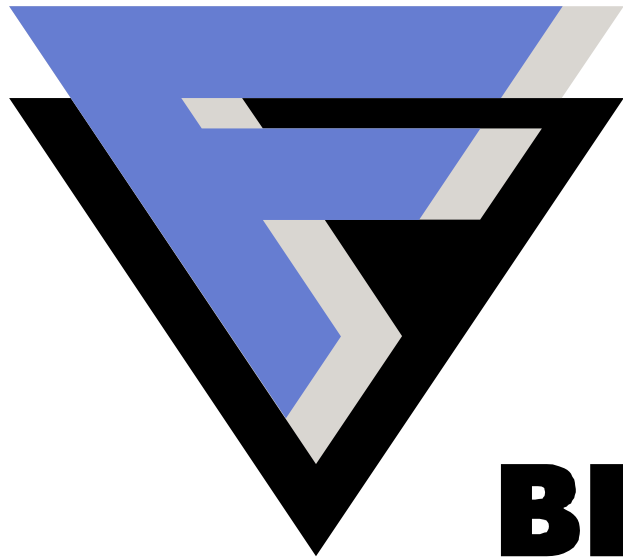


Virus Bulletin 2006 Montreal KEYNOTE

F-SECURE[®]



BE SURE.

Mikko Hypponen
Chief Research Officer
F-Secure Corporation

www.f-secure.com

www.hypponen.com

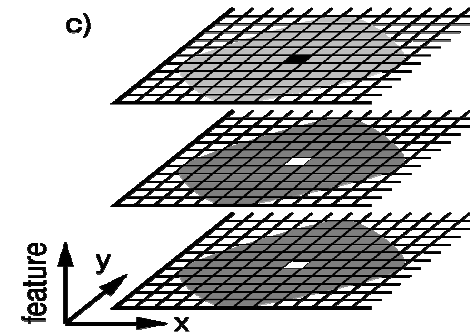
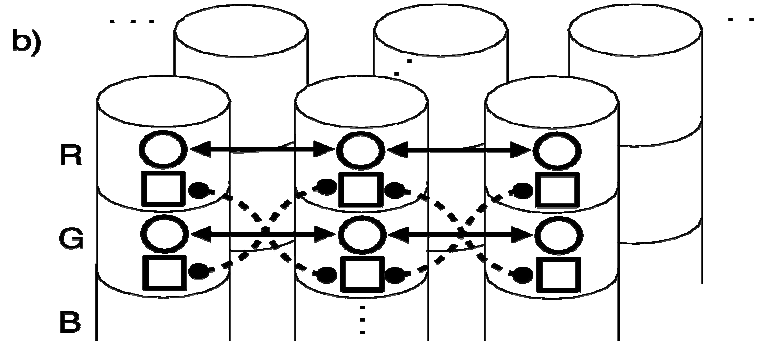
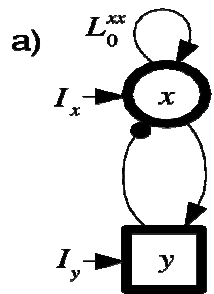
$$g_\alpha(x) = \begin{cases} m_\alpha(x - \theta_\alpha) & \text{if } x > \theta_\alpha \\ 0 & \text{else} \end{cases}$$

$$g_\alpha(x) = \begin{cases} m_\alpha(x - \theta_\alpha) & \text{if } x > \theta_\alpha \\ 0 & \text{else} \end{cases}$$

Simplified example

$$I_x^{lat} = \sum_{s \in S} L_s^{xx} x_s$$

$$I_y^{lat} = \sum_{s \in S} L_s^{yy} y_s$$



(a) Computer virus consists of an excitatory (x) and an inhibitory (y) binary neuron. Each neuron represents the average activity of a cluster of biological cells.

(b) Synchronizing connections (solid) holds between oscillators within one layer and desynchronizing connections (dotted) between different layers. “R” and “G” denote the red and green channel.

