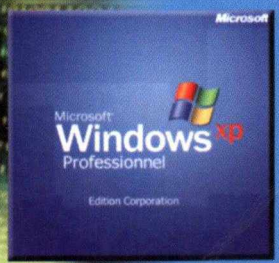
Water PC

xp

TỰ KHẮC PHỤC MÁY TÍNH KHI BỊ VI RÚT TẤN CÔNG



TỦ SÁCH TIN HỌC

NHÀ XUẤT BẢN
VĂN HÓA THÔNG TIN

TỰ KHẮC PHỤC

MÁY TÍNH KHI BỊ VI RÚT TẤN CÔNG

NHÀ XUẤT BẢN VĂN HÓA THÔNG TIN
Số 43 Lò Đúc - Hà Nội. ĐT: 04 39712448

CÔNG TY THƯƠNG MẠI & DỊCH VỤ VĂN HÓA ĐINH TỊ
ĐC: Số 9 - A6 - KĐT Đầm Trầu - Hai Bà Trưng - Hà Nội
ĐT: 04 22192869 - 04 39334889 Fax: 04 39334943
Website: www.dinhtibooks.com.vn Email: dinhti@fpt.vn
Chi nhánh: 107 Đào Duy Anh - P9 - Q. Phú Nhuận - TPHCM
ĐT: 08 38446287 Fax: 08 38447135 Email: cndinhti@hcm.fpt.vn

TỰ KHẮC PHỤC MÁY TÍNH KHI BỊ VIRUS TẤN CÔNG

Chịu trách nhiệm xuất bản
NGUYỄN VĂN KHƯƠNG

Biên tập : THIỆN MINH
Bìa : PHẠM BÌNH
Kỹ thuật vi tính : ĐINH TỊ

In 1000 bản - Khổ 13 cm x 20,5 cm - Tại Xí nghiệp Bản đồ 1, BQP
Giấy chấp nhận ĐKKHXB số: 552-2009/CXB/55/20-53/VHTT
In xong và nộp lưu chiểu năm 2010.

Water PC

TỰ KHẮC PHỤC MÁY TÍNH KHI BỊ VI RÚT TẤN CÔNG

NHÀ XUẤT BẢN
VĂN HÓA THÔNG TIN

Bài 1

LỊCH SỬ PHÁT TRIỂN VIRUS MÁY TÍNH

1. Các giai đoạn phát triển virus máy tính

Virus máy tính có một quá trình phát triển khá dài, và nó luôn song hành cùng những chiếc "máy tính", (tất nhiên là người bạn máy tính chẳng thích thú nó). Khi công nghệ phần mềm cũng như phần cứng phát triển thì virus cũng phát triển theo. Hệ điều hành thay đổi thì virus máy tính cũng tự thay đổi mình để phù hợp với hệ điều hành đó và để có thể ăn bám ký sinh. Tất nhiên là virus không tự sinh ra.

Có thể việc viết virus mang mục đích phá hoại, thử nghiệm hay đơn giản chỉ là một thú đùa vui ác ý. Nhưng chỉ có điều những cái đầu thông minh này khiến chúng ta phải đau đầu đối phó và cuộc chiến này gần như không chấm dứt, nó vẫn đang tiếp diễn.

Có nhiều tài liệu khác nhau nói về xuất xứ của virus máy tính, âu cũng là điều dễ hiểu, bởi lẽ vào thời điểm đó con người chưa thể hình dung ra nổi một "xã hội" đông đúc và nguy hiểm của virus máy tính như ngày nay, điều đó cũng có nghĩa là không mấy người quan tâm tới chúng. Chỉ khi chúng gây ra những hậu quả nghiêm trọng như ngày nay, người ta mới lật lại hồ sơ để tìm hiểu. Tuy vậy, đa số các câu chuyện xoay quanh việc xuất xứ của virus máy tính đều ít nhiều liên quan tới những sự kiện sau:

1983 - Để lộ nguyên lý của trò chơi "Core War"

"Core War" là một cuộc đấu trí giữa hai đoạn chương trình máy tính do hai lập trình viên viết ra. Mỗi đấu thủ sẽ đưa một

chương trình có khả năng tự tái tạo gọi là Organism vào bộ nhớ máy tính. Khi bắt đầu cuộc chơi, mỗi đấu thủ sẽ cố gắng phá huỷ Organism của đối phương và tái tạo Organism của mình. Đấu thủ thắng cuộc là đấu thủ tự nhân bản được nhiều nhất.

Trò chơi "Core War" này được giữ kín đến năm 1983, Ken Thompson - người đã viết phiên bản đầu tiên cho hệ điều hành UNIX, đã để lộ ra khi nhận một trong những giải thưởng danh dự của giới điện toán - Giải thưởng A.M Turing. Trong bài diễn văn của mình ông đã đưa ra một ý tưởng về virus máy tính dựa trên trò chơi "Core War". Cũng năm 1983, tiến sỹ Frederick Cohen đã chứng minh được sự tồn tại của virus máy tính.

Tháng 5 năm 1984, tờ báo Scientific America có đăng một bài báo mô tả về "Core War" và cung cấp cho độc giả những thông tin hướng dẫn về trò chơi này. Kể từ đó virus máy tính xuất hiện và đi kèm theo nó là cuộc chiến giữa những người viết ra virus và những người diệt virus.

1986 - Brain virus

Có thể được coi là virus máy tính đầu tiên trên thế giới, Brain âm thầm đổ bộ từ Pakistan vào nước Mỹ với mục tiêu đầu tiên là Trường Đại học Delaware. Một nơi khác trên thế giới cũng đã mô tả sự xuất hiện của virus, đó là Đại học Hebrew - Israel.

1987 - Lehigh virus xuất hiện

Lại một lần nữa liên quan tới một trường Đại học. Lehigh chính là tên của virus xuất hiện năm 1987 tại trường Đại học này. Trong thời gian đó cũng có một số virus khác xuất hiện, đặc biệt WORM virus (sâu virus), cơn ác mộng với các hệ thống máy chủ cũng xuất hiện. Cái tên Jerusalem chắc sẽ làm cho công ty IBM nhớ mãi với tốc độ lây lan đáng nể: 500000 nhân bản trong một giờ.

1988 - Virus lây trên mạng

Ngày 2 tháng 11 năm 1988, Robert Morris đưa virus vào mạng máy tính quan trọng nhất của Mỹ, gây thiệt hại lớn. Từ

đó trở đi người ta mới bắt đầu nhận thức được tính nguy hại của virus máy tính.

1989 - AIDS Trojan

Xuất hiện Trojan hay còn gọi là "con ngựa thành Troie", chúng không phải là virus máy tính, nhưng luôn đi cùng với khái niệm virus. "Những chú ngựa thành Troie" này khi đã gắn vào máy tính của bạn thì nó sẽ lấy cắp một số thông tin mật trên đó và gửi đến một địa chỉ mà chủ của chú ngựa này muốn nó vận chuyển đến, hoặc đơn giản chỉ là phá huỷ dữ liệu trên máy tính của bạn.

1991 - Tequila virus

Đây là loại virus đầu tiên mà giới chuyên môn gọi là virus đa hình, nó đánh dấu một bước ngoặt trong cuộc chiến giữa cái thiện và cái ác trong các hệ thống máy tính.

Đây thực sự là loại virus gây đau đầu cho những người diệt virus và quả thật không dễ dàng gì để diệt chúng. Chúng có khả năng tự thay hình đổi dạng sau mỗi lần lây nhiễm, làm cho việc phát hiện ra chúng quả thật là khó.

1992 - Michelangelo virus

Tiếp nối sự đáng sợ của "virus đa hình" năm 1991, thì công cụ năm 92 này tạo thêm sức mạnh cho các loại virus máy tính bằng cách tạo ra sự đa hình cực kỳ phức tạp. Chúng luôn biết cách gây ra khó khăn cho những người diệt virus.

1995 - Concept virus

Sau gần 10 năm kể từ ngày virus máy tính đầu tiên xuất hiện, đây là loại virus đầu tiên có nguyên lý hoạt động gần như thay đổi hoàn toàn so với những tiền bối của nó. Chúng gây ra một cú sốc cho những công ty diệt virus cũng như những người tình nguyện trong lĩnh vực phòng chống virus máy tính.

Những năm sau đó, những virus theo nguyên lý của Concept được gọi chung là virus Macro, chúng tấn công vào

các hệ soạn thảo văn bản của Microsoft (Word, Excel, PowerPoint). Tuy nhiên cho tới nay, các virus Macro hầu như không còn tồn tại nữa và cùng với việc mọi người không còn sử dụng các Macro trong văn bản của mình nữa thì virus Macro đang dần bị quên lãng.

1996 - Boza virus

Khi hãng Microsoft chuyển sang hệ điều hành Windows95 và họ cho rằng virus không thể công phá thành trì của họ được, thì năm 1996 xuất hiện virus lây trên hệ điều hành Windows95.

1999 - Melissa, Bubbleboy virus

Đây thật sự là một cơn ác mộng với các máy tính trên khắp thế giới. Sâu Melissa không những kết hợp các tính năng của sâu Internet và virus Macro, mà nó còn biết khai thác một công cụ mà chúng ta thường sử dụng hàng ngày là Microsoft Outlook Express để chống lại chính chúng ta. Khi máy tính của bạn bị nhiễm Mellissa, nó sẽ tự phân phát mình đi mà khổ chủ không hề hay biết. Và bạn cũng sẽ rất bất ngờ khi bị mang tiếng là phát tán virus.

Chỉ từ ngày thứ sáu tới ngày thứ hai tuần sau, virus này đã kịp lây nhiễm 250 ngàn máy tính trên thế giới thông qua Internet, trong đó có Việt Nam, gây thiệt hại hàng trăm triệu USD. Một lần nữa cuộc chiến lại sang một bước ngoặt mới, báo hiệu nhiều khó khăn bởi Internet đã được chứng minh là một phương tiện hữu hiệu để virus máy tính có thể lây lan trên toàn cầu chỉ trong vài tiếng đồng hồ.

Năm 1999 đúng là một năm đáng nhớ của những người sử dụng máy tính trên toàn cầu, ngoài Melissa, virus Chernobyl hay còn gọi là CIH đã phá huỷ dữ liệu của hàng triệu máy tính trên thế giới, gây thiệt hại gần 1 tỷ USD vào ngày 26 tháng 4.

2000 - DDoS, Love Letter virus

Có thể coi là một trong những vụ việc virus phá hoại lớn nhất từ trước đến thời điểm đó, Love Letter có xuất xứ từ Philippines

do một sinh viên nước này tạo ra, chỉ trong vòng có 6 giờ đồng hồ đã kịp đi vòng qua 20 nước trong đó có Việt Nam, lây nhiễm 55 triệu máy tính, gây thiệt hại 8,7 tỷ USD.

Năm 2000 cũng là năm ghi nhớ cuộc tấn công "Từ chối dịch vụ phân tán" - DDoS (Distributed Denial of Service) quy mô lớn do virus gây ra đầu tiên trên thế giới, nạn nhân của đợt tấn công này là Yahoo!, Amazon.com... Tấn công "Từ chối dịch vụ" - DDoS là cách tấn công gây "ngập lụt" bằng cách từ một máy gửi liên tiếp các yêu cầu vượt mức bình thường tới một dịch vụ trên máy chủ, làm ngưng trệ, tê liệt khả năng phục vụ của dịch vụ hay máy chủ đó. Những virus loại này phát tán đi khắp nơi và nằm vùng ở những nơi nó lây nhiễm. Chúng sẽ đồng loạt tấn công theo kiểu DDoS vào các hệ thống máy chủ khi người điều hành nó phất cờ, hoặc đến thời điểm được định trước.

2001 - Winux Windows/Linux Virus, Nimda, Code Red virus

Winux Windows/Linux Virus đánh dấu những virus có thể lây được trên các hệ điều hành Linux chứ không chỉ Windows. Chúng nguỵ trang dưới dạng file MP3 cho download.

Nimda, Code Red là những virus tấn công các đối tượng của nó bằng nhiều con đường khác nhau (từ máy chủ sang máy chủ, sang máy trạm, từ máy trạm sang máy trạm...), làm cho việc phòng chống vô cùng khó khăn, cho đến tận cuối năm 2002, ở Việt Nam vẫn còn những cơ quan với mạng máy tính có hàng trăm máy tính bị virus Nimda quấy nhiễu. Chúng cũng chỉ ra một xu hướng mới của các loại virus máy tính là "tất cả trong một", trong một virus bao gồm nhiều virus, nhiều nguyên lý khác nhau.

2002 - Sự ra đời của hàng loạt loại virus mới

Ngay trong tháng 1 năm 2002 đã có một loại virus mới ra đời. Virus này lây những file.SWF, điều chưa từng xảy ra trước đó (ShockWaveFlash - một loại công cụ giúp làm cho

các trang Web thêm phong phú). Tháng 3 đánh dấu sự ra đời của loại virus viết bằng ngôn nhữ C#, một ngôn ngữ mới của Microsoft. Con sâu.Net này có tên SharpA và được viết bởi một người phụ nữ!

Tháng 5, SQLSpider ra đời và chúng tấn công các chương trình dùng SQL. Tháng 6, có vài loại virus mới ra đời: Perrun lây qua Image JPEG Scalper tấn công các FreeBSD/Apache Web server.

Người sử dụng máy tính trên thế giới bắt đầu phải cảnh giác với một một loại chương trình độc hại mới mang mục đích quảng cáo bất hợp pháp - Adware và thu thập thông tin cá nhân trái phép - Spyware (phần mềm gián điệp). Lần đầu tiên các chương trình Spyware, Adware xuất hiện như là các chương trình độc lập, không phải đi kèm theo các phần mềm miễn phí như trước đó. Chúng bí mật xâm nhập vào máy của người dùng khi họ vô tình "ghé thăm" những trang Web có nội dung không lành mạnh, các trang Web bẻ khóa phần mềm...Và với nguyên lý như vậy, ngày nay các phần mềm Adware và Spyware đã thực sự trở thành những "bệnh dịch" hoành hành trên mạng Internet.

2003 - Các virus khai thác lỗ hổng phần mềm

Năm 2003 mở đầu thời kỳ phát triển mạnh mẽ của các virus khai thác lỗ hổng phần mềm để cài đặt, lây nhiễm lên các máy tính từ xa - đây cũng chính là xu hướng phát triển hiện nay của virus trên thế giới. Đầu tiên là virus Slammer khai thác lỗ hổng phần mềm Microsoft's SQL 2000 servers, chỉ trong vòng 10 phút đã lây nhiễm trên 75000 máy tính trên khắp thế giới. Tiếp đến là hàng loạt các virus khác như Blaster (MsBlast), Welchia (Nachi), Mimail, Lovgate...khai thác lỗi tràn bộ đệm trong công nghệ DCOM - RPC trên hệ điều hành Window2K, XP. Xuất hiện trên thế giới vào ngày 11/8, virus Blaster nhanh chóng lây lan trên 300.000 máy tính trên khắp thế giới, trong đó có Việt Nam. Những người

sử dụng máy tính ở Việt Nam hẳn không quên được sự hỗn loạn vì hàng loạt máy tính bị Shutdown tự động trong ngày 12/8 khi virus Blaster lây vào các máy tính ở Việt Nam.

Virus cũng bắt đầu được sử dụng như một công cụ để phát tán thư quảng cáo (spam) nhanh nhất. Các virus họ Sobig nổi lên như những cỗ máy phát tán một lượng thư quảng cáo khổng lồ trên khắp thế giới. Cũng trong năm này, thế hệ những virus mới như Lovgate, Fizzer đã bắt đầu sử dụng những mạng chia sẻ file ngang hàng peer to peer như KaZaa để phát tán virus qua các thư mục chia sẻ trên mạng.

2004 - Cuộc chạy đua giữa Skynet và Beagle

Cuộc chạy đua giữa hai họ virus cùng có nguồn gốc từ Đức và lây nhiễm nhiều nhất trong năm này bắt đầu bằng việc các biến thể mới của virus Skynet khi lây nhiễm vào một máy tính sẽ tìm cách loại bỏ các virus họ Beagle ra khỏi máy đó và ngược lại. Mỗi biến thể của Skynet xuất hiện trên thế giới thì gần như ngay lập tức sẽ lại có một biến thể của Beagle được viết ra để chống lại nó và ngược lại. Cuộc chạy đua này kéo dài liên tục trong mấy tháng đã làm cho số lượng virus mới xuất hiện trong năm 2004 tăng lên một cách nhanh chóng.

Năm 2004 cũng là năm xuất hiện virus khai thác lỗ hổng của dịch vụ LSASS (Local Security Authority Subsystem Service) trên hệ điều hành Window 2K, Window XP để lây lan giữa các máy tính - virus Sasser. Cũng giống như virus Blaster, virus Sasser nhanh chóng gây nên một tình trạng hỗn loạn trên mạng khi làm Shutdown tự động hàng loạt máy tính mà nó lây nhiễm.

2005 - Sự xuất hiện của các virus lây qua các dịch vụ chatting

Các dịch vụ chatting trực tuyến như Yahoo!, MSN bắt đầu được virus lợi dụng như một công cụ để phát tán virus trên mạng. Trong vòng 6 tháng đầu năm, đã có tới 7 virus lây lan qua các dịch vụ chatting xuất hiện ở Việt Nam. Trong thời gian tới, những virus tấn công thông qua các dịch vụ chatting

sẽ còn tiếp tục xuất hiện nhiều hơn nữa khi số người sử dụng dịch vụ này ngày càng tăng.

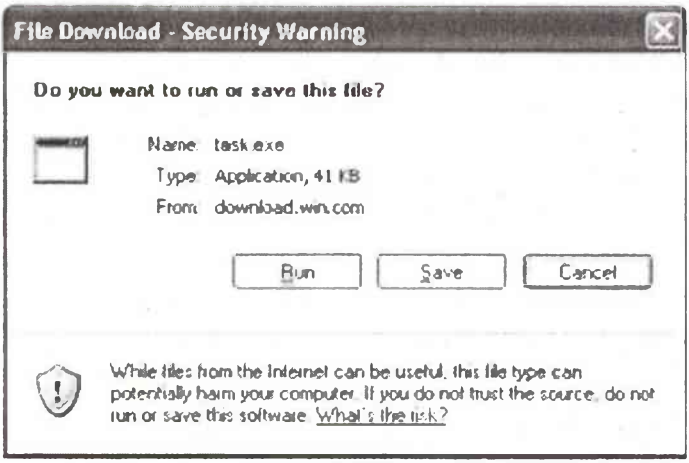
2. Phòng chống và khắc phục sự cố máy tính nhiễm virus qua Yahoo! Messenger

Khi đề cập đến virus lây qua Internet, người dùng thường nghĩ đến các loại sâu trình thư điện tử và cho rằng không mở file đính kèm E-mail lạ là không bị nhiễm. Nay tình hình đã khác trước, không đạt được mục đích gì với trò *"hãy mở tập tin trong thư này để xem nhé"*, các hacker đã chuyển hướng bằng cách lợi dụng lỗ hổng của chương trình Instant Messenger để lây nhiễm. Khi các virus này được giới tin tặc trong nước thu thập mã nguồn từ Internet rồi "Việt hóa", tình hình càng thêm tệ hại!

Hiện trạng "nhức nhối"

Tháng 4-2006, virus Gaixinh được tung lên mạng để gài bẫy những kẻ hiếu kỳ bằng lời dụ dỗ *"Gai dep!... hay xem cai nay di..."*. Trong khi biên bản vi phạm hành chính của công an dành cho kẻ quấy rối chưa kịp ráo mực thì tháng 7 này, các virus nội YMHeart, Vlove lại giở trò lừa đảo người sử dụng Yahoo! Messenger bằng mánh lới mời nhấp chuột vào các đường link có nội dung "rẻ tiền" như: *Nhan Vao Day De Gui 1 Trai Tim Cho Ban Be; nguoiiu.com/life/Tang ban tam thiep ne; Vui qua ne; Truyen cuoi do, vao di...* Thâm hiểm hơn, virus Viet8xYM còn lợi dụng tình hình rối ren để lừa nạn nhân "dính" thêm một virus khác: *"Neu ai bi nhiem virus minhut.be thi vao day coi cach diet nhe"*.

Khi đường link được kích hoạt, một file EXE ẩn trên Website sẽ được tải về máy đích. Nếu tình trạng an ninh của máy được đặt ở chế độ cao (điều chỉnh trong Internet Explorer - Tools - Internet Options - Security Setting), bạn sẽ nhận được cảnh báo của Windows. Hãy nhấn Cancel để từ chối, nếu không mã virus sẽ được kích hoạt.



Nếu vì lý do nào đó tập tin EXE vẫn được thi hành (bạn đã nhấn Run, hoặc tình trạng an ninh trên máy bạn đang đặt ở chế độ thấp), virus sẽ nhanh chóng khống chế hệ thống. Một trong những hành vi phổ biến là lấy cắp sổ địa chỉ và mật khẩu tài khoản trên máy. Do người Việt Nam chưa có thói quen giao dịch ngân hàng qua mạng, nên trước mắt thiệt hại của loại virus này là không lớn. Tuy nhiên, khả năng tiềm ẩn nguy cơ rất cao, khi mà đối tượng chúng nhắm đến là cộng đồng sử dụng Yahoo! Messenger, môi trường giao lưu qua Internet phổ biến nhất hiện nay của thanh thiếu niên.

Cũng giống như sâu trình E-mail, để đề phòng loại virus này, tốt nhất bạn không nên nhấp chuột vào các đường link chưa rõ nguồn gốc, đặc biệt là trong lúc chat. Nghe có vẻ đơn giản, nhưng thật không dễ thực hiện chút nào, nhất là khi cuộc trò chuyện trực tuyến đang hồi thân mật. Sau đây tôi sẽ mách bạn một số mẹo nhỏ phòng khi máy tính bị nhiễm các loại virus Internet này.

