail kèm file còu chòuc naêng thòôøng truù ñeã laáy caép thoàng tin trong maùy, ñaéc bieät laø password roài töi ñoäng gôûi cho Hacker
- Ñaùnh caép file löu Password roài duøng caùc kyõ thuaät beù maät khaâu
- Duøng phaàn meàm ñaùnh bomb thò
- Tìm möi khe hôu cuûa caùc phaàn meàm heã thoáng vaø caùc phaàn meàm công cui, keã caù caùc Anti-Virus ñeã taán công

THỦ ĐOẠN

- Cung cấp trên mạng những mã nguồn Virus làm sẵn để kẻ khác có thể lắp ráp, lại ghép thành nhiều Virus mới. Hacker nào nhanh chóng nào tạo ra các Hacker
- Thành lập tổ chức của các Hacker trên mạng, hình thành các “liên minh ma quỷ”, tạo thành một lực lượng rất nguy hiểm.

CÁC KIỂU BẺ MẬT KHẨU

- **DÙNG TỪ ĐIỂN (WORD-LIST)**
 - TỰ ĐIỂN DO HACKER TẠO
 - TỪ ĐIỂN NGÔN NGỮ SẴN CÓ
 - DÙNG CÙNG MỘT GIẢI THUẬT MÃ HOÁ MẬT KHẨU
 - DÙNG MÁY TÍNH TỐC ĐỘ CAO
- **THỬ HÀNG LOẠT (BRUTE-FORCING)**
 - THỬ CÁC TỔ HỢP VỚI CÁC ĐỘ DÀI KHÁC NHAU
 - PHƯƠNG PHÁP MẠNH NHƯNG RẤT CHẬM



- KẾT HỢP CẢ 2 CÁCH TRÊN
- CÓ NHIỀU CHƯƠNG TRÌNH BẰ MẬT KHẨU NHƯ 10pht PASSWORD CRACK
- NHƯNG LẤY GÌ ĐỂ SO KHỚP KHI CHƯA THÂM NHẬP ĐƯỢC VÀO MẠNG ? PASSWORD ĐƯỢC LƯU GIỮ NHƯ THẾ NAO ?
- ĐÁNH CẮP PASSWORD BỞI VIRUS LẤY CẮP FILE ?

CÁCH PHÒNG CHỐNG

1. CHOÁNG TRUY NHẬP TRÀUÌ PHEÙP
BAÈNG CAÙCH ÑAËT VAØ BAÙO
VEÀ PASSWORD

2. NGĂN CHẶN TỪ XA



CÁC CÁCH ĐẶT PASSWORD

- SYSTEM
- NO SYSTEM
- FILE .DOC
- LỢI VÀ HẠI KHI ĐẶT PASSWORD

9 HƯỚNG DẪN VỀ PASSWORD

- Thông xuyên nào mật khẩu
- Hãy nhớ một mật khẩu phức tạp. Một mật khẩu mạnh thông thường có ít nhất 8 ký tự
- Kể khác nhau nào, ta khác nhau



- Baùo maät caùc thoâng tin caù nhân ñaëc bieät laø soá ñieän thoai
- Caùnh giaùc vôi caùc phaàn meàm Download töø maing
- Caùnh giaùc vôi caùc file göui kèm theo E-mail keã caù caùc file ñöôic göui töø baïn beø vì rất coù khaù naêng chính maùy tính của hoï cuõng bà nhieãm virus



- Tăng cường tính bảo mật của trình duyệt và chống trình gửi nhận e-mail bằng cách nâng cao chất lượng bảo mật của trình duyệt Internet.

Nhờ trong Windows :

Computer/Control
Panel/Internet/Security

- Hợp tác với ISP để cài đặt các chương trình chống xâm nhập

5.4 DỰ BÁO



DỰ BÁO

- Các loại virus sẽ lây nhiễm không phải vào hàng trăm ngàn máy tính mà là hàng triệu máy tính
- Các virus của tương lai có thể hoạt động theo những xu hướng như sau:
 - Khai thác các lỗ hổng phần mềm của các phần mềm
 - Lây lan theo những cách thức khác nhau như virus lai tạo, hoặc thậm chí trực tuyến,...
 - Các chương trình con phần mềm của Virus

AN NINH MẠNG

- PHẢI NGĂN CHẶN HACKER TỪ XA BỞI CÁC CƠ QUAN AN NINH MẠNG
- NGHIÊN CỨU NẾU TẠO LẬP CÁC ANTI-VIRUS CÒN KHAU NÊN NHẬN ĐĂNG VIRUS MẠO KHOẢNG CẦN CẬP NHẬT THEO CÁCH MIỄN DỊCH.
- TẠO CÁC PHIEÂN BẢN THƯỜNG NGHIÊM HỒI TÔI HẸ CHỖNG TRÌNH CHỌNG VIRUS THÔNG MINH CÒN KHAU NÊN ĐỔI BÀO SỞ XUẤT HIỆN CỦA CÁC LOẠI VIRUS MỚI
- XÁC LẬP VÀO THỜI THỰC THỰC CÁC NẾU KHOA LẬP TRONG BỐ LỰA HÌNH SỞ VÀ

AN NINH MẠNG

- CÓ NHIỀU LỖ HỔNG TRONG CÁC PHẦN MỀM ĐỂ HACKER THÂM NHẬP

*NHƯ LẤY MAIL VỀ TUY KHÔNG MỞ FILE ĐÍNH KÈM, SONG NẾU LÀ FILE ÂM THANH THÌ CHƯƠNG TRÌNH **OUTLOOK EXPRESS** TỰ ĐỘNG MỞ VÀ VIRUS THÂM NHẬP*

- CẦN XAÙC ÑÒNH LOÃI SÒÙM NHAÁT CỦA CÁC PHẦN MỀM ÑEẢ TÌM BIỀÑ PHAÙP GIAÙI QUYỀÁT KHAÙ THI