(c) Oscillators are arranged in a 3D-topology. The shaded circles visualize the range of synchronizing (light gray) and desynchronizing (dark gray) connections of a neuron in the top layer (black pixel).

$$I_\alpha = I_\alpha^0 + I_\alpha^{lat} - I_\alpha^{norm}$$

$$I_x^{lat} = \sum_{s \in S} L_s^{xx} x_s$$

$$I_y^{lat} = \sum_{s \in S} L_s^{yy} y_s$$

$$L_s^{\alpha\alpha} = \begin{cases} \frac{j^\alpha}{\sqrt{2\pi\sigma^2}} \exp\left(-\left(\frac{d(s)}{2\sigma}\right)^2\right) & \text{if } d(s) < r \\ 0 & \text{else} \end{cases}$$

$$\dot{x} = -\tau_x x - g_y(y) + L_0^{xx} g_x(x) + I_x + \eta_x$$

$$\dot{y} = -\tau_y y + g_x(x) - I_y + \eta_y$$

$$g_\alpha(x) = \begin{cases} m_\alpha(x - \theta_\alpha) & \text{if } x > \theta_\alpha \\ 0 & \text{else} \end{cases}$$

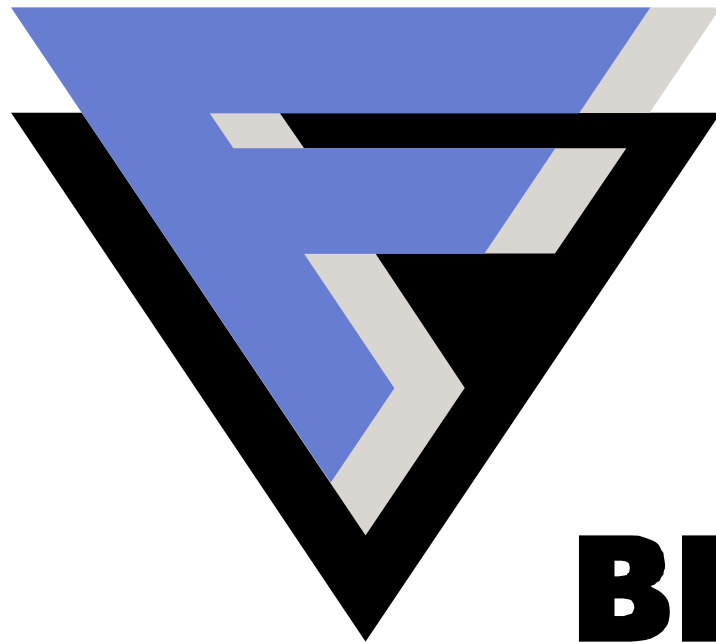
Hello

name:

Mikko Hyppönen

CRO

F-SECURE[®]



BE SURE.

Helsinki





1990

300 PC viruses

200,000

Good

Evil



2006
MONTREAL

Canada!

eh

VIRUS
BULLETIN
VIRUS
INTERNATIONAL
CONFERENCE

93

Mikko Hypponen
Data Fellows Ltd, Finland

VIRUS
BULLETIN
VIRUS
INTERNATIONAL
CONFERENCE

94

SPEAKER

MIKKO HYPÖNNEN
DATA FELLOWS, FINLAND

VIRUS
BULLETIN
VIRUS
INTERNATIONAL
CONFERENCE

'95

SUBSCRIBER

MIKKO HYPONEN
DATA FELLOWS LTD, FINLAND

Keynote

Criminal investigation

For-profit botnet gang

Attacked us

Investigation

Several months

Busted

3 arrests

Excellent case study

Keynote



2006
MONTREAL

www.f-secure.com/weblog



Tuesday, September 5, 2006

Keynoting

Posted by Mikko @ 13:22 GMT

Virus Bulletin is the most important annual conference of the antivirus industry. This year's conference, VB2006, will be held next month in Montreal, Canada.

I've attended every VB Conference since 1993, so I was honored to learn that this year I have been invited to deliver the keynote presentation on the first day of the conference. Cool.

So, here's a rare opportunity to address hundreds of people working in my field. What to speak about? Well, I came up with a brilliant idea of documenting a recent case we were working with: an investigation into an underground network gang. Great.

The problem is that a friendly authority has just told me that I cannot speak about that case. Oops.