Phát hiện máy nhiễm

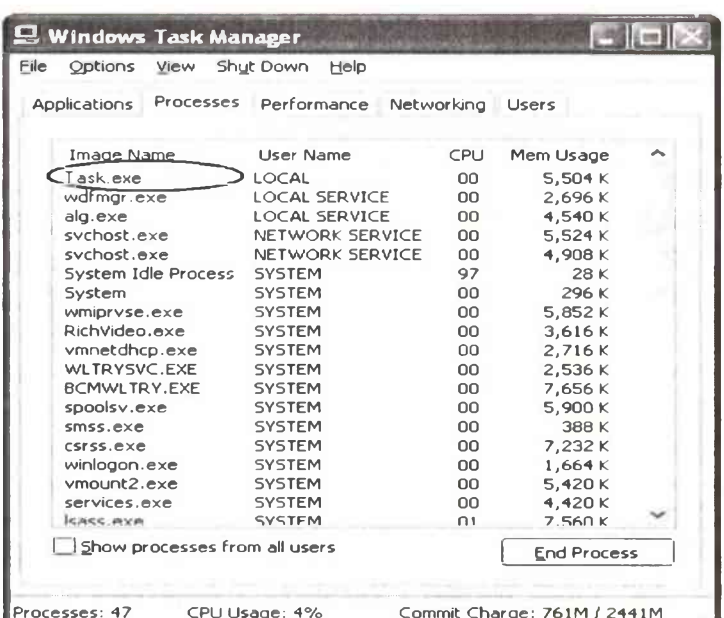
Không có một kịch bản chung cho mọi trường hợp nhiễm virus. Khi nhiễm vào máy, VloveYM sẽ thay trang chủ của trình duyệt Internet Explorer thành địa chỉ trỏ đến

fun.nguoiiu.com. Virus Myheart thì "ngụy trang" với hình trái tim và bông hoa đẹp kèm theo một đường link xuất hiện trên cửa sổ Yahoo! Messenger. Một số virus khác che phần mở rộng của các tập tin rồi vô hiệu trình đơn Folder Options từ menu Tools của Windows Explorer để chèn file virus lẫn lộn vào cấu trúc folder hệ thống.

Nói chung, khi nhiễm virus, máy tính sẽ hoạt động không bình thường: bạn thường xuyên nhận được các tin nhắn vớ vẩn từ những người không quen biết, hoặc thỉnh thoảng các popup lạ tự động bật lên yêu cầu connect vào một trang Web nào đó.

Như đã đề cập, khi nhiễm vào máy, virus sẽ chạy file EXE chứa mã lệnh của nó. Phần lớn các virus sẽ nằm thường trực để thực hiện định kỳ các tác vụ được giao phó: lấy và gửi từng phần danh bạ, giám sát hoạt động bàn phím để đánh cắp password...

Để giám sát các tiến trình đang chạy, đầu tiên bạn hãy kích hoạt trình Task Manager bằng tổ hợp phím CTrl - Alt - Del.



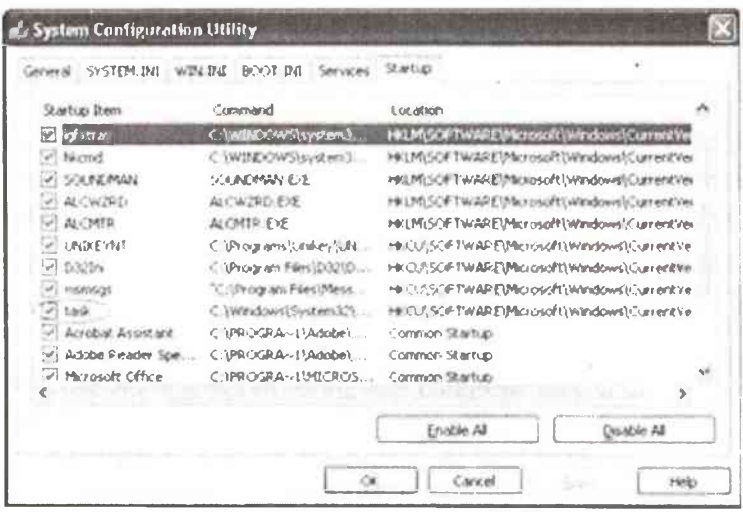
Nếu phát hiện các tập tin thực thi lạ trong thẻ Processes (ví dụ task.exe), bạn hãy chọn tập tin trong danh sách rồi nhấn nút End Process. Kế tiếp bạn dùng chức năng Search của Windows để tìm tập tin tương ứng (task.exe) trên đĩa.

Vấn đề là làm sao phân biệt tiến trình lạ với các tiến trình hợp thức trên máy? Để làm được điều này, bạn cần thường xuyên giám sát và nhớ tên chúng. Có thể bạn sẽ thấy khó chịu khi hàng ngày phải quan sát danh sách các tiến trình buồn tẻ của Windows. Tuy nhiên việc làm này là cần thiết bởi vì bạn cần biết trong nhà mình có những món đồ nào. Hôm nào có vật lạ xuất hiện, bạn phải thắc mắc ngay: Cái này ở đâu ra? Ai đã đặt nó chỗ này? Lúc nào? Với mục đích gì? Nếu không, bạn có nguy cơ gặp rắc rối, ví dụ như bị công an chất vấn vì nghi có dính líu với vụ trộm nhà bên, trong khi món đồ đó do kẻ trộm quẳng vào nhà bạn trong lúc trốn chạy...

Để tránh xóa nhầm các file thực thi hữu ích, bạn có thể tham khảo địa chỉ www.processlibrary.com. Trang Web này cung cấp cho bạn thông tin về các file thực thi EXE và DLL của Microsoft và các hãng phần mềm nổi tiếng. Nếu không tìm thấy tên tập tin cần truy vấn trên trang Web, có thể bạn

đang sử dụng phần mềm của một hãng không tên tuổi, hoặc một virus lạ đang rình rập trên máy bạn.

Thông thường các virus đều khởi động cùng Windows để tiếp tục thường trú ở các phiên làm việc tiếp theo. Để khảo sát danh sách đăng ký tự kích hoạt, bạn có thể sử dụng lệnh MsConfig từ hộp thoại Run. Chọn thẻ Startup và đối chiếu tên tập tin virus trong Windows Task Manager, bạn tiến hành xóa hộp kiểm tương ứng trong danh sách.



Trong thực tế, một số virus khi thường trú thường ngăn cản bạn thực hiện những công việc này. Sẽ tốt hơn nếu máy hoạt động trong chế độ an toàn (nhấn phím F8 khi máy vừa khởi động, chọn Safe mode with command prompt).

Để gây khó khăn cho việc khắc phục sự cố, một số virus còn vô hiệu các công cụ hệ thống như Registry Editor, Task Manager...

Khôi phục cấu hình hệ thống

Việc khôi phục cấu hình hệ thống chủ yếu thực hiện bằng Registry Editor, vốn đòi hỏi bạn một ít kiến thức về bộ đăng ký Windows Registry. Nếu chưa có kinh nghiệm, bạn sẽ gây

nguy hiểm cho máy tính. Mặt khác, nếu Registry Editor của máy đã bị khóa, bạn cũng không thể sử dụng lệnh Regedit, kể cả import từ file.REG như nhiều người thường nghĩ.

Để giúp bạn theo dõi tình trạng và phục hồi cấu hình hệ thống từ Windows Registry, phần mềm D32 Anti-virus* đã biên dịch công cụ RescueReg. Bạn chỉ cần chạy ứng dụng này, thiết lập các lựa chọn, nhấn nút Apply rồi logoff máy theo đề nghị. Sau khi Windows khởi động xong, bạn vào lại RescueReg nhấn nút Test (hoặc nhấp chuột phải trên cửa sổ ứng dụng) để kích hoạt trình đơn cảm ngữ cảnh, rồi chọn kiểm tra các chức năng đã thiết lập.

3. Không cho Spyware chiếm quyền điều khiển Home Page

Máy tính của bạn nhiễm Spyware, bạn sử dụng các phần mềm chẳng hạn như Adware SE Pro hoặc Hijackthis để quét Spyware trên máy tính của bạn. Phát hiện thấy có Web lạ chiếm quyền điều khiển trang chủ (Home Page) của bạn trong trình duyệt Internet Explorer thì bạn làm như sau:

Mở trình soạn thảo văn bản Note Pad, nhập đoạn code này vào.

```
Option Explicit
Dim WSHShell, RegKey, ValueA, Result
On Error Resume Next
Set WSHShell = CreateObject("WScript.Shell")
RegKey =
"HKEY_CURRENT_USER\Software\Policies\Microsoft\Inte
rnet Explorer\Control
Panel\"
ValueA = WSHShell.RegRead (regkey & "HomePage")
If ValueA = 0 Then 'Change Homepage is Enabled.
Result = MsgBox("Ability to Change Homepage is currently
[Enabled]." & _
```

```
vbNewLine & "Would you like to Disable?" & _
vbNewLine & "Will lock and Gray it out." & _
vbNewLine & "May need to Log-off for effect.", 36)
If Result = 6 Then 'clicked yes
WSHShell.RegWrite regkey & "HomePage", 1
End If
Else 'Change Homepage is Disabled
Result = MsgBox("Ability to Change Homepage is currently
[Disabled]." & _
vbNewLine & "Would you like to Enable?", 36)
If Result = 6 Then 'clicked yes
WshShell.RegDelete
"HKCU\Software\Policies\Microsoft\Internet
Explorer\Control
Panel\HomePage"
End If
End If
```

Lưu lại và đặt tên là DisableHomePage.vbs.

Để chạy nó, bạn nhấn chuột vào tập tin này và chọn Yes. Logoff để thay đổi có hiệu lực.

Bài 2

CÁCH PHÁT HIỆN VÀ PHÒNG CHỐNG VIRUS

1. Kinh nghiệm phòng chống virus

Khái niệm

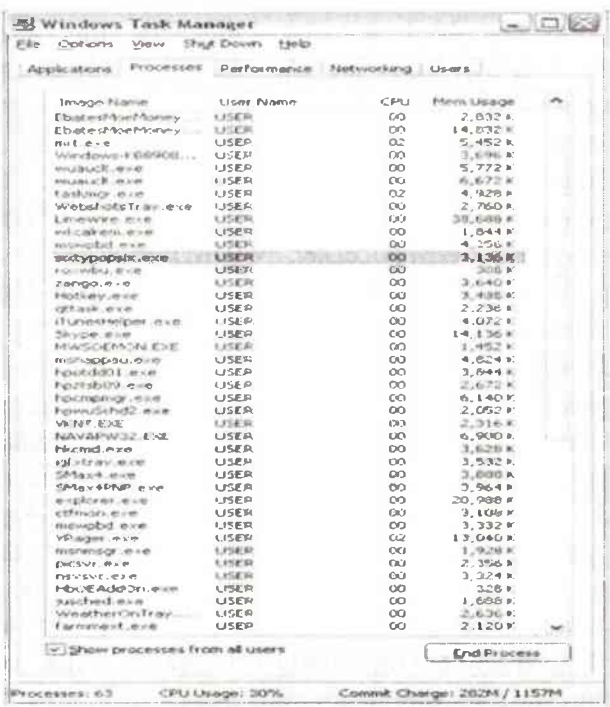
Virus: Là một đoạn mã, một chương trình nhỏ được viết ra nhằm thực hiện một việc nào đó trên máy tính bị nhiễm mà không được sự cho phép hoặc người dùng không biết. Chúng có khả năng tự nhân bản, lây lan sang các tập tin, chương trình khác trong máy tính và sang máy tính khác. Virus máy tính thường được chia thành một số loại như: File virus (Jerusalem, Cascade...) là loại virus lây vào những tập tin của một số phần mềm thường sử dụng trong hệ điều hành Windows như tập tin.com,.exe,.bat,.pif,.sys...; Boot virus (Disk Killer, Michelangelo, Stoned...) là loại virus lây nhiễm vào đoạn mã trong cung từ khởi động (boot sector) của đĩa cứng; Macro virus (W97M.Melissa, WM.NiceDay, W97M.Groov...) lây nhiễm vào tập tin trong MS. Office. Ngoài ra, còn một số loại virus khác như virus lưỡng tính (kết hợp giữa boot virus và file virus), master boot record virus...

Trojan horse: Là những chương trình được ngụy trang bằng vẻ ngoài vô hại nhưng ẩn chứa bên trong những đoạn mã nguy hiểm nhằm đánh cắp thông tin cá nhân, mở các cổng để hacker xâm nhập, biến máy tính bị nhiễm thành nguồn phát tán thư rác hoặc trở thành công cụ tấn công một Website nào đó, chẳng hạn như W32.Mimic. Không như virus và worm, Trojan horse không có khả năng tự nhân bản để lây lan, vì vậy chúng thường kết hợp với virus, worm để xâm nhập vào máy tính người dùng.

Spyware: Là phần mềm theo dõi những hoạt động của bạn trên máy tính. Chúng thu thập tất cả những thông tin cá nhân, thói quen cá nhân, thói quen lướt Web của người dùng và gửi về cho tác giả. Spyware là mối đe dọa lớn nhất đối với sự an toàn của một máy tính, một hệ thống máy tính.

Adware: Đơn giản là một dạng phần mềm quảng cáo lén lút cài đặt vào máy tính người dùng hoặc cài đặt thông qua một phần mềm miễn phí, được người dùng cho phép (nhưng không ý thức được mục đích của chúng). Tuy nhiên, chúng không dừng lại ở tính đơn giản là quảng cáo khi kết hợp với những loại virus khác nhằm tăng "hiệu quả" phá hoại.

Worm: Sâu máy tính là một loại phần mềm có sức lây lan nhanh, rộng và phổ biến nhất hiện nay. Không giống với virus thời "nguyên thủy", worm không cần đến các tập tin "mồi" để lây nhiễm. Chúng tự nhân bản và phát tán qua môi trường Internet, mạng ngang hàng, dịch vụ chia sẻ...



Nhận biết máy tính bị nhiễm virus

Sau khi xâm nhập vào hệ thống, một số máy virus lập tức thực hiện việc phá hoại. Số khác lại ẩn nấp, âm thầm lây lan sang những máy tính khác, chờ đợi giờ G để đồng loạt "tổng tấn công" khiến người dùng trở tay không kịp; điển hình như virus CIH, Melissa. Một số hiện tượng thường gặp khi máy tính nhiễm virus: Có những triệu chứng bất thường như đĩa cứng bị truy cập liên tục; hệ thống hoạt động ì ạch; một số trang Web lạ, popup quảng cáo tự động nhảy ra khi bạn làm việc. Nếu sử dụng Windows NT/2000/XP, bạn có thể tham khảo thông tin trong Windows Task Manager như CPU Usage luôn ở mức 100%, xuất hiện một số tập tin thực thi lạ trong tab Processes của Windows Task Manager...

Quét virus

Khi đã nghi ngờ hệ thống nhiễm virus, bạn cần tìm phần mềm để kiểm tra và tiêu diệt chúng. Lưu ý: phòng chống virus trước khi chúng xâm nhập vào hệ thống bao giờ cũng đơn giản hơn việc tiêu diệt chúng. Mỗi sản phẩm đều có những điểm mạnh yếu khác nhau từ miễn phí cho đến có phí để bạn tự mình chọn lựa phần mềm thích hợp.

Sau khi lựa chọn phần mềm phù hợp, bạn cần cài đặt chúng vào hệ thống. Một số virus "quỷ quái" đến mức sau khi lây nhiễm vào hệ thống, chúng ngăn chặn người dùng cài đặt hoặc khống chế luôn những phần mềm này để không phát hiện được chúng, ngăn chặn việc truy cập đến Website của nhà sản xuất. Nếu không cài đặt được ở chế độ Normal trong Windows, hãy thử cài đặt ở chế độ Safe mode. Để khởi động máy tính trong chế độ Safe mode, thực hiện như sau:

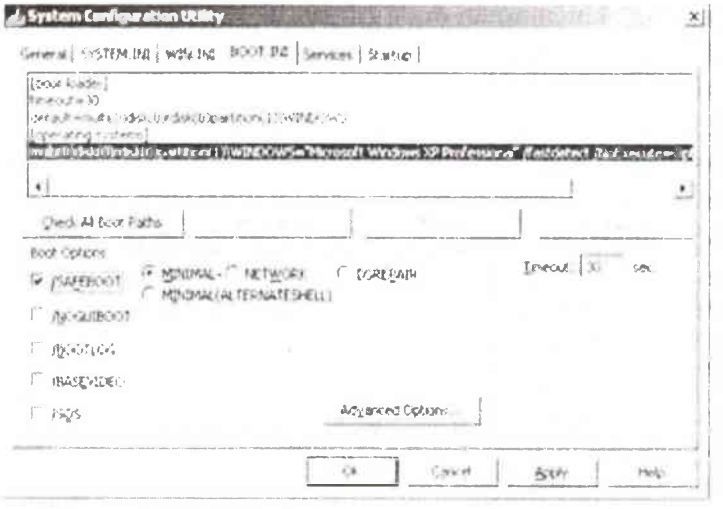
Sử dụng System Configuration Utility hoặc nhấn phím F8 trong quá trình khởi động Windows để vào chế độ Safe mode:

- Đóng tất cả các ứng dụng đang sử dụng.

- Chọn Start > Run... Gõ dòng lệnh msconfig và nhấn OK để mở cửa sổ System Configuration Utility.

- Trong tab BOOT.INI, đánh dấu tùy chọn /SAFEBOOT trong mục Boot Options.

- Nhấn OK và chọn Restart để xác nhận việc khởi động lại máy tính để vào chế độ Safe mode.



Lưu ý:

Khởi động lại máy tính trong chế độ Normal: Thực hiện các bước trên và bỏ tùy chọn /SAFEBOOT trong mục Boot Options.

Cập nhật danh sách virus. Như đã đề cập bên trên, nếu không thể truy cập đến các Website của nhà sản xuất, không thể cập nhật danh sách virus (virus definition) trực tuyến; bạn hãy tải chúng về từ máy tính khác để cập nhật.

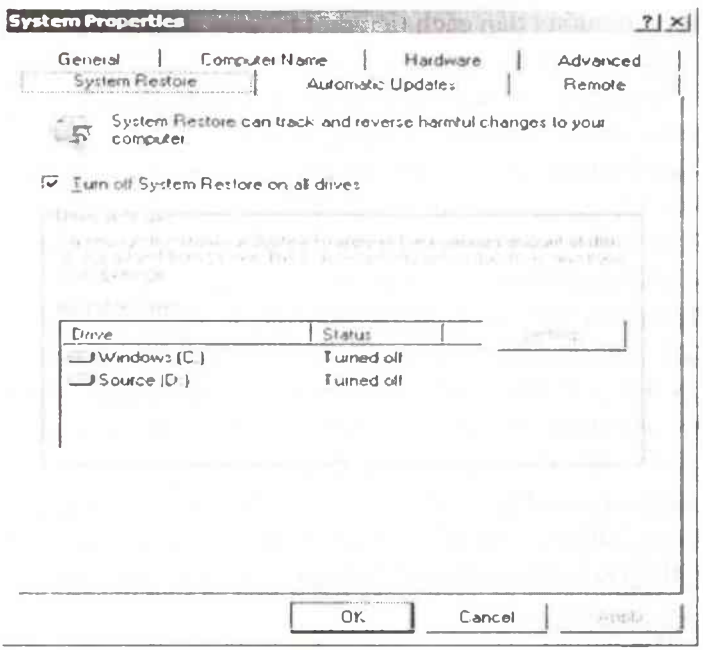
Tắt System Restore. Nếu sử dụng Windows ME hoặc XP, bạn nên tắt tính năng System Restore khi máy tính bị nhiễm virus. Mặc định trong Windows ME và XP, tính năng này được kích hoạt để giúp bạn khôi phục hệ thống khi gặp sự cố. Các phần mềm chống virus không thể quét được thư mục System Volume Information, nơi System Restore lưu trữ những tập tin, thư mục giúp khôi phục hệ thống. Vì vậy sẽ xảy ra tình trạng "tái nhiễm" virus khi System Restore phục hồi hệ thống các bản lưu trữ bị nhiễm virus.

Để tắt System Restore trong Windows XP, thực hiện như sau:

- Nhấn phải chuột trên My Computer, chọn Properties.
- Trong cửa sổ System Properties, tab System Restore, đánh dấu tùy chọn Turn off System Restore on all drivers và nhấn OK.
- Chọn Yes khi xuất hiện yêu cầu xác nhận việc này.

Nếu sử dụng Windows ME, thực hiện như sau:

- Trên màn hình Desktop, nhấn phải chuột vào biểu tượng My Computer và chọn Properties.
- Trong cửa sổ System Properties, chọn Performance\File System\Troubleshooting.
- Đánh dấu tùy chọn lên Disable System Restore và nhấn OK.
- Chọn Close và Yes để khởi động lại Windows.



Lưu ý:

Tắt tính năng System Restore đồng nghĩa với việc xóa tất cả các điểm khôi phục (restore points). Bạn hãy tạo thủ công một điểm khôi phục khi System Restore được bật trở lại.

Quét ở chế độ đầy đủ (full system scan). Thiết lập mặc định của một số chương trình phòng chống virus chỉ quét một số loại tập tin được chỉ định trước. Để chắc ăn, bạn nên thiết lập "full system scan" để máy tính được kiểm tra đầy đủ nhất. Một số lưu ý trong quá trình quét:

- Nếu gặp thông báo lỗi phần mềm không thể xóa được virus hoặc một tập tin nào đó của virus. Bạn hãy khởi động lại máy tính ở chế độ Safe mode và tiếp tục việc kiểm tra.

- Kết thúc quá trình quét, chương trình sẽ đưa ra báo cáo tổng kết những virus được phát hiện và cách xử lý chúng. Nếu chương trình không thể diệt được một vài loại virus nào đó, bạn thử diệt chúng một cách thủ công. Sử dụng công cụ tìm kiếm với từ khóa là tên virus đó, bạn sẽ tìm thấy những thông tin hướng dẫn cách tiêu diệt tại một số Website nhà sản xuất phần mềm phòng chống virus.

- Sau khi khởi động lại Windows trong chế độ Normal, nếu gặp thông báo lỗi tương tự như: "Windows cannot find [FILE NAME]. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search" thì máy tính của bạn vẫn đang bị ảnh hưởng của virus - mặc dù chúng đã được diệt. Ví dụ: với virus W32.Lecna.A, bạn sẽ gặp thông báo lỗi không tìm thấy tập tin iexplore.exe. Đây là những "tàn tích" còn sót lại của virus W32.Lecna.A dù chúng đã bị diệt. Để xóa chúng, bạn cần tìm và xóa những khóa do virus này thêm vào trong Registry. Người dùng nên sao lưu Registry trước khi bạn can thiệp đến chúng.

Chọn Start\ Run để mở cửa sổ DOS Prompt; gõ vào lệnh "regedit" để mở cửa sổ Registry Editor. Nếu gặp thông báo lỗi "Registry editing has been disable by your administrator" ta làm như sau:

- Tìm và xóa các khóa có liên quan đến spyware trong các nhánh sau:

KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Xóa khoá "iexplore.exe" = "iexplore.exe" ở khung bên phải.

HKEY_LOCAL_MACHINE\Software\Microsoft\Current NetInf. Xóa khóa "hostid" = "[RANDOM NUMBER]" và "pid" = "[ENCRYPTED DATA]"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Control\Lsa. Xóa khóa "forceguest" = "0"

- Thoát khỏi Registry. Editor và khởi động lại máy tính.

Cập nhật các bản sửa lỗi cho HĐH, phần mềm. Một số virus như W32.Blaster.Worm thường khai thác lỗ hổng trong dịch vụ Remote Procedure Call của HĐH Windows NT/2000/XP để phá hoại. Nếu sử dụng các phần mềm của Microsoft, bạn có thể cập nhật bản sửa lỗi từ http://www.microsoft.com/ tránh tình trạng tái nhiễm sau khi quét.

2. Phòng chống virus

Một mô hình phòng thủ hiệu quả và chắc chắn là thiết lập nhiều tuyến phòng vệ, nào là phòng vệ bên ngoài với tường lửa cứng (tích hợp trong router), tường lửa mềm (phần mềm trong máy tính), phần mềm chống virus, phần mềm chống spyware... rồi phải cập nhật bản sửa lỗi những lỗ hổng bảo mật của hệ điều hành và của những phần mềm cài đặt trên máy tính. Tuy nhiên, nhiều người dùng không đủ khả năng (tài chính, kiến thức) để thực hiện điều này. Vậy tuyến phòng vệ nào là cần thiết và phù hợp?

Tường lửa (firewall)

Kiểm soát dữ liệu ra vào máy tính của bạn và cảnh báo những hành vi đáng ngờ; là công cụ bảo vệ máy tính chống lại sự xâm nhập bất hợp pháp bằng cách quản lý toàn bộ các cổng của máy tính khi kết nối với môi trường bên ngoài (mạng Lan, Internet...). Tường lửa có sẵn trong Windows XP chỉ giám sát được dòng dữ liệu vào máy tính chứ không kiểm soát được dòng dữ liệu ra khỏi máy tính. Chúng ta thường ít có kinh nghiệm về bảo mật và virus, tường lửa sẽ không phát huy tác dụng vì người dùng không thể xử lý các cảnh báo.

Hơn nữa, việc cài đặt tường lửa sẽ làm cho máy tính hoạt động chậm đi.

Sử dụng chương trình chống virus

Người dùng có thể sử dụng một hay nhiều chương trình diệt virus cài vào máy nhằm bảo vệ máy tính, hiện nay hầu hết các chương trình diệt virus (Anti-Virus) đều có kết hợp tính năng tự động bảo vệ (Auto Protect) chương trình sẽ chạy thường trực cùng với Windows, khi phát hiện thấy có sự xâm nhập của virus hoặc khi phát hiện ra virus, ngay lập tức nó sẽ cảnh báo cho người dùng và đưa ra các giải pháp xử lý như khoá file, di chuyển đến vùng cách ly hoặc có thể xoá file mà chương trình nghi ngờ có virus.

Ghi chú:

- Thường xuyên cập nhật danh sách nhận dạng virus (virus definitions) sẽ giúp phần mềm làm việc hiệu quả hơn.

- Với các virus có xuất xứ ở Việt Nam, người dùng nên sử dụng chương trình Bkav để diệt sẽ hiệu quả hơn và cũng dễ sử dụng hơn.

Cập nhật bản sửa lỗi

Lỗ hổng bảo mật của phần mềm là "điểm yếu" virus lợi dụng để xâm nhập vào máy tính của bạn. Thật không may là những điểm yếu này lại khá nhiều và người dùng cũng không quan tâm đến việc này. Hãy giữ cho hệ điều hành, trình duyệt Web và phần mềm chống virus luôn được cập nhật bằng tính năng tự động cập nhật (auto update); nếu tính năng này không hoạt động (do sử dụng bản quyền bất hợp pháp), hãy cố gắng tải về từ Website của nhà sản xuất bằng cách thủ công. Bạn sẽ tăng cường tính năng phòng thủ hiệu quả cho hệ thống và tránh tình trạng virus "tái nhiễm" sau khi diệt.

Trình duyệt an toàn hơn

Nếu so sánh, bạn dễ dàng nhận thấy Internet Explorer là trình duyệt Web có nhiều lỗ hổng bảo mật nhất dù Microsoft

liên tục đưa ra những bản sửa lỗi. Sử dụng những trình duyệt thay thế như Mozilla FireFox, Opera, Chorme... hoặc cài đặt thêm một trong những trình duyệt này để tận dụng những ưu điểm của mỗi phần mềm và tăng tính bảo mật khi lướt Web.

Suy nghĩ kỹ trước khi cài đặt

Nhiều bạn đọc thích táy máy, tải về và cài đặt nhiều phần mềm khác nhau để thử nghiệm. Điều này dẫn đến việc chúng ta không kiểm soát được những phần mềm sẽ làm gì trên máy tính. Thực tế cho thấy cài đặt quá nhiều phần mềm sẽ "bổ sung" thêm những lỗ hổng bảo mật mới, tạo điều kiện cho tin tặc dễ dàng xâm nhập vào máy tính của bạn, góp phần làm đổ vỡ hệ thống phòng thủ mà bạn dày công tạo dựng.

Sử dụng máy tính với quyền User

Với Windows NT/2000/XP, việc đăng nhập và sử dụng máy tính với tài khoản mặc định thuộc nhóm Administrators là một hành động mạo hiểm vì virus sẽ được "thừa hưởng" quyền hạn của tài khoản này khi xâm nhập vào hệ thống, máy tính của bạn có thể trở thành zombie và tấn công máy tính khác. Tài khoản thuộc nhóm Users sẽ không được phép thay đổi các thiết lập liên quan đến hệ thống, bạn sẽ tránh được nhiều nguy cơ bị phá hoại và những phiền toái, cả khi virus xâm nhập vào máy tính.

Sử dụng máy tính với quyền User sẽ khiến người dùng gặp nhiều khó khăn trong quá trình cài đặt ứng dụng và thực hiện một số tác vụ liên quan đến hệ thống nhưng chúng tôi vẫn khuyến khích bạn đọc tự giới hạn quyền sử dụng trên máy tính của mình. Hơn nữa, bạn không cần cài thêm phần mềm phòng chống spyware. Tài nguyên hệ thống không bị chiếm dụng, máy tính hoạt động sẽ nhanh hơn.

Sao lưu hệ thống

Bạn có thể bỏ qua bước này nếu tin rằng máy tính của mình luôn chạy tốt. Hãy thực hiện việc sao lưu vào thời điểm máy tính hoạt động ổn định, đã cài đặt những phần mềm cần

thiết. Bạn có thể đưa hệ thống trở lại trạng thái đã sao lưu chỉ với vài thao tác đơn giản khi cần thiết. Để tạo tập tin ảnh của phân vùng đĩa cứng, bạn có thể sử dụng một trong những phần mềm như: Drive Image của PowerQuest, Norton Ghost của Symantec, DriveWorks của V Communications, Acronis True Image của Acronis...

Việc sao lưu sẽ rất hữu ích với những bạn đọc thích táy máy, thử nghiệm tính năng phần mềm. Bạn sẽ tiết kiệm rất nhiều thời gian thay vì phải đi xử lý những sự cố do virus gây ra hoặc phải cài lại HĐH và những phần mềm cần thiết.

3. Phòng chống "điệp viên" Keylogger

Vào một ngày đẹp trời, bạn mở hộp thư điện tử của mình nhưng mở hoài không được vì thông báo đăng nhập sai password cứ hiện ra. Chắc bạn sẽ rất ngạc nhiên vì mình đã gõ đúng password kia mà. Vậy là password của bạn đã bị người khác biết mặc dù bạn rất cẩn thận. Tại sao password bạn lại bị mất?

Trong số những cách lấy password, cách cài chương trình Keylogger lên máy tính là một phương pháp khá đơn giản. Vậy chương trình Keylogger là gì? Hiểu một cách đơn giản đó là chương trình ghi lại những thao tác sử dụng bàn phím. Một số chương trình mới có thể ghi lại cả những hình ảnh trang Web mà bạn sử dụng. Chương trình Keylogger được dùng để đánh cắp những thông tin cá nhân, ví dụ như tài khoản cá nhân ở ngân hàng, công ty...

Cảnh giác với Keylogger

Hiện nay, việc sử dụng Keylogger khá phổ biến ở Việt Nam. Các chương trình này được truyền nhau thông qua các diễn đàn (forum) trên mạng, có cả hướng dẫn chi tiết nên việc sử dụng rất dễ dàng. Đối tượng sử dụng thường là sinh viên, học sinh. Keylogger thường được cài ở dịch vụ Internet công cộng hoặc trường học. Sau khi cài chương trình Keylogger, người cài đặt sẽ nhận được rất nhiều thông tin và cũng phải

mất khá nhiều thời gian để lọc những thông tin cần thiết. Thông thường, người cài đặt Keylogger sẽ có được tài khoản (account) từ hộp thư điện tử, qua chat (thường là Yahoo! Messenger), khi chơi game online (MU, Gunbound...), điện thoại Internet và đôi khi là những tài khoản thẻ tín dụng...

Nếu bạn không cẩn thận khi dùng chung máy tính hoặc cho một người nào đó mượn máy, bạn sẽ có nguy cơ bị lấy cắp thông tin cá nhân. Ngoài ra, máy tính của bạn cũng có thể bị cài Keylogger một cách gián tiếp qua việc nhận file đính kèm có cài chương trình Keylogger. Do những file này kèm theo những thông điệp hấp dẫn khiến bạn tò mò mở ra xem. Phổ biến nhất vẫn là trường hợp bạn tham gia vào các forum. Hiện nay, trên các forum thường cung cấp những phần mềm "miễn phí" (thường là phải mua mới được sử dụng đầy đủ). Do đó, các forum này có sức hút rất lớn nên người tải file về mất cảnh giác.

Bạn tham gia vào một forum, thấy một thông báo đây là những bản vá lỗi mới nhất của Windows và cho bạn đường link để download (đường link này không xuất phát từ trang chủ của Microsoft). Bạn vô tư download chúng về và sử dụng mà không nghĩ rằng mình có thể đã bị nhiễm Keylogger.

Nhận dạng và tiêu diệt Keylogger

Về cách nhận dạng và tiêu diệt Keylogger, một trong những cách phòng chống hiệu quả nhất là dùng các phần mềm có chức năng tường lửa (Personal firewall của McAfee, AntiHacker của Kaspersky, Hacker Smacker của Farstone...) và kết hợp các chương trình diệt spyware (Ad-Aware professional SE của Lavasoft, Spywepper của Webroot...). Những chương trình này sẽ rất hữu ích.

Theo cơ chế hoạt động của Keylogger là sau khi ghi file log tới kích thước là bao nhiêu (do chủ nhân quy định) nó sẽ gửi qua mail tới chủ nhân của nó. Các phần mềm có chức năng tường lửa sẽ chặn lại, hỏi chúng ta có cho phép chương trình này thực hiện việc gửi file không.

Ví dụ: Tên file thực thi của một chương trình Keylogger là akl.exe. Bạn nên xem kỹ chi tiết của các ứng dụng Internet trước khi cấp quyền cho nó chạy khi sử dụng firewall. Nếu thấy không biết gì về chương trình đó thì không nên cấp quyền (block).

Tiếp theo thì bạn nên chạy các chương trình diệt spyware có uy tín để phát hiện ra chúng. Trên thực tế, sau khi cài Keylogger vào máy và chạy chương trình Ad-Aware professional SE thì sẽ phát hiện đầy đủ các chương trình Keylogger đã cài.

Một số lời khuyên:

- Khi nhận những file lạ, bạn nên cẩn thận xem mình có biết nó không và có cần không, nếu không thì nên bỏ qua.

- Khi bạn tải những file chương trình từ Internet về, cần chú ý một số thông tin về nguồn gốc của file đó và hãy tải file trực tiếp từ trang chủ. Tránh trường hợp bạn tải một file ở những địa chỉ mà bạn không biết thông tin gì cả. Lúc này nguy cơ bị nhiễm rất cao.

- Đôi khi cũng nên cẩn thận khi nhận file từ bạn bè vì biết đâu trong các file đó có cài chương trình Keylogger thì sao. Nếu bạn hay sử dụng dịch vụ Internet công cộng, tốt nhất không nên sử dụng những tài khoản cá nhân quan trọng như thẻ tín dụng.

Các cách phòng chống trên sẽ không bảo đảm an toàn cho bạn 100% (vì có một số chương trình Keylogger mới có khả năng vượt qua firewall), nhưng sẽ giúp bạn hạn chế rất lớn khả năng bị cài Keylogger lên máy của mình, giúp giữ an toàn những thông tin cá nhân.

4. Man In The Middle và phương pháp phòng chống

Để chẩn đoán và khắc phục sự cố mạng, các nhà quản trị hệ thống thường sử dụng các chương trình phân tích gói tin như Network Monitor, Sniffer Pro... Tuy nhiên, đây cũng là những công cụ thường được hacker sử dụng để "nghe lén" hệ

thống mạng và lấy cắp các thông tin nhạy cảm như username (tên đăng nhập), password (mật mã đăng nhập) hay các thông tin quan trọng khác.

Để đối phó với mối nguy hiểm này, chúng ta sử dụng thiết bị chuyển mạch như switch để bảo đảm các gói tin chỉ được truyền đến đúng máy tính có địa chỉ thích hợp chứ không truyền cho tất cả các máy trong hệ thống mạng nội bộ (LAN) mà người ta thường gọi bằng thuật ngữ truyền thông broadcast.

Nhưng thật không may, ngay cả với mạng dùng switch chúng ta vẫn có thể bị tấn công bởi các chương trình phân tích gói tin mạnh như: dsniff, snort hay ettercap (chương trình được mệnh danh là Lord Of The TokenRing). Ettercap có thể giả danh địa chỉ MAC của card mạng máy tính bị tấn công, thay vì gói tin dược truyền đến máy tính cần đến thì nó lại được chuyển đến máy tính có cài đặt ettercap trước rồi sau đó mới truyền đến máy tính đích. Đây là một dạng tấn công rất nguy hiểm được gọi là Man In The Middle, trong trường hợp này phiên làm việc giữa máy gửi và máy nhận vẫn diễn ra bình thường nên người sử dụng không hề hay biết mình đang bị tấn công, giống như trường hợp bị đặt máy nghe lén mà chúng ta thường gặp trên phim ảnh. Những chương trình dạng này thường được gọi là sniffer.

Trong quá trình tư vấn cho một số công ty cũng như quá trình giảng dạy, tôi nhận thấy đây là một trong những trường hợp tấn công thường xảy ra nhất và do chính người sử dụng trong mạng nội bộ gây ra (hoặc những người có khả năng tương tác trực tiếp với hệ thống).

Những nhà quản trị hệ thống hay người chịu trách nhiệm về vấn đề an toàn cho dữ liệu trong quá trình truyền thông cần phải nắm rõ cả hai khía cạnh của vấn đề: cách tấn công và giải pháp phòng ngừa, nói theo ngôn ngữ binh pháp là biết người biết ta, trăm trận trăm thắng.

Man In The Middle với Ettercap

Bạn có thể tải ettercap từ Website http://rpmfind.net hay http://ettercap.sourceforge.net, và tiến hành cài đặt trên một máy chạy hệ điều hành Linux như sau (ettercap cũng có phiên bản cho Windows XP/2000):

#rpm –ivh ettercap-0.6.9-1.7.2.i386

Nếu tập tin ettercap là tập tin nén dạng tar thì hãy giải nén bằng lệnh tar và tiến hành cài đặt bằng các dòng lệnh:

#tar –zxvf ettercap-0.6.9-1.7.2.i386.tar

#cd ettercap-0.6.9-1.7.2

#./configure && make && make install

Sau khi cài đặt hoàn tất, ta khởi động quá trình phân tích gói tin bằng cách gõ lệnh ettercap (ở cửa sổ console), chọn card mạng muốn kiểm tra. Sau khi kiểm tra xong, màn hình ettercap sẽ xuất hiện danh sách các máy tính đang hoạt động trong mạng được chia làm hai phần nguồn (bên trái) và đích (bên phải).

Để lưu giữ được nhiều thông tin nhất, ta có thể để trống khung nguồn và chọn đích là default gateway trên hệ thống của mình, nghĩa là bạn sẽ đứng giữa thiết bị dùng để truy cập các lớp mạng khác (thông thường là mạng Internet) và các máy trạm trong mạng. Nhấn phím A để bắt đầu "bắt" các gói tin, chỉ sau một thời gian ngắn bạn sẽ thấy rất nhiều thông tin xuất hiện trên màn hình, trong đó có những thông tin nhạy cảm như username, password của các ứng dụng quan trọng được truyền đi mà không được mã hóa như pop3, ftp...

Thậm chí, bạn có thể bắt giữ được cả những tin nhắn của Y!Messenger bằng cách chọn chỉ mục tương ứng rồi nhấn Enter. Hoặc khi người sử dụng đang xem các tập tin trên Internet hay tải về thông qua giao thức http, bạn cũng có thể bắt giữ bằng cách nhấn phím P và chọn plug-in thứ 13. Bạn có thể lưu các thông tin bắt được thành một tập tin bằng cách nhấn phím L.

Giải pháp phòng chống

Qua một số ví dụ trên, chúng ta nhận thấy các thông tin quan trọng và những tập tin riêng tư có thể bị đánh cắp khá dễ dàng. Để phòng ngừa các trường hợp như vậy, chúng ta không nên tiến hành các hình thức chứng thực username và password dưới dạng văn bản đơn thuần (không mã hóa) mà nên mã hóa chúng bằng IPSec hay SSL. Tuy nhiên, không phải lúc nào chúng ta cũng có thể thực hiện được các giải pháp này và cũng không phải lúc nào các giải pháp đó cũng mang lại hiệu quả tốt nhất (vẫn có thể bị các chương trình như dsniff hay ettercap bẻ khoá). Do đó, trong vai trò quản trị mạng, cách tốt nhất là bạn thường xuyên giám sát các hành động bất thường trong hệ thống của mình để đưa ra hành động thích hợp.

Như trong trường hợp ở trên, hệ thống bị tấn công do cơ chế giả danh ARP (hay còn gọi bằng thuật ngữ "spoofing arp") - một giao thức dùng để phân giải địa chỉ vật lý MAC của máy tính. Ta có thể dùng arpwatch giám sát các thông tin arp trong hệ thống để phát hiện khi bị tấn công bằng các phương pháp spoofing arp hay sniffer. Hoặc bạn tiến hành cài đặt các hệ thống IDS như Snort, GFI để phát hiện các hành động bất thường trên mạng.

Thực tế, bạn có thể dùng chính etteracp để dò tìm ra chính nó cũng như các chương trình sniffer khác trên mạng theo phương pháp "dĩ độc trị độc". Ettercap có hai plug-in rất hữu ích, một dùng để tìm kiếm các máy tính chạy chương trình ettercap khác trên mạng và plug-in còn lại dùng để phát hiện các chương trình sniffer khả nghi khác. Ví dụ, nếu nghi ngờ có ai đó đang "nghe lén" trên mạng, bạn khởi động ettercap và nhấn phím P, sau đó chọn plug-in đầu tiên sẽ tìm ra các máy đang chạy ettercap. Còn khi đối phương sử dụng các chương trình khác như dsniff, ta có thể dò tìm thông qua plug-in thứ 15 là arpcop, lúc đó một cửa sổ mới sẽ hiển thị những máy tính đang chạy các chương trình spoofing arp trên mạng.

Khi xác nhận được đối tượng, ta có thể tiến hành cô lập máy tính này khỏi mạng ngay lập tức bằng cách chọn P và chọn plug-in thứ 23 tên là leech và sau đó chọn Yes, nhấn Enter. Một số người quản trị hệ thống còn dùng ettercap để phát hiện các máy bị nhiễm virus đang phát tán trên mạng rồi cô lập chúng bằng leech, sau đó diệt bằng các chương trình chống virus rất hiệu quả.