I have one month to come up with something, so I'm looking for help. Any ideas? What should I talk about in my keynote presentation at VB2006?

| | | |
|---|---|--|
|  | Opening address | |
| | Case: Virus X Mikko Hyppönen , F-Secure | |
| Data exfiltration techniques: how attackers steal your sensitive data Rob Murawski , CERT Coordination Center | | |
| Lunch | | |
| The myth of user education Stefan Göring , Royal Institute of Technology, Stockholm | Using expert systems for automated analysis systems: advantages and techniques Ryan Hicks , iCSA Labs | |
| User education: teaching techniques and learning styles for damage limitation Peter Cooper , Sophos | Real-time multilanguage threat descriptions using an intelligent template system | |

F-Secure - September 5th Poll

What should Mikko's VB Keynote presentation be?

- A generic product sales pitch
- ...or tell us your suggestion:



F-Secure - September 5th Poll

What should Mikko's VB Keynote presentation be?

- A generic product sales pitch
- ...or tell us your suggestion:

Submit

BE SURE

2006

19886



Brain

Stoned

Cascade

Yankee Doodle

Dark Avenger

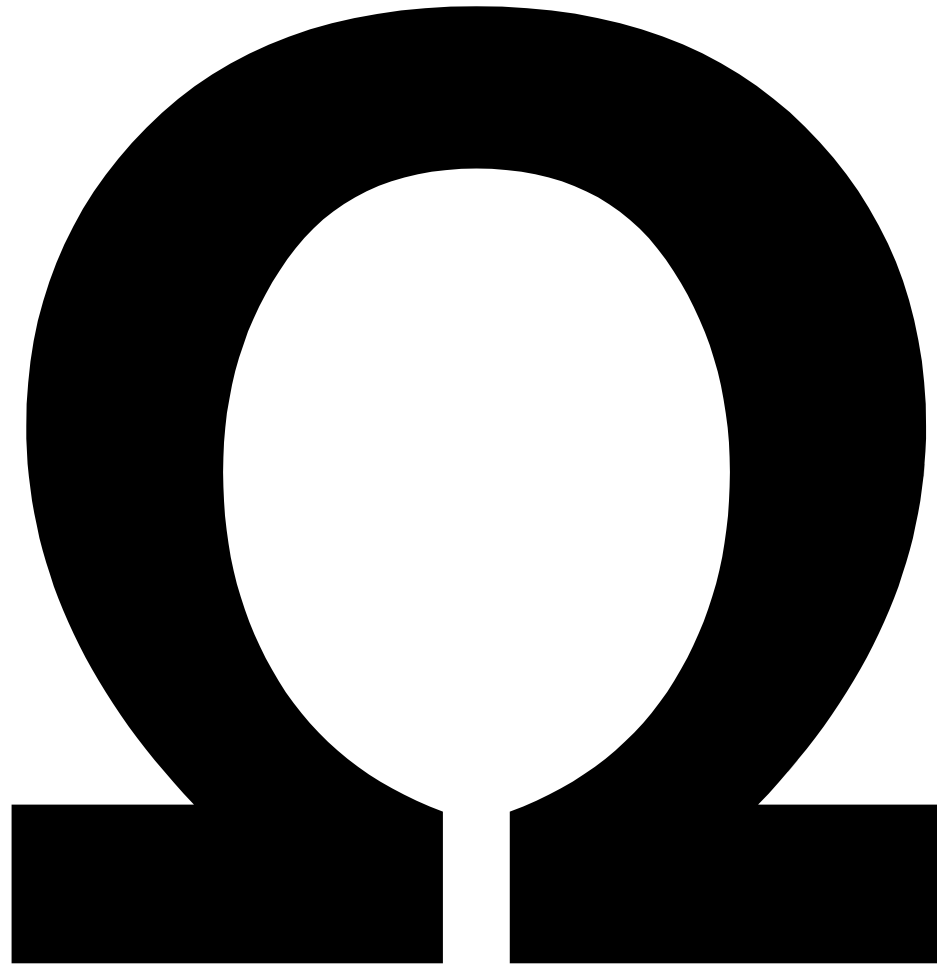
Form

1991

Omega

13th of September

1991





Michelangelo

V-Sign

<C:\horror\vdemo\ELVIRA-G.COM>

<C:\horror\vdemo\Q-V-SIGN.COM>

<C:\horror\vdemo\WALKER.COM>

DENZUKO

Type "Happy Birthday Joshi" !