Cách tốt nhất để giữ an toàn cho hệ thống mạng của mình là nên thường xuyên giám sát hệ thống cũng như có các chính sách để ngăn ngừa các trường hợp gây hại vô tình hay cố ý của người sử dụng. Thông qua việc thực hiện các chính sách hợp lý, chúng ta có thể quy định những chương trình không nên sử dụng cũng như các hành động bị nghiêm cấm như tiến hành thao tác phân tích gói tin, trừ khi phục vụ cho mục đích đặc biệt để xử lý sự cố mạng. Hy vọng bài viết này sẽ giúp bạn có được những biện pháp thích hợp để phòng chống và giảm thiểu tối đa những thiệt hại cho mạng.

5. Firewall phòng chống hacker

Tổng quan về tường lửa

- Hiện nay trên thị trường có hai loại tường lửa: ủy nhiệm ứng dụng (application proxies) và cổng lọc gói tin (packet filtering getways).

Nhận dạng tường lửa

Hầu hết thì các tường lửa thường có một số dạng đặc trưng, chỉ cần thực hiện một số thao tác như quét cổng và firewalking và lấy banner (thông tin giới thiệu - tiêu đề) là hacker có thể xác định được loại tường lửa, phiên bản và quy luật của chúng.

Quét trực tiếp - kỹ thuật lộ liễu

+ Cách tiến hành:

- Một cách đơn giản nhất để tìm ra tường lửa là quét các cổng mặc định. Một vài tường lửa trên thị trường tự nhận

dạng mình bằng việc quét cổng - ta chỉ cần biết những cổng nào cần quét. Ví dụ như Proxy Sever của Microsoft nghe các cổng TCP 1080 và 1745 etc...

Như vậy để tìm tường lửa ta sử dụng nmap đơn giản như sau:

Nmap -n -vv -p0 -p256,1080,1745 192.168.50.1 -60.250

Từ những kẻ tấn công vụng về cho đến những kẻ sành sỏi đều dùng phương pháp quét diện rộng đối với mạng làm việc của bạn để nhận diện tường lửa. Tuy nhiên, những hacker nguy hiểm sẽ tiến hành công việc quét càng thầm lặng, càng kín đáo càng tốt. Các hacker có thể dùng nhiều kĩ thuật để thoát khỏi sự phát hiện của chúng ta, bao gồm ping ngẫu nhiên... Các hệ thống dò xâm nhập (IDS - Intruction Detection System) không thể phát hiện những hành động quét cổng áp dụng những kĩ thuật tinh vi để lẩn tránh bởi chúng được ngầm định lập cấu hình chỉ để nghe những hành động quét cổng lộ liễu nhất mà thôi.

Trừ khi chúng ta có những thiết lập đúng đắn cho IDS, nếu không việc quét cổng sẽ diễn ra rất âm thầm và nhanh chóng. Chúng ta hoàn toàn có thể tạo ra những hành vi quét cổng như vậy khi sử dụng những đoạn script có sẵn trên nhiều trang Web.

+ Cách đối phó:

Nếu dùng RealSecure 3.0 thì có thể làm như sau:

- Để RealSecure 3.0 có thể phát hiện ra các hành vi quét cổng, chúng ta cần phải nâng cao tính nhạy cảm của nó, có thể sử dụng những thay đổi sau:

- Chọn Network Engine Policy.

- Tìm "Port Scan " và chọn nút Options.

- Sửa Ports thành 5 ports.

- Sửa Delta thành 60 seconds.

- Để ngăn chặn việc quét cổng tường lửa từ Internet, ta cần phải khóa các cổng này ở những router đứng trước Firewall. Trong trường hợp những thiết bị này do ISP quản lý, ta phải liên hệ với họ.

Lần theo tuyến (Route tracking)

- Sử dụng chương trình traceroute để nhận diện tượng lửa trên một mạng làm việc là một phương pháp âm thầm và không khéo hơn. Chúng ta có thể sử dụng traceroute trên môi trường UNIX và tracert.exe trên môi trường Windows NT để tìm đường đến mục tiêu. Traceroute của LINUX có khóa lựa chọn -I để thực hiện việc lần theo tuyến bằng cách gửi đi các gói ICMP:

```
[vtt]$ traceroute -I 192.168.51.100
traceroute to 192.168.51.101 (192.168.51.100), 30 hops
max, 40 byte packages
1 attack-gw (192.168.50.21) 5.801 ms 5.105 ms 5.445 ms
2 gw1.smallisp.net (192.168.51.1)
....
15 192.168.51.101 (192.168.51.100)
```

Lấy banner (banner grabbing)

- Quét cổng là một biện pháp rất hiệu quả trong việc xác định firewall nhưng chỉ có Checkpoint và Microsoft nghe trên các cổng ngầm định, còn hầu hết các tường lửa thì không như vậy, do đó chúng ta cần phải suy diễn thêm. Nhiều tường lửa phổ biến thường thông báo sự có mặt của mình mỗi khi có kết nối tới chúng. Bằng việc kết nối tới một địa chỉ nào đó, ta có thể biết được chức năng hoạt động, loại và phiên bản tường lửa. Ví dụ khi chúng ta dùng chương trình netcat để kết nối tới một máy tính nghi ngờ có tường lửa qua cổng 21 ta có thể thấy một số thông tin thú vị như sau:

```
c:\>nc -v -n 192.168.51.129 21
(unknown) [192.168.51.129] 21 (?) open
220 Secure Gateway FTP sever ready
```

- Dòng thông báo (banner) "Secure Gateway FTP sever ready" là dấu hiệu của một loại tường lửa cũ của Eagle Raptor. Để chắc chắn hơn chúng ta có thể kết nối tới cổng 23 (telnet):

```
C:\>nc -v -n 192.168.51.129 23
(unknown) [192.168.51.129] 23 (?) open
```

Eagle Secure Gateway.

Hostname:

- Cuối cùng nếu vẫn chưa chắc chắn ta có thể sử dụng netcat với cổng 25 (SMTP).

C:\>nc -v -n 192.168.51.129 25

(unknown) [192.168.51.129] 25 (?) open

421 fw3.acme.com Sorry, the firewall does not provide mail service to you.

- Với những thông tin và giá trị thu thập được từ banner, hacker có thể khai thác các điểm yếu của Firewall (đã được phát hiện ra từ trước) để tấn công.

Cách đối phó

Để đối phó thì chúng ta cần phải giảm thiểu thông tin banner, điều này phụ thuộc rất nhiều vào các nhà cung cấp Firewall. Ta có thể ngăn chặn việc bị lộ quá nhiều thông tin tường lửa bằng cách thường xuyên sửa đổi các file cấu hình banner. Điều này thì các bạn nên tham khảo thêm từ các nhà cung cấp dịch vụ.

Nhận diện cổng (port identification)

Một vài Firewall có "dấu hiệu nhận dạng " có thể được dùng để phân biệt với các loại tường lửa khác bằng cách hiện ra một số các con số.

Ví dụ như CheckPoint Firewall khi ta kết nối tới cổng TCP 257 quản lý SNMP. Sự hiện diện của các cổng từ 256 tới 259 trên hệ thống chính là dấu hiệu báo trước sự có mặt của CheckPoint Firewall-1, ta có thể thử như sau:

[vtt]# nc -v -n 192.168.51.1 257

(unknown) [192.168.51.1] 257 (?) open

30000003

[vtt]# nc -v -n 172.29.11. 191 257

(unknown) [172.29.11. 191] 257 (?) open

30000000

6. Những phương thức lây lan của malware và cách phòng chống

Bạn thường không hiểu tại sao virus lại có thể nhiễm vào máy mình mặc dù đã cài đặt các Anti-virus và rất cẩn thận. Vậy chúng đã lây lan qua những con đường nào và phải phòng tránh ra sao?

Lây lan qua USB

Virus thường tạo ra một tệp autorun.inf trong thư mục gốc của USB hay đĩa mềm của bạn. Khi phát hiện có thiết bị lưu trữ mới được cắm vào (USB, CD, Floppy Disk...), Windows mặc nhiên sẽ kiểm tra tệp autorun.inf nằm trong đó, nếu có nó sẽ tự động thực hiện các dòng lệnh theo cấu trúc được sắp xếp trước.

Tệp autorun.inf thông thường sẽ có nội dung:

[autorun]

open=virus.exe

icon=diskicon.ico

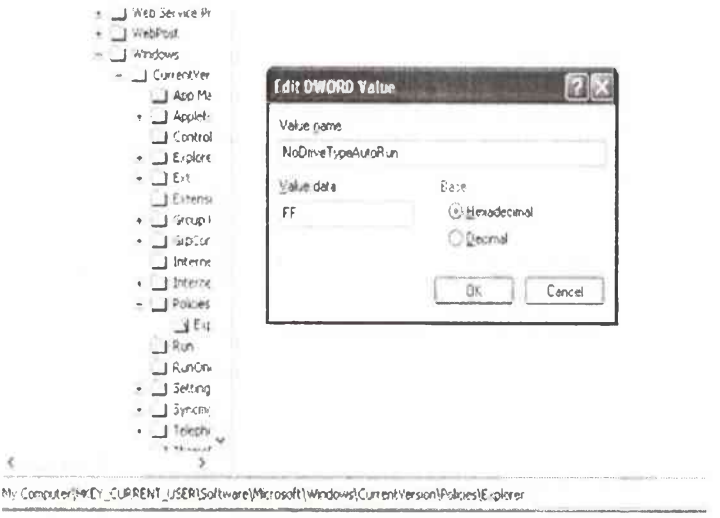
Câu lệnh trên sẽ tự động thực thi một tệp có tên là virus.exe (tệp virus) và thiết lập icon của ổ đĩa là diskicon.ico. Những tệp này đều nằm ở thư mục gốc của thiết bị lưu trữ. Giả sử ổ USB của bạn là ổ G thì tệp đó sẽ nằm ở G:\virus.exe. Khi cắm USB vào, máy tính sẽ mặc nhiên chạy tệp G:\virus.exe nếu chưa được config đúng cách.

Cách ngăn chặn

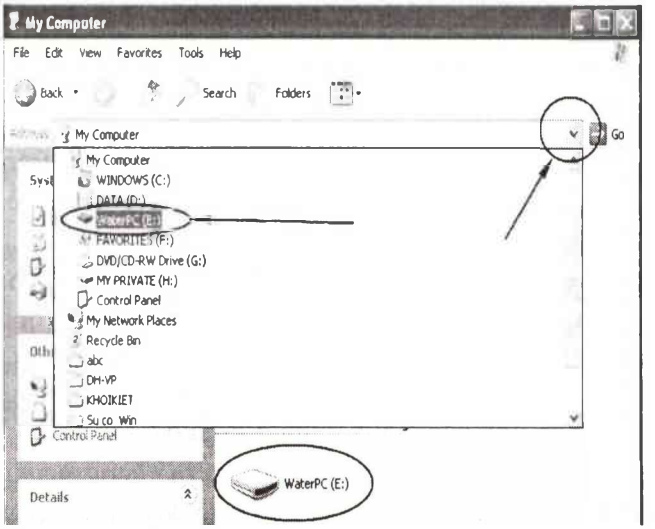
Để disable chế độ tự động autorun, bạn vào Start\Run, gõ regedit và ấn Ok, bên tay trái, bạn truy cập vào khóa:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

Bên tay phải bạn kích đúp vào biến NoDriveTypeAutoRun và chỉnh lại thành FF để vô hiệu hóa autorun của tất cả các ổ đĩa. Nhấp OK và restart lại máy để có hiệu lực.



Tuy nhiên cách này chỉ hạn chế được tính năng tự động của tệp autorun.inf. Nếu trong USB có tệp autorun mà bạn kích đúp vào ổ thì window vẫn mặc nhiên chạy nó. Vì vậy bạn nên dùng các phương thức khác để truy cập vào USB mà không cần kích đúp, cũng như nên sửa thói quen truy cập gây hại này và thay vào đó là mở USB bằng thanh địa chỉ Address.



Để mở ổ USB (là ổ E:) bạn tìm tên ổ trong thanh địa chỉ và mở ổ, tránh mở trực tiếp từ cửa sổ Windows Explorer.

Nếu phát hiện trong USB có virus (hay tệp autorun), bạn có thể vào cmd và gõ hai lệnh sau để xóa (phải gõ cả hai lệnh theo tuần tự):

attrib -s -h [ổ đĩa:\]autorun.inf

del [ổ đĩa:\]autorun.inf

Lệnh đầu dùng để gỡ bỏ thuộc tính ẩn của autorun.inf, lệnh sau có tác dụng xóa autorun.inf. Nếu bạn chỉ dùng lệnh del thì cmd sẽ không phát hiện ra autorun.inf và lệnh sẽ không được thực thi.

Lây lan qua Yahoo! Messenger

Những loại virus kiểu này có một thời rất được thịnh hành ở Việt Nam vì khả năng lây lan với tốc độ cao của nó. Thỉnh thoảng bạn gặp một vài tin nhắn rất hấp dẫn của bạn bè gửi cho và sau đó là đường link đến một trang Web lạ nào đó.

Và nếu ai không cảnh giác sẽ vô tình click vào, đột nhiên cửa sổ IE của bạn bị đơ cứng lại trong vài giây. Virus đã được tự động down về máy và kích hoạt, chỉ vài giây sau bạn sẽ gửi đi những tin nhắn vô tình gây hại cho người khác giống như bạn bè của bạn.

Cách ngăn chặn

Virus dạng này sử dụng một đoạn VBScript gắn trên link Web được gửi có tác dụng tự động download file exe về máy và kích hoạt.

- Hiện nay phần lớn các trình duyệt đều không hỗ trợ VbScript, chỉ có Internet Explorer (trình duyệt mặc định của Windows) từ bản 6 trở xuống là vẫn hỗ trợ loại mã này. Nên tốt nhất bạn nên tải bản IE 6 trở lên hoặc sử dụng các trình duyệt khác có tính bảo mật hơn như: FireFox, Opera...

- Ngoài ra trước mỗi link lạ, bạn có thể xem qua source của nó để khẳng định nó không có gì nguy hiểm, bạn có thể

sử dụng các trang xem trước mã html. Nên chú ý các từ khóa đặc biệt như: vbscript, exe... Tuy nhiên phương pháp này tỏ ra không hiệu quả vì trong trang Web đó có thể embed thêm một số url khác, và sau một loạt các url embed mới đến link của trang Web chứa script.

Lây lan qua trình duyệt truy cập Web

Giống như cách lây lan qua Yahoo! Messenger, khi bạn truy cập vào đường link (một trang Web) nào đó, bạn sẽ vô tình vào phải các trang Web bị nhiễm mã độc (dạng VBScript). Cách giải quyết giống như trên, sử dụng các trình duyệt có tính bảo mật tốt không hỗ trợ vbscript để truy cập Web.

Lây lan qua E-mail, Outlook Express

Tiện ích E-mail thì chắc không ai còn lạ gì rồi, nhất là nếu bạn hay check mail, công việc khiến bạn phải tiếp xúc với E-mail nhiều. Bạn rất khó phân biệt được E-mail nào có nội dung tốt, xấu hay chỉ là spam. Hacker đã lợi dụng E-mail để "giả dạng" một e mail với môt địa chỉ bất kỳ nào mà họ muốn, với nội dung là một tấm thiệp, một file attach hay đường link nào đó. Đó đều là những file malware gây nguy hiểm cho máy tính. Vậy làm sao để nhận dạng?

Cách ngăn chặn

Phần này chủ yếu dựa trên kinh nghiệm hiểu biết của bạn. Bạn nên cảnh giác với những bức Mail có nội dung chung chung. Giả sử như ở phần đầu của bức Mail không có phần Gửi/Chào... Hoặc không ghi rõ tên: Gửi bạn/Chào bạn... những bức mail dạng này mà kèm theo attach file hay đường link nào đó thì bạn đừng nên down về, hoặc bạn nên quét virus cẩn thận trước khi chắc chắn mở nó ra.

Lây lan vào các tệp tin thực thi

Những trang Web bạn truy cập đều là các trang Web sạch (không chứa mã độc, không có virus và có thể là các trang

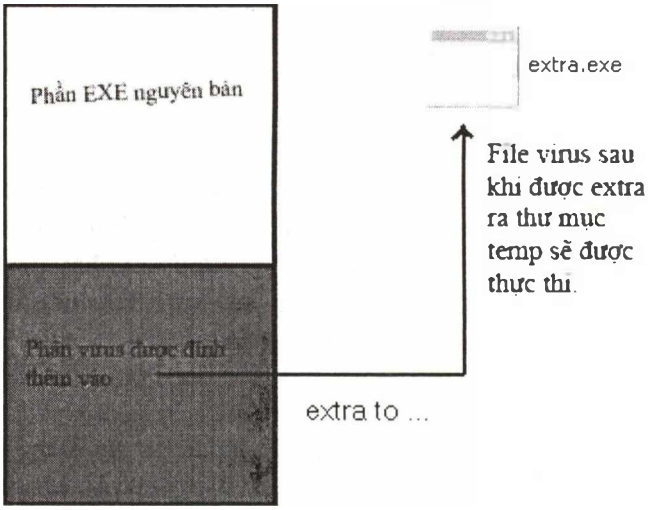
Web có uy tín). Nhưng dù vậy, bạn vẫn có nguy cơ bị dính virus mà không biết mình đã bị khi nào.

Vì một lý do nào đó, chương trình ứng dụng gốc sau khi được chuyển dịch từ server này lên server khác... đã bị "đính" thêm một con virus vào (đánh tráo thành một tệp bị nhiễm virus). Bạn không hề biết nó có nguy hiểm hay không nên mở vào, ngay lập tức, virus đã được extra và thực thi trên máy bạn từ file cài đặt của ứng dụng.

Cách ngăn chặn

Hacker sau khi download một ứng dụng nguyên bản từ trên mạng về, sẽ sử dụng một phần mềm "exe joiner" nào đó để có thể đính 2 tệp .exe vào với nhau. Rồi tiếp tục đem lên các trang Web khác phát tán ứng dụng đã được đính virus. Nguyên lý của việc đính .exe này có thể hiểu đơn giản như sau:

- Virus sẽ được quảng vào cuối file của ứng dụng (hoặc một nơi nào đó không làm ảnh hưởng tới tiến trình).
- Sau khi chạy ứng dụng, virus sẽ được tự động extra ra thư mục temp (thư mục tạm của window) rồi tự động chạy tệp .exe vừa được extra ra.



Cách ngăn chặn việc này rất khó, vì hacker có trăm phương nghìn kế để che mắt chúng ta. Ta chỉ có thể "xem qua" tính an toàn của ứng dụng.

Nếu bạn đã biết qua cấu trúc của một tệp.exe chắc cũng biết phần MZ ở đầu một tệp.exe, khi nó được đính vào ứng dụng sẽ có một phần dấu hiệu nhận biết nào đó.

```
00  ...à.......?.ÿ..
00  ...à.......?.ÿ..
00  ...ð.......▌.ÿ..
00  ...ø.0.....▌.ÿ..
00  ...ù.1.....ÿ.ÿ..
5D  ...ÿ.ÿ.Ç.[start]
00  MZ▌.........ÿÿ..
00  ¸.......@.......
00  ................
00  ............È...
68  .º..´.Í!¸.LÍ!Th
6F  is program canno
20  t be run in DOS
00  mode....$.......
88  Ë ÎA ÎA ÎA Î
```

Thông thường thì trong một tệp .exe chỉ có một cụm chữ MZ, nếu có hai cụm và ở phía trước có một dấu hiệu lạ nào đó thì tệp setup đã bị "dính virus". Bạn nên xóa tệp đó và báo cho nhà cung cấp hoặc nơi lưu trữ ứng dụng biết để không làm nhiều người khác bị nhiễm.

Trên thực tế thì các phần mềm diệt virus hiện nay đều có tính năng nhận dạng những kiểu "đính" virus lộ liễu như thế này. Nhưng vì khả năng phòng thủ và tấn công luôn luôn song hành nên bạn khó lòng có thể tránh khỏi.

7. Các vấn đề cần quan tâm khi mua sản phẩm Anti-spyware

Spyware là vấn đề đáng lo ngại về bảo mật máy tính. Do đó, khi quyết định việc chọn lựa giải pháp Anti-spyware cho hệ thống mạng của mình, bạn cần cân nhắc nhiều yếu tố quan trọng sau:

Trình Anti-spyware có công cụ dò tìm mạnh mẽ hay không?

"Trái tim" của bất kỳ giải pháp chống spyware nào cũng đều nằm trong cơ sở dữ liệu quét của nó. Hãy tìm những sản phẩm Anti-spyware có cơ sở dữ liệu lớn, phạm vi hoạt động của phần mềm rộng để nó có thể quét và nhận dạng nhiều spyware.

Cơ sở dữ liệu và chương trình có được cập nhật tự động?

Chương trình phải được tự động cập nhật đến dữ liệu spyware mới nhất một cách thường xuyên cũng như tự dò tìm những phiên bản mới của chương trình hay công cụ quét (scan engine) để có những nâng cấp thích hợp.

Chương trình có thể tự vận hành?

Hầu hết người dùng sẽ mau chóng quên vận hành thủ công cho chương trình Anti-spyware và cũng không muốn các nhân viên IT thường xuyên thao tác trên máy tính của họ nên phương thức tốt nhất là trình Anti-spyware có thể tự hoạt động.

Chương trình có nhiều tùy chọn quét hay không?

Quét toàn bộ hệ thống hay từng thư mục hay tập tin tùy chọn, quét những thiết lập Registry hay bộ nhớ đang sử dụng hoặc những nguy cơ có thể bị lây nhiễm spyware khác.

Chương trình có hỗ trợ theo dõi hoạt động trong thời gian thực?

Đừng đợi đến khi spyware lây nhiễm rồi mới tiến hành quét và diệt vì đôi lúc việc này có thể đã quá muộn màng cho dữ liệu của bạn. Chương trình phải là lá chắn đầu tiên và luôn vận hành lá chắn này trong suốt thời gian người dùng hoạt động trên máy. Một chế độ quét tùy chọn định kỳ thường xuyên cũng là một tính năng hữu ích cho người dùng.

Chương trình có chức năng quản trị trung tâm?

Để bảo vệ hệ thống mạng hiệu quả, người quản trị không thể nào đến từng máy trong mạng để xử lý tình huống mà phải thông qua phần quản lý trung tâm của chương trình. Đại

đa số chương trình Anti-spyware ngày nay có thêm phần quản lý bảo vệ trung tâm, cho phép quản trị ra lệnh cập nhật, quét hay lên lịch quét... dễ dàng.

Chế độ bảo vệ khi khởi động?

Gần như tất cả spyware đều được lập trình tự vận hành khi Windows khởi động. Do đó, chế độ bảo vệ và ngăn chặn spyware hoạt động ngay từ lúc khởi động hệ thống là điều rất cần thiết.

Khóa và diệt tận gốc

Khả năng dò tìm không chưa đủ, chương trình phải có khả năng khoanh vùng, khóa spyware hoặc diệt tận gốc chúng mà không cần phải nhờ cậy đến sự can thiệp của người dùng. Hãy tìm hiểu thông tin mô tả cách thức chương trình xử lý spyware và so sánh với những giải pháp cạnh tranh khác.

Báo cáo cũng là chức năng cần quan tâm

Để biết được hiệu suất của việc quét và diệt spyware, bạn cần phải biết số lượng, những loại spyware nào và những tập tin nào đã được khoanh vùng. Các báo cáo sẽ hiển thị thông tin sau khi quét hoàn tất hay cả khi có bất kỳ lỗi nào xảy ra hoặc thông báo về một bản cập nhật vừa được cài đặt.

Chức năng theo dõi hoạt động của những tiến trình (Process Monitoring)

Sẽ không có chương trình Anti-spyware nào có khả năng diệt 100% spyware nếu những spyware này được tái tạo thật sự đặc biệt. Do đó, chương trình Anti-spyware cũng cần có thêm chức năng theo dõi hoạt động của những tiến trình đang chạy trên Windows để người quản trị có thể quan sát và xử lý khi gặp những tiến trình đáng nghi.

Một số giải pháp bảo mật hệ thống mạng hiện nay đều trang bị thêm khả năng chống spyware như: Spyware Doctor, ZoneAlarm Pro, Bitdefender Total Security, Webroot AntiSpyware Corporate Edition, Trend Micro Antispyware...

8. Phòng chống virus, spyware, malware... tuy dễ mà không dễ

Để phòng chống virus, một nguyên tắc cơ bản là luôn đề cao cảnh giác. Tuyệt đối không bao giờ mở những E-mail đính kèm lạ, không bao giờ chạy những chương trình thực thi mà không rõ nguồn gốc. Tuy nhiên, chỉ bấy nhiêu thôi chưa đủ. Bởi vì tình hình hiện nay đã khác trước rất nhiều, virus máy tính ngày càng "tinh ranh" hơn và khó nhận ra hơn.

Nhiều khi bạn không bao giờ chạy những file thực thi lạ do người khác gởi đến nhưng máy tính của bạn lại vẫn cứ bị nhiễm virus. Bạn nhận được những đường link gởi qua tin nhắn Y!M từ nick của người quen với những lời "đường mật". Nếu bạn nhẹ dạ cả tin click vào thì ngay lập tức một file .exe ẩn sẽ được tải về từ Website nhiễm virus và tự động thực thi nếu máy tính của bạn được đặt ở tình trạng an ninh thấp. Sau đó chương trình sẽ khống chế hệ thống, lấy cắp mật khẩu tài khoản Yahoo!, biến sổ địa chỉ của bạn làm nguồn để phát tán virus đến những "nạn nhân" trong đó.

Như vậy, cũng giống như sâu lây lan qua E-mail, biện pháp đề phòng loại virus này là không nên nhấp chuột vào những đường link không rõ nguồn gốc.

Đó là cách phòng chống về mặt "ý thức". Tuy nhiên, thực tế không đơn giản thế. Bạn cần phải thường xuyên "tiêm ngừa" cho máy tính để nó có "sức đề kháng" vượt qua mọi "bệnh tật". Thường xuyên truy cập vào trang chủ Microsoft www.microsoft.com để tải về những bản vá lỗi mới nhất cho Windows và trình duyệt IE.

Cũng xin nói thêm là trình duyệt IE thường xuyên bị các hacker khai thác lỗi bảo mật nhất, cho nên nếu cảm thấy không "yên tâm", bạn có thể chuyển sang sử dụng một trình duyệt Web khác, chẳng hạn như FireFox. Tất nhiên bạn cũng nên thường xuyên truy cập vào trang chủ của hãng sản xuất phần mềm để tải về những bản vá lỗi (nếu có).

Một điều quan trọng nhất là trên máy bạn phải có ít nhất một phần mềm diệt virus "ngoại" được cài thường trú, và phải bật tính năng tự động bảo vệ lên. Có thể kể đến những phần mềm diệt virus nổi tiếng được tổ chức Topten Reviews đánh giá cao là: BitDefender, Kaspersky, F-Secure Antivirus, PC-cillin, ESET Nod32, McAfee, Norton Antivirus... (xếp theo thứ tự đánh giá từ cao xuống thấp).

Theo kinh nghiệm của nhiều người thì BitDefender, Kaspersky diệt virus rất tốt, chúng có khả năng phát hiện và phát cảnh báo ngay lập tức khi bạn truy cập vào những trang Web có chứa virus và mã độc hại. Nên trang bị cho máy tính một phần mềm diệt virus "nội" như D32 hoặc Bkav để chúng bổ sung với các phần mềm diệt virus ngoại vì mỗi phần mềm diệt virus có những ưu nhược điểm riêng.

Khi sử dụng các phần mềm diệt virus, bạn nên thường xuyên cập nhật cơ sở dữ liệu cho nó để chương trình tăng thêm sức đề kháng chống chọi với những virus mới xuất hiện. Nếu sợ quên, bạn nên bật chức năng "Auto Update" để chúng cập nhật tự động cho bạn. Đa số các chương trình chống virus đều có chức năng nhận dạng virus mới chưa có trong cơ sở dữ liệu, dựa trên những hành tung "đáng ngờ" của chúng, bạn nên bật chức năng này lên, nó sẽ rất hữu ích cho bạn.

Cuối cùng, lời khuyên dành cho bạn là nên thường xuyên truy cập vào các trang Web thông tin virus để có thêm nhiều kiến thức về phòng chống virus, càng nhiều càng tốt.

Bài 3

TỔNG HỢP CÁC LOẠI VIRUS, WORM, TROJAN, SPYWARE... CÁCH DIỆT VÀ KHÔI PHỤC MÁY VI TÍNH BỊ NHIỄM

Sau đây chúng tôi sẽ giới thiệu đến độc giả thông tin mô tả, cách diệt các họ Virus, Worm, Trojan, Spyware... điển hình và đặc trưng. Bản thân các chương trình diệt virus có thể sẽ loại bỏ, tuy nhiên những hư hại, hỏng hóc thì không phải chương trình nào cũng có thể khắc phục,

Ví dụ: Có thể hiểu đơn giản như tủ bếp của bạn bị một con chuột phá hoại, nó gặm nhấm thân tủ, ăn các thức ăn trong tủ... Và bạn đã may mắn dùng bẫy bắt được con chuột đó, vậy là từ nay chiếc tủ bếp của bạn sẽ an toàn rồi tuy nhiên làm thế nào mà chiếc bẫy có thể khôi phục lại được tình trạng ban đầu của cái tủ? Thật khó phải không?

Hiện nay, một số chương trình diệt virus có kết hợp tính năng tự sửa chữa những tổn hại do virus gây ra tuy nhiên khả năng là không nhiều và để mục sở thị việc khôi phục này bạn có thể sử dụng các chương trình sửa chữa chuyên nghiệp hoặc tự sửa chữa thủ công bằng tay.

1. Cách diệt virus W32.Randsom.A

Mô tả

Phát hiện: Tháng 11 năm 2008.

Tên: W32.Randsom.A.

Kiểu: Sâu.

Mức độ phát tán: Lây lan.
Hệ thống bị ảnh hưởng:Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE- E0AC10B4E666}\"StubPath" = "%Windir%\UNINSTLV16.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}\"StubPath" = "%Windir%\UNINSTLV16.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\torn.exe

5. Thoát khỏi Registry.

2. Cách diệt W32.Redlofs

Mô tả
Phát hiện: Tháng 11 năm 2008.
Tên: W32.Redlofs.
Kiểu: Sâu.
Mức độ phát tán: 73,000 Bytes.
Hệ thống bị ảnh hưởng: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"10.1.08" = "C:\WINDOWS\10.1.08.exe hlmrun"
   HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".key" = "exefile"
   HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.key
5. Khôi phục lại các giá trị ban đầu.

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Shell" = "Explorer.exe C:\WINDOWS\1o.1.o8.exe shell"

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Userinit" = "C:\WINDOWS\10.1.08.exe init"
   HKEY_USERS\S-1-5-21-1172441840-534431857-1906119351-500\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\"NoFolderOptions" = "1"
   HKEY_USERS\S-1-5-21-1172441840-534431857-1906119351-500\Software\Microsoft\Windows\CurrentVersion\Policies\System\"DisableTaskMgr" = "1"
   HKEY_USERS\S-1-5-21-1172441840-534431857-1906119351-500\Software\Microsoft\Windows\CurrentVersion\Policies\System\"DisableRegistryTools" "1"
   HKEY_USERS\S-1-5-21-1172441840-534431857-1906119351-

500\Software\Microsoft\Windows\CurrentVersion\Run\"1o.1.o8" = "C:\WINDOWS\1o.1.o8.exe hcurun"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".bat" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".cmd" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".com" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".hta" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".js" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".JSE" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".msi" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".pif" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".reg" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".scr" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".VBE" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".vbs" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".WSF" = "exefile"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\".WSH" = "exefile"

6. Thoát khỏi Registry.

3. Cách diệt Spyware CompuSpy

Mô tả

Phát hiện: Tháng 11 năm 2008.

Tên: CompuSpy.

Kiểu: Spyware.

Phát triển bởi: Upsilon Dynamics.

Mức độ nguy hiểm: Trung bình.

Hệ thống bị ảnh hưởng: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Management\ARPCache\CompuSpy KeyLogger
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\cswin2008.exe
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CompuSpy KeyLogger
   HKEY_LOCAL_MACHINE\SOFTWARE\Upsilon Dynamics
   HKEY_LOCAL_MACHINE\SOFTWARE\UpsilonDynamics
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"CompuSpy KeyLogger" = "C:\Program Files\CompuSpy\cswin2008.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"CompuSpy" = "C:\Program Files\CompuSpy\CompuSpy.exe"
5. Thoát khỏi Registry.

4. Cách diệt Trojan.Fakemess

Mô tả

Phát hiện: Tháng 11 năm 2008.
Tên: Trojan.Fakemess.
Kiểu: Trojan.
Hệ thống bị ảnh hưởng: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK..
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\run\"sasa" = "[PATH TO TROJAN]"

5. Khôi phục các giá trị gốc trong Registry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360Safe.exe\"Debugger" = "%System%\svchost.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360rpt.exe\"Debugger" = "%System%\svchost.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360tray.exe\"Debugger" = "%System%\svchost.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

Options\CCenter.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\IceSword.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KASMain.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KASTask.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAV32.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVDX.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVPFW.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVStart.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KISLnchr.exe\"Debugger" =

"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KMFilter.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KMailMon.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFW32.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFWSvc.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KRegEx.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KRepair.COM\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVCenter.kxp\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVMonXP.kxp\"Debugger" =
"%System%\svchost.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution Optio
ns\KVMonXP_1.kxp\\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVSrvXP.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVStub.kxp\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KWatch.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KWatch9x.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KWatchX.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KaScrScn.SCR\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KsLoader.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution Options\KvDetect.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KvReport.kxp\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KvXP.kxp\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KvfwMcl.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\NAVSetup.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFWLiveUpdate.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQDoctor.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RStray.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

Options\Ras.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Rav.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavMon.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavMonD.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavStub.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution Option\
RavTask.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RegClean.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RfwMain.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RsAgent.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\Rsaupd.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\SysSafe.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Systom.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TNT.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TrojDie.kxp\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TrojanDetector.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Trojanwall.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TxoMoU.exe\"Debugger" =
"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UFO.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution Options\UIHost.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UmxAttachment.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UmxCfg.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UmxFwHlp.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UmxPol.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UpLive.EXE\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WoptiClean.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\avp.com\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\avp.exe\"Debugger" = "%System%\svchost.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ccSvcHst.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kabaload.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kvol.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kvolself.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kvupload.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kvwsc.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\nod32krn.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\nod32kui.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwProxy.exe\"Debugger" =

"%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwcfg.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwsrv.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\runiep.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\scan32.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svch0st.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\symlcsvc.exe\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ua80.EXE\"Debugger" = "%System%\svchost.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\zxsweep.exe\"Debugger" = "%System%\svchost.exe"

6. Thoát khỏi Registry.

5. Cách diệt W32.Gaut.A

Mô tả

Phát hiện: Tháng 11 năm 2008

Tên: W32.Gaut.A.

Kiểu: Worm (Sâu).

Mức độ phát tán: 281,551 Bytes.

Hệ thống bị ảnh hưởng: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Yahoo Messengger" = "C:\WINDOWS\system32\chrome.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares\"shared" = "\New Folder.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\"NofolderOptions" = "1"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\"DisableTaskMgr" = "1"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\"DisableRegistryTools" = "1"

5. Khôi phục lại các giá trị ban đầu được ghi trong Registry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Shell" = "Explorer.exe chrome.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Inte

rnet Explorer\Main\"Default_Page_URL" = "http://h1.ripway.com/poojasharma2/index.html" HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\"Default_Search_URL" = "http://h1.ripway.com/poojasharma2/index.html" HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\"Search Page" = "http://h1.ripway.com/poojasharma2/index.html" HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\"Start Page" = "http://h1.ripway.com/poojasharma2/index.html" HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\"Start Page" = "http://h1.ripway.com/poojasharma2/index.html" HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule\"NextAtJobId" = "2"

6. Thoát khỏi Registry.

6. Cách diệt Trojan.Newarxy

Mô tả

Phát hiện: Tháng 11 năm 2008.

Tên: Trojan.Newarxy.

Kiểu: Trojan.

Mức độ phát tán: 25,600 Bytes.

Hệ thống bị ảnh hưởng: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000.

1. Khởi động lại máy sử dụng Windows Recovery Console.
- Đưa đĩa cài Windows XP vào ổ đĩa CD-Rom.
- Khởi động lại máy từ CD-Rom.

- Ấn R để bắt đầu sử dụng chương trình Recorvery Console đến màn hình "Welcome to Setup".
- Chọn cài đặt nếu bạn muốn cài đặt bằng Recorvery Console.
- Chọn administrator và password, sau đó Enter.
- Đánh cd c:\windows\system32.
- Ấn Enter.
- Đánh copy ws2_32_.dll ws2_32.dll.
- Ấn Enter.
- Gõ Y để ghi đè files.
- Ấn Enter.
- Gõ Exit.
- Ấn Enter, Computer sẽ tự động khởi lại.

2. Tắt chế độ System Restore (Windows Me/XP).
3. Cập nhật chương trình diệt virus mới.
4. Scan toàn bộ hệ thống.
5. Xoá các giá trị được ghi vào Registry.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyServer" = "http=127.0.0.1:9191"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyOverride" = "*.local;<local>"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet

Settings\"ProxyEnable" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyServer" = "http=127.0.0.1:9191"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyOverride" = "*.local;<local>"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyEnable" = "1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\"AllowProtectedRenames" = "1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\0001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyServer" = "http=127.0.0.1:9191"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\0001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyOverride" = "*.local;<local>"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyServer" = "http=127.0.0.1:9191"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyOverride" = "*.local;<local>"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\"C:\WINDOWS\system32\netsh.exe" = "C:\WINDOWS\system32\netsh.exe:*:Enabled:TINYPROXY"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\

Services\SharedAccess\Parameters\FirewallPolicy\Standar
dProfile\AuthorizedApplications\List\"C:\Program
Files\Internet Explorer\IEXPLORE.EXE" = "C:\Program
Files\Internet
Explorer\IEXPLORE.EXE:*:Enabled:TINYPROXY"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\FirewallPolicy\Standar
dProfile\GloballyOpenPorts\List\"9191:TCP" =
"9191:TCP:*:Enabled:TINYPROXY"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\SFC\"wmiprvse.exe" = " "
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\SFC\"netsh.exe" = " "
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\SFC\"IEXPLORE.EXE" = " "
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\"ProxyServer" =
"http=127.0.0.1:9191"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\"ProxyOverride" =
"*.local;<local>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\"ProxyEnable" = "1"

5. Khôi phục lại các giá trị ban đầu của Registry.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Hardware
Profiles\0001\Software\Microsoft\windows\CurrentVersio
n\Internet Settings\"ProxyEnable" = "1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Hardware
Profiles\Current\Software\Microsoft\windows\CurrentVers
ion\Internet Settings\"ProxyEnable" = "1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\

Services\SharedAccess\Epoch\"Epoch" = "0x00000B96"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyEnable" = "1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SFC

6. Thoát khỏi Registry.

7. Cách diệt W32.Wecorl

Mô tả

Phát hiện: Tháng 11 năm 2008.

Tên: W32.Wecorl.

Được biết với tên khác: W32/Wecorl [McAfee], WORM_WECORL.A [Trend].

Kiểu: Sâu (Worm).

Hệ thống bị ảnh hưởng: Windows 2000, Windows Server 2003, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK..
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Licenses\"[MAC ADDRESS]" = "[HEXADECIMAL DATA]"
HKEY_LOCAL_MACHINE\SOFTWARE\Google\"[MAC ADDRESS]" = "[HEXADECIMAL DATA]"

5. Thoát khỏi Registry.

8. Cách diệt Backdoor Bifrose M

http://images.google.com.vn/imgres?imgurl=http://www.bangdientu.vn/DesktopModules/tNew/Images/12062008PC.jpg&imgrefurl=http://www.bangdientu.vn/Default.aspx%3Ftabid%3D61%26cateId%3D1%26newId%3D61&h=267&w=400&sz=27&hl=vi&start=11&usg=__MT-Jz96w5wXpm6Z6sNVPXo3SBak=&tbnid=sIb4h7J6Hv_lhM:&tbnh=83&tbnw=124&prev=/images%3Fq%3DTrojan%2Bpc%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Phát hiện: Tháng 10 năm 2008.
Tên: Backdoor.Bifrose.M.
Kiểu: Trojan.
Mức độ phát tán: 40,179 Bytes.
Hệ thống bị ảnh hưởng: Windows XP, Windows Server 2003, Windows 2000.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"StartKey" = "%System%\msnmsie.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\SKav\"nck" = "99 6F D5 66 A0 AC EA 5F F7 EC 7F 84 DC 8A DA 00 A8 5F E4 52 A0 AC EA 5F F7 EC 7F 84 DC 8A DA 00"
HKEY_CURRENT_USER\Software\SKav\"klg" = "00"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}\"stubpath" =

"C:\WINDOWS\system32\msnmsie.exe s\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}
HKEY_LOCAL_MACHINE\SOFTWARE\SKav
HKEY_CURRENT_USER\SOFTWARE\Skav

5. Thoát khỏi Registry.

9. Cách diệt Infostealer Bancos AC

http://images.google.com.vn/imgres?imgurl=http://www.techshout.com/images/talking-trojan.jpg&imgrefurl=http://www.techshout.com/internet/2007/07/new-talking-virus-botneta-trojan-deletes-pc-files-warns-pandalabs/&h=368&w=450&sz=30&hl=vi&start=5&usg=__0Yrc5Ol_2S5vhv_7PgVBTXXOtwA=&tbnid=gDkChKVb8D3W2M:&tbnh=104&tbnw=127&prev=/images%3Fq%3DTrojan%2Bpc%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Phát hiện: Ngày 19 tháng 10 năm 2008.
Tên: Infostealer.Bancos.AC.
Kiểu: Trojan.
Mức độ phát tán: 3,174 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK..

4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\"@#E@#n%^a&^%b#$%l^%$e^& %^&B#$%r&^%o$%w@#$s^%$e&*r(*& &*E*^&x$^%t%$#e@#$n&^%s#%i*^o$%^n(&*s%^&" = "yes"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\[RANDOM CLSID]\"(Default)" = "Google Accelerator!"

HKEY_CLASSES_ROOT\CLSID\[RANDOM CLSID]\"(Default)" = "Google Accelerator!"

HKEY_CLASSES_ROOT\CLSID\[RANDOM CLSID]\InProcServer32\"(Default)" = "%System%\googlejd.dll"

HKEY_CLASSES_ROOT\CLSID\[RANDOM CLSID]\InProcServer32\"ThreadingModel" = "Apartment"

5. Thoát khỏi Registry.

10. Cách diệt W32.Harakit

http://images.google.com.vn/imgres?imgurl=http://www.baomatthongtin.com/images/news/10.jpg&imgrefurl=http://www.baomatthongtin.com/news.asp%3FPerl.php%3DDetails%26action%3D365&h=281&w=400&sz=28&hl=vi&start=4&usg=__e-I7G2CLEilT9b2j4eACm16rdcM=&tbnid=ktIqCsv0Ah53cM:&tbnh=87&tbnw=124&prev=/images%3Fq%3DTrojan%2Bpc%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Phát hiện: Tháng 10 năm 2008.