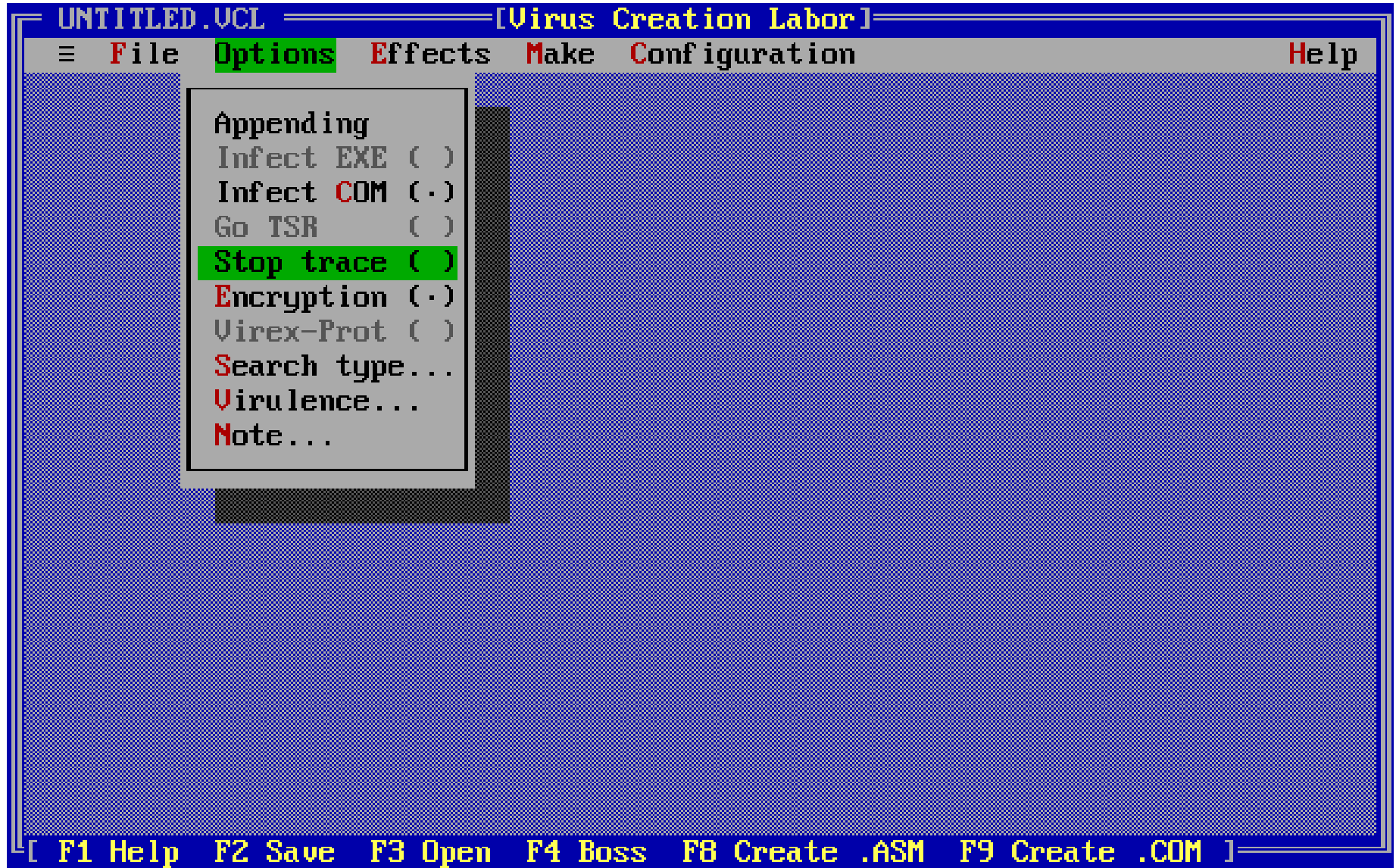
<C:\horror\vdemo\ELVIRA-G.COM>

<C:\horror\vdemo\MARS-G.COM>

<C:\horror\vdemo\Q-CASINO.COM>

MtE

VCL



WinVir

Monkey

One_half

Concept

Bail:

```
If Err <> 102 Then
```

```
FileSaveAs dlg
```

```
End If
```

Done:

```
End Sub
```

Payload:

```
Sub MAIN
```

```
    REM That's enough to prove my point
```

```
End Sub
```