Tên: W32.Harakit.

Kiểu: Trojan, sâu (Worm).

Mức độ phát tán: 454,134 Bytes.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"cftm" = "C:\WINDOWS\system32\cftm.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"csrcs" = "C:\WINDOWS\system32\csrcs.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"cftm" = "C:\WINDOWS\system32\cftm.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\"cftm" = "C:\WINDOWS\system32\cftm.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DRM
   HKEY_LOCAL_MACHINE\SOFTWARE\ESET\Nod

5. Khôi phục các giá trị sau nếu cần thiết:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Shell" = "Explorer.exe csrcs.exe"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\"ShowSuperHidden" = "0"

6. Thoát khỏi Registry.

11. Cách diệt Win32/PSW OnLineGames NNT

http://images.google.com.vn/imgres?imgurl=http://images4.dantri.com.vn/Uploaded/vinhtt/virus30052007.gif&imgrefurl=http://halong.net.vn/main.aspx%3FMNU%3D1022%26Style%3D1&h=263&w=350&sz=133&hl=vi&start=17&usg=__SuQzJhukWEac9Vtn3uvcMHNYVvo=&tbnid=i3nlnrhfsHNnyM:&tbnh=90&tbnw=120&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Tên: Trojan.Win32.Vaklik.ya (Kaspersky),
W32/Autorun.worm.bx.gen (McAfee),
Packer.Win32.Mian007.a (Rising).
Kiểu: Trojan.
Kích thước: 107854 Bytes.
Hệ thống ảnh hưởng: Microsoft Windows.
Phiên bản trong cơ sở dữ liệu: 2988 (20080331).
Mô tả: Win32/PSW.OnLineGames.NNT là một Trojan trộm cắp thông tin nhạy cảm. Các Trojan có thể gửi thông tin đến một máy từ xa.

Cài đặt

Khi thực hiện, Trojan bản sao của chính nó trong hệ thống %system% thư mục bằng cách sử dụng file mmvo.exe.
Dưới đây là tập tin có trong cùng một thư mục:
mmvo%number%.dll.
Những tập tin sau đây được ghi vào vào thư mục:
%temp%uveyg.dll
%variable%.sys.
Những chuỗi và biến được sử dụng và chèn vào %variable%.
Các biến %number% đại diện một số ngẫu nhiên tạo ra trong khoảng 0-9.

Files có tên sau đây được chèn vào quá trình chạy của hệ thống: %system%\mmvo%number%.dll .
Khi đã lây lan vào hệ thống, Trojan sẽ ghi thêm giá trị vào Registry ở khoá sau:

[HKEY_CURRENT_USER\SoftWare\Microsoft\
Windows\CurrentVersion\Run]
"mmva" = "%system%\mmvo.exe"
Và sửa lại các giá trị sau trong Registry
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced]
"Hidden" = 2

[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced]
"ShowSuperHidden" = 0

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL]
"CheckedValue" = 0

[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun" = 91

Sự lây lan:

Trojan bản sao của chính nó vào trong thư mục gốc của cố định và / hoặc ổ đĩa bằng cách sử dụng các tên sau đây: uevr.cmd

Files được chạy cùng là Autorun.inf

Vì thế, nó đảm bảo cho Trojan này là một phương tiện phát tán khi mỗi thông tin được nhập vào máy tính.

Lấy cắp thông tin

Các Trojan lấy cắp thông tin thu thập được thông qua quá trình tạo ra những files sau:

Ragexe.exe
lin.bin
YPagerj.exe
YahooWidgetEngine.exe
pol.exe

Các Trojan có thể đăng nhập vào bằng một tổ hợp phím.
Các Trojan có thể gửi thông tin đến một máy từ xa.
Các HTTP / HTTPS giao thức được sử dụng.

Thông tin khác

Các Trojan được gửi dữ liệu và lệnh từ xa từ một máy tính hay mạng Internet. Các Trojan chứa một danh sách các URL. Các Trojan có thể tải về và thực hiện một tập tin từ Internet. Hồ sơ được lưu như sau đó % temp% \ uu.exe và thi hành Khi bị nhiễm loại Trojan này các bạn có thể dựa vào những thông tin ở trên để loại bỏ nó ra khỏi máy tính.

12. Cách diệt Win32/Mabezat.A

http://images.google.com.vn/imgres?imgurl=http://www.canhtoan.com/dportal_resources/images/news/200804031626120.FV1645_computer_virus.jpg&imgrefurl=http://www.canhtoan.com/%3Fmod%3Dnews%26act%3Ddetail%26id%3D202&h=602&w=800&sz=96&hl=vi&start=5&usg=__hC4GwZRFhCDNs3dMDubBRLQP9r0=&tbnid=TJHzImbpatWvjM:&tbnh=108&tbnw=143&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Tên: Worm.Win32.Mabezat.b (Kaspersky), W32/Mabezat (McAfee), Win32/Mabezat.A (Grisoft).
Kiểu phát hiện: Virus.

Kích thước: Khoảng 155Kb.
Hệ thống bị ảnh hưởng: Microsoft Windows.
Phiên bản trong cơ sở dữ liệu: 2649 (20071109)
Win32/Mabezat.A là một tệp tin.

Cài đặt

Khi được khởi tạo, virus tạo ra chính nó lưu trong %drive%\Documents and Settings\
Trong thư mục tạo ra những tệp có tên sau:
tazebama.dl_
hook.dl_
Những tập tin sau có trong thư mục:
tazebama.dll (32768 B)
Virus tạo ra những thư mục sau:
%appdata%\tazebama\
Những giá trị sau trong Registry bị xoá:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"

Những giá trị mới được ghi:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Hidden" = 2

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"HideFileExt" = 1

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"ShowSuperHidden" = 0

Sự lây nhiễm

Khi máy bị nhiễm virus thì virus sẽ tìm và đính kèm cùng với đuôi mở rộng .exe.

Khi tài liệu bị nhiễm virus, nó tạo ra một file tương tự và có đuôi mở rộng là .exe.

Sự lây lan

Khi bị nhiễm virus, nó copy chính nó vào tất cả các forder được sử dụng trong tất cả các ổ được sử dụng với tên sau:
zPharaoh.exe
Những tập tin sau có trong từng thư mục:
Autorun.inf
Virus tạo ra chính nó vào các thư mục được sử dụng. Những tập tin sau được sử dụng:
Adjust Time.exe
AmericanOnLine.exe
Antenna2Net.exe
BrowseAllUsers.exe
CD Burner.exe
Crack_GoogleEarthPro.exe
Disk Defragmenter.exe
FaxSend.exe
FloppyDiskPartion.exe
GoogleToolbarNotifier.exe
HP_LaserJetAllInOneConfig.exe
IDE Conector P2P.exe
InstallMSN11Ar.exe
InstallMSN11En.exe
JetAudio dump.exe
KasperSky6.0 Key.doc.exe
Lock Folder.exe
LockWindowsPartition.exe

Make Windows Original.exe
MakeUrOwnFamilyTree.exe
Microsoft MSN.exe
Microsoft Windows Network.exe
msjavx86.exe
NokiaN73Tools.exe
Office2003 CD-Key.doc.exe
Office2007 Serial.txt.exe
PanasonicDVD_DigitalCam.exe
RadioTV.exe
Recycle Bin.exe
RecycleBinProtect.exe
ShowDesktop.exe
Sony Erikson DigitalCam.exe
Win98compatibleXP.exe
Windows Keys Secrets.exe
WindowsXp StartMenu Settings.exe
WinrRarSerialInstall.exe
Tên của tập tin có thể được dựa trên tên của một tập tin hoặc thư mục hiện hành và nó có đuôi mở rộng là ".exe".

Thông tin khác

Nếu ngày hiện tại hệ thống phù hợp với điều kiện, các tập tin và các files sẽ được mã hoá với đuôi mở rộng: ASP; ASPX; ASPX; CS; BAS; C; CPP; DOC; H; HLP; HTM; HTML; MDB; MDF; PAS; PDF; PHP; PPT; PSD; RAR; RTF; TXT; XLS; ZIP.

Virus tạo chính nó và copy vào folder %userprofile%\Local Settings\Application Data\Microsoft\CD Burning. Nếu hoàn thành nó sẽ ghi tên file dược sử dụng là zPharaoh.exe cùng với files đính kèm là Autorun.inf. Virus tạo ra một file text %appdata%\tazebama\zPharaoh.dat.

Các virus có thể tạo những tập tin theo %drive%\Documents and Settings\tên thư mục MyDocuments.rar backup.rar; documents_backup.rar; imp_data.rar; source.rar; windows_secrets.rar; passwords.rar; serials.rar; office_crack.rar; windows.rar;

Khi bị nhiễm loại virus này, các bạn có thể tham khảo các thông tin ở trên để có thể xoá được nó.

13. Cách diệt Spyware Guard 2008

http://images.google.com.vn/imgres?imgurl=http://www.spyware-free.biz/spyware-709821.jpg&imgrefurl=http://www.spyware-free.biz/&h=384&w=339&sz=46&hl=vi&start=8&usg=__VHmwSV_DEY9fit7-aBzWwHpdPRY=&tbnid=2_uABOCv6KNS7M:&tbnh=123&tbnw=109&prev=/images%3Fq%3Dspyware%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Ngày 1 tháng 10 năm 2008.
Tên: SpywareGuard2008.
Kiểu: Làm lỗi các chương trình ứng dụng.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.

4. Tìm và xoá các giá trị:

   KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"spywareguard" = "C:\Program Files\Spyware Guard 2008\spywareguard.exe"
   HKEY_CURRENT_USER\Software\Spyware Guard
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Spyware Guard 2008

5. Thoát khỏi Registry.

14. Cách diệt Trojan.Hexzone

http://images.google.com.vn/imgres?imgurl=http://www.gccom.net/home/Upload/News/2008/1/25/gccom_images977357_images573387_virus_sober.jpg&imgrefurl=http://www.gccom.net/home/%3Froot:gccom%3Dnewsview.html%3Fresuilt%3B_gnews%3D44085b8b282a17a69efe0274ffe816f8%26n%3D331%26c%3D3&h=291&w=400&sz=19&hl=vi&start=5&usg=__k820nZ9YbKUoGSHz6nLLvom3ZCM=&tbnid=7VvNmFkOJ94fCM:&tbnh=90&tbnw=124&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Tháng 10 năm 2008.

Tên: Trojan.Hexzone.

Kiểu: Trojan.

Mức độ nguy hiểm: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\qlplib.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{B0ED4726-5BC8-4E22-A7A8-3074A73CE64E}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1408E208-2AC1-42D3-9F10-78A5B36E05AC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{143537BB-C1AD-456A-927A-CF7B5F1D12AE}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{D82C6C8A-3561-4A19-A128-F42ED5C15D45}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{FBC65A12-7967-4E53-B852-D6BCE504827A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\06C867BE-5BDA-4AE6-9A83-B55436397E8A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\FBC65A12-7967-4E53-B852-D6BCE504827A}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xvideoplugin.JetMimeFiltr
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xvideoplugin.JetMimeFiltr.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xvideoplugin.JetVideoPlugin
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xvideoplugin.JetVideoPlugin.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{143537BB-C1AD-456A-927A-CF7B5F1D12AE}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\qlplib.DLL\"AppID" = "{B0ED4726-5BC8-4E22-A7A8-

3074A73CE64E}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{B0ED4726-5BC8-4E22-A7A8-3074A73CE64E}\"" = "qlplib"

5. Thoát khỏi Registry.

15. Cách diệt EKerberos

Mô tả

Phát hiện: Tháng 10 năm 2008.

Tên: eKerberos.

Phiên bản: 1.0.

Kiểu: Làm lỗi các chương trình ứng dụng.

Phát triển bởi: Innovagest 2000.

Mức độ nguy hiểm: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\eKerberos" = "C:\Program Files\eKerberos\eKerberos.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\eKerberos
   HKEY_LOCAL_MACHINE\SOFTWARE\eKerberos.

5. Thoát khỏi Registry.

16. Cách diệt Cleaner2009

http://images.google.com.vn/imgres?imgurl=http://www.gccom.net/home/Upload/News/2008/1/25/gccom_images977357_images573387_virus_sober.jpg&imgrefurl=http://www.gccom.net/home/%3Froot:gccom%3Dnewsview.html%3Fresuilt%3B_gnews%3D44085b8b282a17a69efe0274ffe816f8%26n%3D331%26c%3D3&h=291&w=400&sz=19&hl=vi&start=6&usg=__SRl6zUbdlciYeaUj4zmPxCa2GDI=&tbnid=7VvNmFkQJ94fCM:&tbnh=90&tbnw=124&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Tháng 9 năm 2008.
Tên: Cleaner2009.
Phiên bản: 1.0.11.0.
Kiểu: Làm lỗi các chương trình ứng dụng.
Phát triển bởi: Cleaner2009, Inc.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Cleaner2009 Freeware" = "C:\Program Files\Cleaner2009 Freeware\UCLN.exe" /min
HKEY_CURRENT_USER\Software\Cleaner2009 Freeware
HKEY_CLASSES_ROOT\AppID\iercpt.DLL
HKEY_CLASSES_ROOT\AppID\{3A9377A6-BE7F-

485D-908C-D44114691389}
HKEY_CLASSES_ROOT\CLSID\{D4CDC21D-43BE-4101-A1EF-E379F134771E}
HKEY_CLASSES_ROOT\Interface\{59C345BA-3D5E-44E3-9D10-D3848AF15D73}
HKEY_CLASSES_ROOT\TypeLib\{A6FBD2E4-1C7E-4EAB-80DD-01DE2645566A}
HKEY_CLASSES_ROOT\iercpt.iercptbho.1
HKEY_CLASSES_ROOT\iercpt.iercptbho
HKEY_LOCAL_MACHINE\SOFTWARE\Cleaner2009 Freeware
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D4CDC21D-43BE-4101-A1EF-E379F134771E}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\QuickInstallPack
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\UCLN_install_is1

5. Thoát khỏi Registry.

17. Cách diệt Spyware SpyMonitor

http://images.google.com.vn/imgres?imgurl=http://images4.dantri.com.vn/Uploaded/vinhtt/virus30052007.gif&imgrefurl=http://halong.net.vn/main.aspx%3FMNU%3D1022%26Style%3D1&h=263&w=350&sz=133&hl=vi&start=17&usg=__ZHONp04rBpiVFZQPTylcMRDvJnE=&tbnid=i3nlnrhfsHNnyM:&tbnh=90&tbnw=120&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Ngày 11 tháng 8 năm 2008.

Tên: Spyware.SpyMonitor.

Kiểu: Spyware.
Phát triển bởi: eMatrixSoft.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"adsnwk" = "%System%\adsnwk.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\comdlg32.OCX" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\MSCOMCTL.OCX" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mscomct2.OCX" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\msvbvm60.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mxpvct22.dat" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mxpvct25.dat" = "1"

HKEY_CLASSES_ROOT\Chilkat.E-mail2.1
HKEY_CLASSES_ROOT\Chilkat.E-mail2
HKEY_CLASSES_ROOT\Chilkat.E-mailBundle2.1
HKEY_CLASSES_ROOT\Chilkat.E-mailBundle2
HKEY_CLASSES_ROOT\Chilkat.MailMan2.1
HKEY_CLASSES_ROOT\Chilkat.MailMan2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mail2.1
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mail2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mailBundle2.1
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mailBundle2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatMailMan2.1
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatMailMan2
HKEY_CLASSES_ROOT\Interface\{06544919-F559-4AE5-9001-F903BD8A84E6}
HKEY_CLASSES_ROOT\Interface\{51A0888C-9970-44DE-8C2C-835BA870D06F}
HKEY_CLASSES_ROOT\Interface\{5ACAE4B8-62D9-4124-A58A-9B1258B77E99}
HKEY_CLASSES_ROOT\Interface\{7D37DED8-1945-4E42-A3FD-B9620E0AD8E3}
HKEY_CLASSES_ROOT\Interface\{C4C23B78-DB98-444C-B601-DCAC6EBBEC54}
HKEY_CLASSES_ROOT\Interface\{CCB7FB40-99EC-4678-9202-52798DA78ABA}
HKEY_CLASSES_ROOT\Interface\{D12FB216-99DA-4EB3-9CC0-C0F760B174A0}
HKEY_CLASSES_ROOT\Interface\{D56C1AF1-3FDE-471C-9BC2-C52515F260C1}
HKEY_CLASSES_ROOT\Interface\{E656B867-992C-4462-A27D-EBE604EC3A48}
HKEY_CLASSES_ROOT\TypeLib\{1DF3AFED-99E0-4474-9900-954B8FD24E86}
HKEY_CLASSES_ROOT\CLSID\{A4643A87-99A0-4404-9BC5-2322BDD61637}

HKEY_CLASSES_ROOT\CLSID\{A46E5261-9956-4767-88CA-DFCED050D09E}
HKEY_CLASSES_ROOT\CLSID\{A7EC2CD3-9941-4FD4-9D01-105DC16A4313}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\KSM_is1

5. Thoát khỏi Registry.

18. Cách diệt Spyware HBScreenSpy

http://images.google.com.vn/imgres?imgurl=http://tapchipc.com/home/images/stories/anh_st/Virus.jpg&imgrefurl=http://tapchipc.com/home/tin-tuc/internet/1098-cho-ngam-vius-tien-hoa-thanh-sieu-thi-ma-doc.html&h=300&w=450&sz=61&hl=vi&start=3&usg=__N8xXOTyvLfqVEZhbPPJ7nDnivdc=&tbnid=ydxXHQ0vjjwczM:&tbnh=85&tbnw=127&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Tháng 8 năm 2008.
Tên: Spyware.HBScreenSpy.
Kiểu: Spyware.
Phiên bản: 3.3.
Mức độ nguy hiểm: Thấp.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"IEServer" = "C:\Program Files\HB Screen Spy\IEServer.exe"
   HKEY_CURRENT_USER\Software\digi
   HKEY_CLASSES_ROOT\CLSID\{825BF622-FF5D-411A-8B1F-824CA555819F}
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HB Screen Spy3.3
   HKEY_LOCAL_MACHINE\SOFTWARE\digi

5. Thoát khỏi Registry.

19. Cách diệt W32.Auraax

http://images.google.com.vn/imgres?imgurl=http://www.vtv.vn/HTML/Data/resources/Original/Image/2007/2/13/2007213184958_130207Virus.jpg&imgrefurl=http://www.3c.com.vn/Story/vn/hotrokhachhang/anninhbaomat/thongtinbaomat/2008/9/46287.html&h=268&w=351&sz=45&hl=vi&start=10&usg=__vXoKJX4pnL3BmaJJ7xs4EHf1PvY=&tbnid=rFIV-uNiZfs-MM:&tbnh=92&tbnw=120&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi)

Mô tả

Phát hiện: Ngày 24 tháng 9 năm 2008.
Cập nhật: Ngày 24 tháng 9 năm 2008(8:27:27 AM).
Tên: W32.Auraax.
Kiểu: Sâu.
Mức độ lây lan: 27,136 Bytes.
Mức độ nguy hiểm: Thấp.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe\"Debugger" = "%ProgramFiles%\Microsoft Common\wuauclt.exe"
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\"%ProgramFiles%\Microsoft Common\wuauclt.exe" = "%ProgramFiles%\Microsoft Common\wuauclt.exe:*:Enabled:EMOTIONS_EXECUTABLE"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Userinit" = "%System%\userinit.exe, %ProgramFiles%\Microsoft Common\wuauclt.exe"

5. Thoát khỏi Registry.

20. Cách diệt W32.Savix

Mô tả

Phát hiện: Ngày 18 tháng 9 năm 2008.
Cập nhật: Ngày 18 tháng 9 năm 2008 (6:52:26 PM).
Tên: W32.Savix.
Kiểu: Sâu.

Mức độ nguy hiểm: Thấp.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\"DisableSR" = "1"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\ShowAll\"CheckedValue" = "0"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\"NoControlPanel" = "1"
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\"userinit" = "\WINDOWS\system32/userinit.exe,C:\WINDOWS\system32\cmd.exe /C C:\.X, C:\WINDOWS\system32\cmd.exe /C D:\.X, C:\WINDOWS\system32\cmd.exe /C E:\.X, C:\WINDOWS\system32\cmd.exe /C F:\.X, C:\WINDOWS\system32\cmd.exe /C G:\.X, C:\WINDOWS\system32\cmd.exe /C H:\.X, C:\WINDOWS\system32\cmd.exe /C I:\.X"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Userinit" = "\WINDOWS\system32/userinit.exe,C:\WINDOWS\system32\cmd.exe /C C:\.X, C:\WINDOWS\system32\cmd.exe /C D:\.X, C:\WINDOWS\system32\cmd.exe /C E:\.X, C:\WINDOWS\system32\cmd.exe /C F:\.X,

C:\WINDOWS\system32\cmd.exe /C G:\X,
C:\WINDOWS\system32\cmd.exe /C H:\X,
C:\WINDOWS\system32\cmd.exe /C I:\X"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\"CheckedValue" = "0"

5. Thoát khỏi Registry.

21. Cách diệt Backdoor Tidserv

http://images.google.com.vn/imgres?imgurl=http://www.gccom.net/home/Upload/News/2008/2/13/gccom_virus1.JPG&imgrefurl=http://www.gccom.net/home/%3Froot:gccom%3Dnewsview.html%3Fresuilt%3B_gnews%3D44085b8b282a17a69efe0274ffe816f8%26n%3D333%26c%3D3&h=305&w=320&sz=17&hl=vi&start=1&usg=__8ouG9EObyu5Nz34lf7YWwVRRqA0=&tbnid=03znmNuq9bUb-M:&tbnh=112&tbnw=118&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Ngày 18 tháng 9 năm 2008.

Cập nhật: Ngày 18 tháng 9 năm 2008 (4:01:39 PM).

Tên: Backdoor.Tidserv.

Kiểu: Trojan.

Mức độ nguy hiểm: Thấp.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\"build" = "standart"
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\"servers down" = "1"
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\"type" = "popup"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\tdssdata\"affid" = "39"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\tdssdata\"asubid" = "v2test7"
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TDSServ
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TDSServ.sys
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TDSServ.sys
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\version
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\connections
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\disallowed
   HKEY_LOCAL_MACHINE\SOFTWARE\TDSS\injector

5. Thoát khỏi Registry.

22. Cách diệt Spyware RemoteSpy

http://images.google.com.vn/imgres?imgurl=http://www.comphandyman.com/mediac/400_0/media/Spyware%2420Guy.jpg&imgrefurl=http://www.spywarecover.info/&h=480&w=399&sz=36&hl=vi&start=11&usg=__yV038_L3lziIpamayLPCT4yHwq8=&tbnid=IdzrRBTharC1yM:&tbnh=129&tbnw=107&prev=/images%3Fq%3Dspyware%26gbv%3D2%26hl%3Dvi

Mô tả

Phát hiện: Ngày 12 tháng 9 năm 2008.

Tên: RemoteSpy.

Kiểu: Spyware.

Phát Triển: Cyber Spy Software LLC.

Mức độ nguy hiểm: High.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"winchk" = "C:\Documents and Settings\All Users\Application Data\WebExt\winchk.exe

5. Thoát khỏi Registry.

23. Cách diệt Spyware KeyPlusPlus

Mô tả

Phát hiện: Tháng 9 năm 2008.

Tên: Key++ Invisible Spy Keylogger.

Kiểu: Spyware.

Phát Triển: KeyPlusPlus.com.

Mức độ nguy hiểm: Trung Bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"keyplusplus" = "C:\progra~1\common~1\keyplusplus\startk.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Installer\Assemblies
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AD8C27A7-42C0-49CD-9DBE-BB6F1CF7FA04}
   HKEY_LOCAL_MACHINE\SOFTWARE\keyplusplus

5. Thoát khỏi Registry.

24. Cách diệt Spyware Spy Monitor

Mô tả

Phát hiện: Ngày 11 tháng 8 năm 2008.
Tên: Keylogger Spy Monitor.
Kiểu: Spyware.
Phát triển bởi: eMatrixSoft.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"adsnwk" = "%System%\adsnwk.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\comdlg32.OCX" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\MSCOMCTL.OCX" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mscomct2.OCX" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\msvbvm60.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mxpvct22.dat" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs\"C:\WINDOWS\system32\mxpvct25.dat" = "1"
HKEY_CLASSES_ROOT\Chilkat.E-mail2.1
HKEY_CLASSES_ROOT\Chilkat.E-mail2
HKEY_CLASSES_ROOT\Chilkat.E-mailBundle2.1
HKEY_CLASSES_ROOT\Chilkat.E-mailBundle2
HKEY_CLASSES_ROOT\Chilkat.MailMan2.1
HKEY_CLASSES_ROOT\Chilkat.MailMan2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mail2.1
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mail2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mailBundle2.1

HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatE-mailBundle2
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatMailMan2.1
HKEY_CLASSES_ROOT\ChilkatMail2.ChilkatMailMan2
HKEY_CLASSES_ROOT\Interface\{06544919-F559-4AE5-9001-F903BD8A84E6}
HKEY_CLASSES_ROOT\Interface\{51A0888C-9970-44DE-8C2C-835BA870D06F}
HKEY_CLASSES_ROOT\Interface\{5ACAE4B8-62D9-4124-A58A-9B1258B77E99}
HKEY_CLASSES_ROOT\Interface\{7D37DED8-1945-4E42-A3FD-B9620E0AD8E3}
HKEY_CLASSES_ROOT\Interface\{C4C23B78-DB98-444C-B601-DCAC6EBBEC54}
HKEY_CLASSES_ROOT\Interface\{CCB7FB40-99EC-4678-9202-52798DA78ABA}
HKEY_CLASSES_ROOT\Interface\{D12FB216-99DA-4EB3-9CC0-C0F760B174A0}
HKEY_CLASSES_ROOT\Interface\{D56C1AF1-3FDE-471C-9BC2-C52515F260C1}
HKEY_CLASSES_ROOT\Interface\{E656B867-992C-4462-A27D-EBE604EC3A48}
HKEY_CLASSES_ROOT\TypeLib\{1DF3AFED-99E0-4474-9900-954B8FD24E86}
HKEY_CLASSES_ROOT\CLSID\{A4643A87-99A0-4404-9BC5-2322BDD61637}
HKEY_CLASSES_ROOT\CLSID\{A46E5261-9956-4767-88CA-DFCED050D09E}
HKEY_CLASSES_ROOT\CLSID\{A7EC2CD3-9941-4FD4-9D01-105DC16A4313}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\KSM_is1

5. Thoát khỏi Registry.

25. Cách diệt Spyware Key Stalker

Mô tả

Phát hiện: Tháng 8 năm 2008.
Phiên bản: 4.02.
Tên: KeyStalker PRO.
Kiểu: Spyware.
Phát triển bởi: Brown Software Technologies.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\VB and VBA Program Settings\KeyStalker PRO
HKEY_LOCAL_MACHINE\SOFTWARE\Brown Software Technologies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{338DC50B-4C96-4293-8619- CB50D77CAB5A}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\Programs\Brown Software Technologies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\Brown Software Technologies

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\"MSRegScan" = "C:\Program Files\KSP Demo\KSPDemo.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\Memman.vxd" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\actskn43.ocx" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\dijpg.dll" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\ijl11.dll" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\msvbvm50.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\skinboxer43.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\msvcrt.dll" = "4"

5. Thoát khỏi Registry.

26. Cách diệt Spyware.Mod

http://images.google.com/imgres?imgurl=http://bakez.net/pix/spyware.gif&imgrefurl=http://www.spywarecover.info/how-to-choose-a-good-Anti-spyware-program/&h=249&w=278&sz=14&hl=vi&start=6&usg=__T7pXOYoxsIYd52aYIk9MIRipZv8=&tbnid=84tgw3bTCnju4

M:&tbnh=102&tbnw=114&prev=/images%3Fq%3Dspyware%26gbv%3D2%26hl%3Dvi%26rlz%3D1T4GZEZ_viVN282%26sa%3DG

Mô tả

Phát hiện: Tháng 8 năm 2008.
Tên: Spyware.Mod.
Kiểu: Spyware.
Phát triển bởi: QwertyStudio Canada.
Mức độ nguy hiểm: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\mod
   HKEY_LOCAL_MACHINE\SOFTWARE\mod

5. Thoát khỏi Registry.

27. Cách diệt Trojan.Purplebot

http://images.google.com/imgres?imgurl=https://www.rubbersbymail.com/images/condoms/Trojan_Extended_Pleas_LRG.jpg&imgrefurl=https://www.rubbersbymail.com/condoms/trojan_extended_pleasure.html&h=820&w=1024&sz=175&hl=vi&start=9&usg=__SNXbIvxA3uWFupikAkovAkj5GUY=&tbnid=njR6172ggADYQM:&tbnh=120&tbnw=150&prev=/i

mages%3Fq%3Dtrojan%26gbv%3D2%26hl%3Dvi%26rlz%3D1T4GZEZ_viVN282%26sa%3DG

Mô tả

Phát hiện: Tháng 8 năm 2008.

Tên: Trojan.Purplebot.

Kiểu: Trojan.

Mức độ phát tán: 45,056 Bytes.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"msvideoavicap" = "C:\WINDOWS\system\msvideoavicap.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\"gbpsvblust" = "C:\WINDOWS\system\gbpsvblust.exe"

5. Thoát khỏi Registry.

28. Cách diệt Trojan Bankpatch C

http://images.google.com.vn/imgres?imgurl=http://www.rivalart.com/Clipart-Kits/Mascot-Clipart/Trojan-Mascots/TROJAN-CLIPART-IMAGE.jpg&imgrefurl=http://www.rivalart.com/Clipart-Kits/Mascot-Clipart/Trojan-

Mascots/&h=325&w=307&sz=53&hl=vi&start=5&usg=__7BhlugteA9upa3TiLQgVsE0PXZ4=&tbnid=cRETHUuCITMJvM:&tbnh=118&tbnw=111&prev=/images%3Fq%3Dtrojan%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Phát hiện: Tháng 8 năm 2008.
Tên: Trojan.Bankpatch.C.
Kiểu: Trojan.
Mức độ phát tán: 34,304 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\"lwh" = "http://ffcsanta.com
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\rbt

5. Thoát khỏi Registry.

29. Cách diệt W32 Rispif A

http://images.google.com.vn/imgres?imgurl=http://www.canhtoan.com/dportal_resources/images/news/200804031626120.FV1645_computer_virus.jpg&imgrefurl=http://www.canhtoan.com/%3Fmod%3Dnews%26act%3Ddetail%26id%3D202

&h=602&w=800&sz=96&hl=vi&start=5&usg=__hC4GwZRFhCDNs3dMDubBRLQP9r0=&tbnid=TJHzImbpatWviM:&tbnh=108&tbnw=143&prev=/images%3Fq%3Dvirus%26gbv%3D2%26hl%3Dvi%26sa%3DG

Mô tả

Phát hiện: Tháng 8 năm 2008.

Tên: W32.Rispif.A.

Kiểu: Sâu.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\explorer\run\"explorer" = "%System%\wuauclt.exe"

5. Khôi phục lại các giá trị mặc định được ghi vào Registry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\"SHOWALL" = "2"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360rpt.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360safe.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360safebox.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360tray.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ANTIARP.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Ast.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AutoRunKiller.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AvMonitor.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AVP.COM\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AVP.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

Options\CCenter.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Frameworkservice.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\GFUpd.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\GuardField.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\IceSword.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Iparmor.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KASARP.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVPFW.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kavstart.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kmailmon.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KRegEx.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVMonxp.KXP\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVSrvXP.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVWSC.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kwatch.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Mmsk.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\msconfig.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\Navapsvc.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\nod32krn.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Nod32kui.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RAV.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavStub.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Regedit.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwmain.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwProxy.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwsrv.EXE\"debugger" =
"%System%\dllcache\wuauclt.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwstub.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Runiep.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\safeboxTray.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SREngLdr.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VPC32.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VPTRAY.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WOPTILITIES.EXE\"debugger" = "%System%\dllcache\wuauclt.exe"

6. Thoát khỏi Registry.

Chú ý: Trước khi có bất cứ việc chỉnh sửa nào trong Registry, bạn nên sao lưu lại Registry, tránh cho sự chỉnh sửa thất bại có thể gây ảnh hưởng đến hệ điều hành.

30. Cách diệt Spyware.KeyStalker

http://images.google.com/imgres?imgurl=http://www.antispywaresoftwaredownload.com/images/spyware-removers.gif&imgrefurl=http://www.antispywaresoftwaredownload.com/&h=390&w=308&sz=79&hl=vi&start=9&tbnid=JAMtX2i0TfgtEM:&tbnh=123&tbnw=97&prev=/images%3Fq%3Dspyware%26gbv%3D2%26hl%3Dvi%26rlz%3D1T4GZEZ_viVN287VN287

Mô tả

Phát hiện: Tháng 08 năm 2008.
Kiểu: Spyware.
Mức độ nguy hiểm: Trung bình.
Tên: KeyStalker PRO.
Viết bởi:Brown Software Technologies.
Phiên bản: 4.02.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_CURRENT_USER\Software\VB and VBA Program Settings\KeyStalker PRO
   HKEY_LOCAL_MACHINE\SOFTWARE\Brown Software Technologies
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{338DC50B-4C96-4293-8619-CB50D77CAB5A}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\Programs\Brown Software Technologies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\Brown Software Technologies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\"MSRegScan" = "C:\Program Files\KSP Demo\KSPDemo.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\Memman.vxd" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\actskn43.ocx" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\dijpg.dll" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\ijl11.dll" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\msvbvm50.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\skinboxer43.dll" = "2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls\"C:\WINDOWS\system32\msvcrt.dll" = "4"

5. Thoát khỏi Registry.

31. Cách diệt Registry Doctor 2008

Mô tả

Phát hiện: Tháng 07 năm 2008.
Kiểu: Lỗi chương trình ứng dụng.
Mức độ nguy hiểm: Trung bình.
Tên: RegistryDoctor2008.
Viết bởi:NewBonn, Inc.
Phiên bản:1.0.6.0.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"RegistryDoctor2008" = "43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 5C 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 44 00 6F 00 63 00 74 00 6F 00 72 00 32 00 30 00 30 00 38 00 5C 00 72 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 64 00 6F 00 63 00 74 00 6F 00 72 00 2E 00 65 00 78 00 65 00 00 00 00 00 0D 00 00 00 0A 00 00 00 A4 00 01 00 0C 00 00 00 00 00 00 00 00 00 00 00 46 00 00 00 54 00 00 00 57 00 00 00 41 00 00 00 52 00 00 00 45 00 00 00 5C 00 00 00 4D 00 00 00 69 00 00 00 63 00 00 00 72 00 00 00 6F 00 00 00 73 00 00 00 6F 00 00 00 66 00 00 00 74 00 00 00 5C 00 00 00 57 00 00 00 69 00 00 00 6E 00 00 00 64 00 00 00 6F 00 00 00 77 00 00 00 73 00 00 00 5C 00 00 00 43 00 00 00

75 00 00 00 72 00 00 00 72 00 00 00 65 00 00 00 6E 00 00 00 74 00 00 00 56 00 00 00 65 00 00 00 72 00 00 00 73 00 00 00 69 00 00 00 6F 00 00 00 6E 00 00 00 5C 00 00 00 52 00 00 00 75 00 00 00 6E 00 00 00 00 00 00 00 0 0 59 00 69 00 B5 00 D6 00 0E 00 00 00 0D 00 00 00 C8 00 10 00 66 00 00 00 E8 00 01 00 15 00 00 00 E8 00 01 00 15 00 00 00 5A 00 AC 00 E3 00 26 00 7F 00 61 00 C2 00 12 00 B9 00 BD 00 20 20 0E 00 F7 00 40 00 61 00 31 00 3A 20 D1 00 31 00 C5 00 1C 00 92 01 7D 01 AD 00 68 00 61 00 F4 00 92 01 03 00 43 00 3B 00 41 00 4D 00 4F 00 73 00 CE 00 6F 00 76 00 0E 00 19 20 CD 00 66 00 E8 00 F7 00 CD 00 F3 00 A3 00 B0 00 57 00 EF 00 DB 00 CE 00 F3 00 D6 00 22 20 A1 00 E0 00 37 00 FA 00 F1 00 08 00 CB 00 25 00 7F 00 29 00 1A 20 B3 00 D8 00 30 00 76 00 3A 20 09 00 0C 00 2F 00 0F 00 BE 00 8F 00 0F 00 C5 00 7B 00 53 01 4D 00 C2 00 C4 00"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\RegistryDoctor2008

5. Thoát khỏi Registry.

32. Cách diệt Spyware. UltimateKeylog

Mô tả

Phát hiện: Tháng 07 năm 2008.

Kiểu: Spyware.

Mức độ nguy hiểm: Trung bình.

Tên: Spyware.UltimateKeylog.

Viết bởi: KRyLack Software.

Phiên bản: 1.00.

Sự ảnh hưởng: Cao.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"ukl" = "C:\documents and Settings\All Users\Application Data\uklpr\wmpusrvc.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved\{E4F2CA1F-7ED0-25CB-5EEF-F26D9921AC33}
   HKEY_CURRENT_USER\Software\ukl
   HKEY_CLASSES_ROOT\CLSID\{E4F2CA1F-7ED0-25CB-5EEF-F26D9921AC33}

5. Thoái khỏi Registry.

33. Cách diệt Secure Expert Cleaner

Mô tả

Phát hiện: Tháng 07 năm 2008.
Kiểu: Lỗi chương trình ứng dụng.
Mức độ nguy hiểm: Trung bình.
Tên: SecureExpertCleaner.
Viết bởi: NewBonn, Inc.
Phiên bản: 1.0.7.1.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Reminder" = "%ProgramFiles%\SecureExpertCleaner\Reminder.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"SecureExpertCleaner" = "%ProgramFiles%\SecureExpertCleaner\sec.exe"
   HKEY_CURRENT_USER\Software\SEC
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\3P_USEC_is1
   HKEY_LOCAL_MACHINE\SOFTWARE\SEC
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider

5. Thoát khỏi Registry.

34. Cách diệt XLGuarder

Mô tả

Phát hiện: Tháng 7 năm 2008.

Tên: XLife Guarder Security Center.

Phát triển bởi: xlguarder.com.

Kiểu: Lỗi các chương trình ứng dụng.

Mức độ phát tán: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_ALL_USERS\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\"Shell" = "%Windir%\sysutils\sysutil.exe"
   HKEY_ALL_USERS\Software\sysutils
   HKEY_CLASSES_ROOT\CLSID\{D032570A-5F63-4812-A094-87D007C23012}
   HKEY_CLASSES_ROOT\iebho.TIEAdvBHO
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D032570A-5F63-4812-A094-87D007C23012}
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\sysutils

5. Thoát khỏi Registry.

35. Cách diệt Trojan.Wsnpoem

Mô tả

Phát hiện: Tháng 7 năm 2008.
Kiểu: Trojan.
Tên: Trojan.Wsnpoem.
Mức độ phát tán: 68,608 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"userinit" = "%System%\ntos.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\"UID" = "[COMPUTERNAME]_[UNIQUE_ID]"

5. Khôi phục lại các giá trị mặc định:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Userinit" = "%System%\userinit.exe, %System% \ntos.exe

6. Thoát khỏi Registry.

36. Cách diệt W32.Azero.A

Mô tả

Phát hiện: Tháng 7 năm 2008.
Tên: W32.Azero.A.
Kiểu: Virus.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"VisualStyle" = "%System%\desktop.sysm"

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sysm\
" @" = "system mechanic"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sysm\
defaulticon\"@" = "%System%\netsetup.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sysm\
shell\open\command\"@" = "%1"
HKEY_LOCAL_MACHINE\SYSTEM\controlset001\cont
rol\safeboot\"alternateshell" =
"%System%\commandprompt.sysm"
HKEY_LOCAL_MACHINE\SYSTEM\controlset002\cont
rol\safeboot\"alternateshell" =
"%System%\commandprompt.sysm"
HKEY_LOCAL_MACHINE\SYSTEM\currentcontrolset\c
ontrol\safeboot\"alternateshell" =
"%System%\commandprompt.sysm"

5. Khôi phục lại các giá trị mặc định trong Registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced\"Hidden" = "2"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced\"HideFileExt" = "1"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced\"ShowSuperHidden" = "0"
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\cabinetstate\"FullPathAddress"" = "0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows\CurrentVersion\Explorer\Advanced\Folder\HideFile
Ext\"checkedvalue" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows\CurrentVersion\Explorer\Advanced\Folder\HideFile
Ext\"defaultvalue" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows\CurrentVersion\Explorer\Advanced\Folder\ShowFull
Path\"defaultvalue" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows\CurrentVersion\Explorer\Advanced\Folder\ShowFull Path\"uncheckedvalue" = "0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\ShowFull PathAddress\"defaultvalue" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\ShowFull PathAddress\"uncheckedvalue" = "0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\"checkedvalue" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\"defaultvalue" = "1"

6. Thoát khỏi Registry.

37. Cách diệt WistaAntivirus

Mô tả

Phát hiện: Tháng 7 năm 2008.

Tên: Wista Antivirus.

Phiên bản: 1.0.

Tạo bởi: Wista-Antivirus.

Mức độ: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"wistaantivirus" = "C:\Program Files\WistaAntivirus\wistaantivirus.exe"
HKEY_CURRENT_USER\Software\wistaantivirus
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wista Antivirus_is1

5. Thoát khỏi Registry.

38. Cách diệt Anti Virus XP 2008

Mô tả

Phát hiện: Tháng 7 năm 2008.

Kiểu: Lỗi chương trình ứng dụng.

Mức độ: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform\"AntivirXP08" = "AntivirXP08"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"[RANDOM NAME]" = "C:\Program Files\[RANDOM NAME]\[RANDOM NAME].exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\[RANDOM NAME]

HKEY_LOCAL_MACHINE\SOFTWARE\[RANDOM NAME]
KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\[RANDOM NAME]

5. Thoát khỏi Registry.

39. Cách diệt SpywareScanner2008

Mô tả

Phát hiện: Tháng 07 năm 2008.

Tên: SpywareScanner2008.

Kiểu: Làm lỗi chương trình ứng dụng.

Phiên bản: 1.0.

Tạo bởi: SpywareISOScanner.com.