Laroux

Good

Evil

Boza



Bizatch by Quantum / VLAD



The taste of fame just got tastier!
VLAD Australia does it again with the world's first Win95 Virus

From the old school to the new..

Metabolis

Qark

Darkman

Automag

Antigen

RhinceWind

Quantum

Absolute Overlord

CoKe

OK

Marburg



My Computer

Setup for Microsoft Internet Explorer 3.01

Network Places

Inbox

Recycle Bin

My Briefcase

Set Up The Microsoft Network

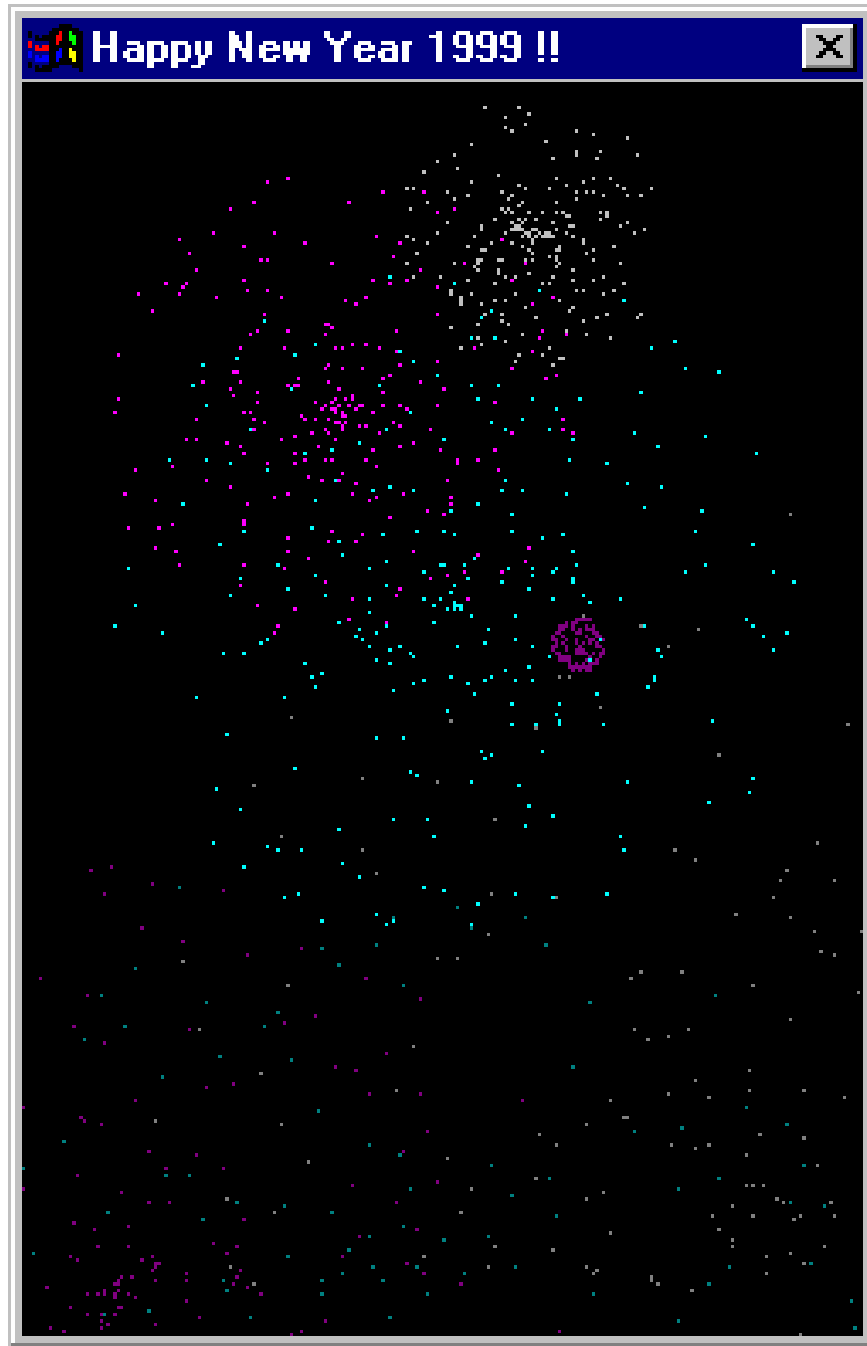
Start

En

1:15 AM

Remote Explorer

1998



Funlove

ZipperedFiles

Melissa

1999

Bubbleboy

 **BubbleBoy is back! - Message (HTML)** _ □ X


File Edit View Insert Format Tools Actions Help

 Send



Options... >>

Arial >>

 This message has not been sent.

To...

Cc...

Bcc...

John Doe

Subject:

BubbleBoy is back!

The BubbleBoy incident, pictures and sounds

<http://www.towns.com/dorms/tom/bblboy.htm> ■ ■

Loveletter

Date: Thu, 4 May 2000 10:23:38 +0100
From: "Alex at MessageLabs" <ashipp@messagelabs.com>
To: "F-Secure Samples" <samples@f-secure.com>
Subject: URGENT HEADS UP - LoveBug virus sample

This is a big one guys.
600 copies in the last hour.

Call me for details

Alex

[WORLD](#)[U.S.](#)[WEATHER](#)[BUSINESS](#)[SPORTS](#)[TECHNOLOGY](#)[SPACE](#)[HEALTH](#)[ENTERTAINMENT](#)[POLITICS](#)[LAW](#)[TRAVEL](#)[FOOD](#)[ARTS & STYLE](#)[BOOKS](#)[NATURE](#)[IN-DEPTH](#)[ANALYSIS](#)[LOCAL](#)[myCNN](#)[Headline News brief](#)[news quiz](#)[daily almanac](#)

MULTIMEDIA:

[video](#)[video archive](#)[audio](#)**BREAKING NEWS** Joe and Sue Kainz, an Illinois lottery. Details to come.

New computer virus not expected to become widespread, expert says

Using the replication scheme of the "ILOVEYOU" virus, a new and potentially more destructive virus is on the loose. But its sheer destructiveness should curtail its spread and eventually snuff it out, according to one computer virus expert.