Mức độ: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"spywarescanner" = "C:\Program Files\SpywareScanner\spywarescanner.exe"
HKEY_CURRENT_USER\Software\SpywareScanner2008
HKEY_CURRENT_USER\Software\spywarescanner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SpywareScanner 2008_is1

5. Thoát khỏi Registry.

40. Cách diệt Backdoor.Lancafdo

Mô tả

Phát hiện: Tháng 7 năm 2008.
Kiểu: Trojan.
Mức độ phát tán: 16,384 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"Type" = "00000010"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"Start" = "00000002"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"ObjectName" = "LocalSystem"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"ImagePath" = "%System%\mssrv32.exe"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"ErrorControl" = "00000000"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"DisplayName" = "Microsoft security update service"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\msupdate\"Description" = "This service downloading and installing Windows security updates"
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\AFD\Parameters\"DisableRawSecurity" = "00000001"

5. Thoát khỏi Registry.

41. Cách diệt Trojan.Ushedix

Mô tả

Phát hiện: Tháng 6 năm 2008.

Kiểu: Trojan.

Mức độ phát tán: 19,381 Bytes.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\avp.com\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\avp.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\runiep.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFW.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\FYFireWall.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwmain.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution
Options\rfwsrv.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVPF.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFW32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\nod32kui.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\nod32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Navapsvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Navapw32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\avconsol.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Webscanx.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\NPFMntor.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\vsstat.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\KPfwSvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Ras.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavMonD.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\mmsk.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\WoptiClean.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\QQKav.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\QQDoctor.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\EGHOST.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\360Safe.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\iparmo.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\adam.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\360rpt.exe\"Debugger" = "ntsd -d"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360tray.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AgentSvr.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AppSvc32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\autoruns.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\avgrssvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AvMonitor.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CCenter.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ccSvcHst.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\FileDsty.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\FTCleanerShell.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HijackThis.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution
Options\Iparmor.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\isPwdSvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kabaload.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KaScrScn.SCR\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KASMain.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KASTask.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVDX.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVPFW.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVSetup.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAVStart.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KISLnchr.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\KMailMon.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KMFilter.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFW32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFW32X.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KPFWSvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KRegEx.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KRepair.com\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KsLoader.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVCenter.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KvDetect.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KvfwMcl.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVMonXP.kxp\"Debugger" = "ntsd -d"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVMonXP_1.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kvol.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kvolself.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KvReport.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVScan.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVSrvXP.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KVStub.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kvupload.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\kvwsc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KvXP.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KvXP_1.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution
Options\KWatch.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KWatch9x.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KWatchX.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\MagicSet.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\mcconsol.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\nmqczj.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\KAV32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\nod32krn.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\PFWLiveUpdate.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\QHSET.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RavMonD.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\RavStub.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RegClean.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwcfg.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RfwMain.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwsrv.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RsAgent.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Rsaupd.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\safelive.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\scan32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\shcfg32.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\SmartUp.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\SREng.EXE\"Debugger" = "ntsd -d"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\symlcsvc.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\SysSafe.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TrojanDetector.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\Trojanwall.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\TrojDie.kxp\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UIHost.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UmxAgent.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UmxAttachment.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UmxCfg.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UmxFwHlp.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\UmxPol.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win

dows NT\CurrentVersion\Image File Execution
Options\UpLive.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\procexp.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwstub.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RegTool.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\rfwProxy.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\RawCopy.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\CCenter.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\filemon.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\regmon.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\AntiArp.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution
Options\GFUpd.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win
dows NT\CurrentVersion\Image File Execution

Options\GFRing3.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\taskmgr.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQDoctorMain.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SelfUpdate.exe\"Debugger" = "ntsd -d"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Your Image File Name Here without a path\"Debugger" = "ntsd -d"

5. Thoát khỏi Registry.

42. Các diệt PestSweeper

Mô tả

Phát hiện: Tháng 6 năm 2008.
Kiểu: Misleading Application (Lỗi các chương trình ứng dụng).
Phiên bản: 1.0.
Phát triển: PestSweeper.com.
Mức độ: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"pestsweeper" = "C:\Program

Files\PestSweeper\pestsweeper.exe"
HKEY_CURRENT_USER\Software\pestsweeper
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\PestSweeper_is1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\Programs\PestSweeper
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\PestSweeper

5. Thoát khỏi Registry.

43. Các diệt Trojan.Blusod

Mô tả

Phát hiện: Tháng 6 năm 2008.
Kiểu: Trojan.
Mức độ phát tán: 109,056 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Sysinternals\Bluescreen Screen Saver\"EULAAccepted" = "1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"lph[RANDOM CHARACTERS]" = "%System%\lph[RANDOM CHARACTERS].exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Soft

ware Notifier\"InstallationID" = "906b1f2d-66b5-439e-8c02-9d08858fe527"
HKEY_CURRENT_USER\Control Panel\Desktop\"ConvertedWallpaper" = "%System%\ph[RANDOM CHARACTERS].bmp"
HKEY_CURRENT_USER\Control Panel\Desktop\"SCRNSAVE.EXE" = "%System%\blph[RANDOM CHARACTERS].scr"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\"NoDispBackgroundPage" = "0"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\"NoDispScrSavPage" = "0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\"DisableSR" = "0"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\sr\"Start" = "0"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\sr\"ImagePath" = "*system32\DRIVERS\sr.sys*"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\sr\Parameters\"FirstRun" = "0"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sr\"Start" = "0"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sr\"ImagePath" = "*system32\DRIVERS\sr.sys*"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sr\Parameters\"FirstRun" = "0"
HKEY_CURRENT_USER\Control Panel\Colors\"Background" = "0 0 255"
HKEY_CURRENT_USER\Control Panel\Desktop\"ScreenSaveActive" = "1"
HKEY_CURRENT_USER\Control Panel\Desktop\"TileWallpaper" = "0"

5. Thoát khỏi Registry.

44. Cách diệt Adware.Rabio

Mô tả

Phát hiện: Tháng 3 năm 2008.
Kiểu: Adware.
Phiên bản: 4.1.0.0.
Tên: RCSE.
Viết bởi: Rabio.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform\Rabio RCSE (4.4.0.0) = " "
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{1C2E5D27-A17C-4D89-85DD-3553C189380D}
HKEY_CURRENT_USER\Software\RCSE
HKEY_CLASSES_ROOT\AppID\RCSE.DLL
HKEY_CLASSES_ROOT\AppID\{89CC26BC-9256-4CCA-A7F3-B9D6C48DBA71}
HKEY_CLASSES_ROOT\CLSID\{1C2E5D27-A17C-4D89-85DD-3553C189380D}
HKEY_CLASSES_ROOT\Interface\{923CA88A-AE69-49AF-BF65-9A3123B14CCB}
HKEY_CLASSES_ROOT\Rabio.RabioBHO.1

HKEY_CLASSES_ROOT\Rabio.RabioBHO
HKEY_CLASSES_ROOT\TypeLib\{8C36D71B-0A48-4D38-9DEF-2A2A2669D0C9}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1C2E5D27-A17C-4D89-85DD-3553C189380D}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Rabio
HKEY_LOCAL_MACHINE\SOFTWARE\Rabio

5. Thoát khỏi Registry.

45. Cách diệt Spyware.NokKernel

Mô tả

Phát hiện: Ngày 22 tháng 6 năm 2008.
Kiểu: Spyware.
Phiên bản: 1.2.090.
Tên: Spyware.NokKernel.
Viết bởi: Spin Networks.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\"NokKernel install" = "%System%\Nok_install.exe"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32ins
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\fsram

5. Thoát khỏi Registry.

46. Cách diệt W32.Ircbrute

Mô tả

Phát hiện: Ngày 20 tháng 6 năm 2008.

Cập nhật: Ngày 21 tháng 6 năm 2008. (8:51:56 AM).

Kiểu: Sâu.

Mức độ phát tán: 12,506 Bytes.

Tên: W32.Ircbrute.

Viết bởi: Sean Kiernan.

Sự ảnh hưởng: Rất nhỏ.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"internet security manager" = "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\dll32.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Printer Spooler" = "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\spoolsv.exe"

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{28ABC5C0-4FCB-11CF-AAX5-81CX1C635612}\"StubPath": "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\dll32.exe"
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{88ABC5C0-4FCB-11BB-AAX5-81CX1C635612}\"StubPath" = "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\spoolsv.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{28ABC5C0-4FCB-11CF-AAX5-81CX1C635612}\"StubPath": "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\dll32.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{88ABC5C0-4FCB-11BB-AAX5-81CX1C635612}\"StubPath" = "c:\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\spoolsv.exe"
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{28ABC5C0-4FCB-11CF-AAX5-81CX1C635612}
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{88ABC5C0-4FCB-11BB-AAX5-81CX1C635612}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{28ABC5C0-4FCB-11CF-AAX5-81CX1C635612}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{88ABC5C0-4FCB-11BB-AAX5-81CX1C635612}

5. Thoát khỏi Registry.

47. Cách diệt Spyware.PornCleanser

Mô tả

Phát hiện: Ngày 6 tháng 6 năm 2008.
Cập nhật: Ngày 6 tháng 6 năm 2008 (11:32:30 AM).
Kiểu: Adware.
Mức độ phát tán: 267,264 Bytes.
Tên: PornCleanser.
Viết bởi: L. F. Grundy Software Company.
Phiên bản: 1.04.2008.
Sự ảnh hưởng: Trung bình.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Service Host" = "C:\Program Files\PC\svchosts.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\"wndriversap" = "[RANDOM NAME]"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\"PcPwd" = "0"
HKEY_CURRENT_USER\Software\VB and VBA Program Settings
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\PornCleanser
HKEY_CURRENT_USER\Software\VB and VBA

Program Settings\PornCleanser\Settings
HKEY_CURRENT_USER\Software\VB and VBA
Program Settings\PornCleanser\Startup
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\BitBucket\c

5. Thoát khỏi Registry.

48. Cách diệt Adware.Okcashbackmall

Mô tả

Phát hiện: Ngày 29 tháng 4 năm 2008.
Cập nhật: Ngày 29 tháng 4 năm 2008 (9:17:10 AM).
Kiểu: Adware.
Mức độ phát tán: 267,264 Bytes.
Tên: Adware.Okcashbackmall.
Viết bởi: Okcashbackmall install.
Phiên bản: 1.0.0.0
Sự ảnh hưởng: Trung bình
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunOnce\"dwqblwppx.exe" =
"C:\WINDOWS\system32\dwqblw[RANDOM
CHARACTERS].exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\RunOnce\"dwqblwpvl.exe" = "C:\WINDOWS\system32\dwqblw[RANDOM CHARACTERS].exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"dwqblwrsq.exe" = "C:\WINDOWS\system32\dwqblw[RANDOM CHARACTERS].exe"

5. Khôi phục lại các giá trị mặc định sau trong Registry:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{1DE525ED-EF71-4119-8C3C-1CE5315ADA74}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{D04358AE-CE03-4A26-9F02-69C4D3A5267F}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
HKEY_CLASSES_ROOT\CLSID\{1DDE8A86-89D8-4B55-A936-65C40B6A8DD0}
HKEY_CLASSES_ROOT\CLSID\{1DE525ED-EF71-4119-8C3C-1CE5315ADA74}
HKEY_CLASSES_ROOT\CLSID\{4D2D9681-C234-47A3-B499-9CEE26FF54C2}
HKEY_CLASSES_ROOT\CLSID\{7AC1D6D1-B83B-4D77-A916-839F90216BC7}
HKEY_CLASSES_ROOT\CLSID\{D04358AE-CE03-4A26-9F02-69C4D3A5267F}
HKEY_CLASSES_ROOT\cashbackkorea.cashbackkorea.com
HKEY_CLASSES_ROOT\cashbackkoreabar.cashbackkorea
HKEY_CLASSES_ROOT\cashbacksys.cashbacksys.com
HKEY_CLASSES_ROOT\cashbacksysbar.cashbacksys.com
HKEY_CLASSES_ROOT\mizane.mizane.com
HKEY_CLASSES_ROOT\mizanebar.mizane.com
HKEY_CLASSES_ROOT\okcashbackmall.okcashbackmall.com

HKEY_CLASSES_ROOT\okcashbackmallbar.okcashback mall.com.Bar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win dows\CurrentVersion\Explorer\Browser Helper Objects\{1DDE8A86-89D8-4B55-A936-65C40B6A8DD0}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win dows\CurrentVersion\Explorer\Browser Helper Objects\{4D2D9681-C234-47A3-B499-9CEE26FF54C2}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win dows\CurrentVersion\Explorer\Browser Helper Objects\{7AC1D6D1-B83B-4D77-A916-839F90216BC7}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo ws\CurrentVersion\Uninstall\Windows cashbackkorea Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo ws\CurrentVersion\Uninstall\Windows cashbacksys Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo ws\CurrentVersion\Uninstall\Windows mizane Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win dows\CurrentVersion\Uninstall\okcashbackmall Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\cashbackkorea

6. Thoát khỏi Registry.

49. Cách diệt SpyGuarder

Mô tả

Phát hiện: Ngày 23 tháng 5 năm 2008.
Cập nhật: Ngày 23 tháng 5 năm 2008 (12:12:39 PM).
Kiểu: Làm lỗi chương trình ứng dụng.
Phiên bản: 2.1.
Tên: SpyGuarder.
Viết bởi: Trixo Development.
Sự ảnh hưởng: Trung bình.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"SpyGuarder" = "C:\Documents and Settings\Administrator\spyguarder.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F3642B57-3EA8-4EEA-A643-9DE138381A57}
HKEY_CLASSES_ROOT\CLSID\{F3642B57-3EA8-4EEA-A643-9DE138381A57}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{F3642B57-3EA8-4EEA-A643-9DE138381A57}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F3642B57-3EA8-4EEA-A643-9DE138381A57}

5. Thoát khỏi Registry.

50. Cách diệt Spyware.ExpressKeylog

Mô tả

Phát hiện: Ngày 30 tháng 5 năm 2008.
Cập nhật: Ngày 30 tháng 5 năm 2008 (11:26:02 AM).
Kiểu: Spyware.
Mức độ phát tán: 2,223,616 Bytes.
Tên: Keylogger Express.

Viết bởi: Startupsoft.com.
Sự ảnh hưởng: Trung bình
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\"hsys" = "C:\PROGRAM FILES\PCMONITOR\HSYS.EXE"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations

5. Thoát khỏi Registry.

51. Cách diệt Spyware.TupInsight

Mô tả

Phát hiện: Ngày 5 tháng 6 năm 2008.
Cập nhật: Ngày 5 tháng 6 năm 2008 (2:03:50 PM).
Kiểu: Spyware.
Mức độ phát tán: 2,223,616 Bytes.
Tên: TupInsight.
Viết bởi: Tup Software Ltd.
Sự ảnh hưởng: Cao.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CLASSES_ROOT\WsSysSet
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WsSysSet
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WsSys Set\WsSysInfoExt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Win dows\CurrentVersion\Uninstall\{89CA9704-64BD-4620-8BB3-CA3F4C937034}
HKEY_ALL_USERS\Software\Microsoft\Windows\Curre ntVersion\Explorer\MenuOrder\Start Menu2\Programs\Tupsoft TupInsight
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\En um\Root\LEGACY_TUPINSIGHTCAPTUREENGINE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\En um\Root\LEGACY_TUPINSIGHTCAPTUREENGINE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Enum\Root\LEGACY_TUPINSIGHTCAPTUREENGINE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Ser vices\TupInsightCaptureEngine
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Ser vices\TupInsightCaptureEngine
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\TupInsightCaptureEngine
HKEY_CURRENT_USER\Software\Classes\VirtualStore\ MACHINE\SOFTWARE\Classes\WsSysSet
HKEY_CURRENT_USER\Software\Classes\VirtualStore\ MACHINE\SOFTWARE\Classes\WsSysSet\WsSysInfoExt
HKEY_CURRENT_USER\Software\Classes\VirtualStore\ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi

on\Uninstall\{89CA9704-64BD-4620-8BB3-CA3F4C937034}
HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Classes\WsSysSet
HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Classes\WsSysSet\WsSysInfoExt
HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{89CA9704-64BD-4620-8BB3-CA3F4C937034}
HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\UAS

5. Khôi phục lại giá trị ban đầu:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst

6. Thoát khỏi Registry.

52. Cách diệt Adware.Peppi

Mô tả

Phát hiện: Ngày 13 tháng 6 năm 2008.
Cập nhật: Ngày 13 tháng 6 năm 2008 (8:42:48 PM).
Kiểu: Adware.
Mức độ phát tán: 721,920 Bytes.
Tên: Pepi.
Viết bởi: Synatix GmbH.
Sự ảnh hưởng: Cao.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.

3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"vhost" = "%System%\host.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\peppi (Vorlagen-Wizzard)\"DisplayName" = "peppi (Vorlagen-Wizzard)"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\peppi (Vorlagen-Wizzard)\"UninstallString" = "C:\Program Files\peppi_vorlagen\lisys.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"AutoConfigURL" = "**Error! Hyperlink reference not valid.** Data\proxy.pac"
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\"EnableAutoProxyResultCache" = "0"

5. Thoát khỏi Registry.

53. Cách diệt Backdoor.Bifrose.L

Mô tả

Phát hiện: Ngày 12 tháng 6 năm 2008
Cập nhật: Ngày 12 tháng 6 năm 2008(4:27:32 PM).
Kiểu: Sâu
Mức độ phát tán: 53,248 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.

4. Tìm và xoá các giá trị:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"waults" = "%System%\waults.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"netview" = "%System%\netview.exe"
   HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\"waults" = "%System%\waults.exe"
   HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\"waults" = "%System%\waults.exe"
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}\"stubpath" = "%System%\netview.exe s"
   HKEY_CURRENT_USER\Identities\"Last User Identity" = "0x00029B46"
   HKEY_LOCAL_MACHINE\SOFTWARE\SKav\nck
   HKEY_CURRENT_USER\SOFTWARE\SKav
   HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}
   HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}
   HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\SKav
   HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Skav

5. Thoát khỏi Registry.

54. Diệt virus W32.SillyDC và W32.Almanahe.B!inf

- Tác hại: Không tắt USB được và một số phiền toái khác.

Khi virus này chạy, nó tự copy nó vào thư mục %Windir% hoặc %System%. Sau đó nó tạo một khoá trong Registry để mỗi khi mở máy là nó tự khởi động, mà đôi khi nó không tạo một khóa như cách thông thường là Run, RunOnce... mà nó có thể tạo tại bất cứ điểm nào trong Regitry, miễn sau các điểm nó ghi lên có thể chạy mỗi khi mở máy. Virus này tự download một số phần mềm gián điệp.

Có thể dùng bất cứ phần mềm nào diệt virus cũng có thể diệt được.

55. Cách diệt Virus W32.Almanahe.B!inf

- Mức độ phá hoại: Rất thấp.
- Trước đây virus có tên là W32.Corerink.A!inf.
- Loại virus: Virus
- Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

Virus này ảnh hưởng tới file explorer.exe, do đó các chương trình mở lên sẽ tự nhiên bị nhiễm theo và làm cho máy chạy chậm lại. Đây là loại virus ảnh hưởng theo kiểu sâu Worm nên mục đích chính của nó là download các phần mềm độc hại về máy và đánh cắp thông tin.

Có thể dùng Symantec Antivirus để diệt.

56. Cách diệt W32.Emsenush.A

Mô tả

Phát hiện: Ngày 28 tháng 5 năm 2008.

Cập nhật: Ngày 28 tháng 5 năm 2008 (1:00:53 PM).

Kiểu: Sâu.

Mức độ phát tán: 53,248 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"csrss" = "%Windir%\csrss.exe"
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"MSMSGS" = "[PATH TO INSTANT MESSAGE EXECUTABLE] /background"
5. Thoát khỏi Registry.

57. Cách diệt Trojan.Spryct

Mô tả

Phát hiện: Ngày 26 tháng 5 năm 2008.
Cập nhật: Ngày 26 tháng 5 năm 2008 (1:18:34 PM).
Kiểu: Trojan.
Mức độ phát tán: 79,360 Bytes.
Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.

4. Tìm và xoá các giá trị:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\crypt\"Asynchronous" = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\crypt\"DllName" = "crypts.dll"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\crypt\"Impersonate" = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\crypt\"StartShell" = "Run"

5. Thoát khỏi Registry.

58. Cách diệt virus W32.Tufik.E

Mô tả

Phát hiện: Ngày 17 tháng 05 năm 2008.

Cập nhật: Ngày 17 tháng 05 năm 2008 (10:22:01 AM).

Kiểu: Virus.

Mức độ phát tán: 60,141 Bytes.; 82,944 Bytes.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Cách diệt

1. Vào Start > Run.
2. Gõ Regedit.
3. Click chọn OK.
4. Tìm và xoá các giá trị:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{C1498DA0-135E-46EA-B01B-86042A31ED82}
HKEY_CURRENT_USER\TypeLib\{C1498DB2-135E-46EA-B01B-86042A31ED82}
HKEY_CURRENT_USER\Interface\{C1498DBF-135E-46EA-B01B-86042A31ED82}HKEY_CURRENT_USER\IEFalgObj.IEFalgObj
HKEY_CURRENT_USER\IEFalgObj.IEFalgObj.1
HKCR\CLSID\{C1498DA0-135E-46ea-B01B-86042A31ED82
HKEY_USERS\.default\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{C1498DA0-135E-46EA-B01B-86042A31ED82}

5. Thoát khỏi Registry.

59. Cách diệt Trojan.Cymdos

Mô tả

Phát hiện: Ngày 16 tháng 5 năm 2008.

Cập nhật: Ngày 16 tháng 5 năm 2008 (1:53:20 PM).

Kiểu: Trojan.

Hệ thống bị ảnh hưởng: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

Chú ý: Những chỉ dẫn sau đây gắn liền với mọi sản phẩm diệt của virus Symantec hiện thời và gần đây, bao gồm chương trình diệt virus Symantec và những mặt hàng diệt virus của Norton.

1. Tắt chế độ System Restore (Windows Me/XP).
2. Cập nhật những chương trình diệt virus mới