Mikko Hypponen, director of virus research at anti-virus company F-Secure in Finland, said that while this virus -- dubbed "NewLove" -- can make a computer unbootable, it isn't nearly as stealthy as "ILOVEYOU." The new computer worm is much less widespread than previous outbreaks and has built-in problems that will eventually make the virus fizzle on its own. A worm is a virus that is self-replicating.

FULL STORY

Annakournikova

[aka VBSWG.ASDF]

Badtrans


Sirecam

admin

Klez

Bugbear

Mimail

From: MS Technical Assistance
Date: Thursday, September 18, 2003 9:45 AM
To: user@updates.net
Subject:
Attach:  Q591362.exe (105 KB)

Microsoft






[All Products](#) | [Support](#) | [Search](#) | [Microsoft.com Guide](#)

[Microsoft Home](#)



Microsoft Client

this is the latest version of security update, the "September 2003, Cumulative Patch" update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to help protect your computer from these vulnerabilities, the most serious of which could allow an attacker to run code on your computer. This update includes the functionality of all previously released patches.

| | |
|---|--|
|  System requirements | Windows 95/98/Me/2000/NT/XP |
|  This update applies to | MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later |
|  Recommendation | Customers should install the patch at the earliest opportunity. |
|  How to install | Run attached file. Choose Yes on displayed dialog box. |
|  How to use | You don't need to do anything after installing this item. |

Microsoft Product Support Services and Knowledge Base articles can be found on the [Microsoft Technical Support](#) web site. For security-related information about Microsoft products, please visit the [Microsoft Security Advisor](#) web site, or [Contact Us](#).

Thank you for using Microsoft products.

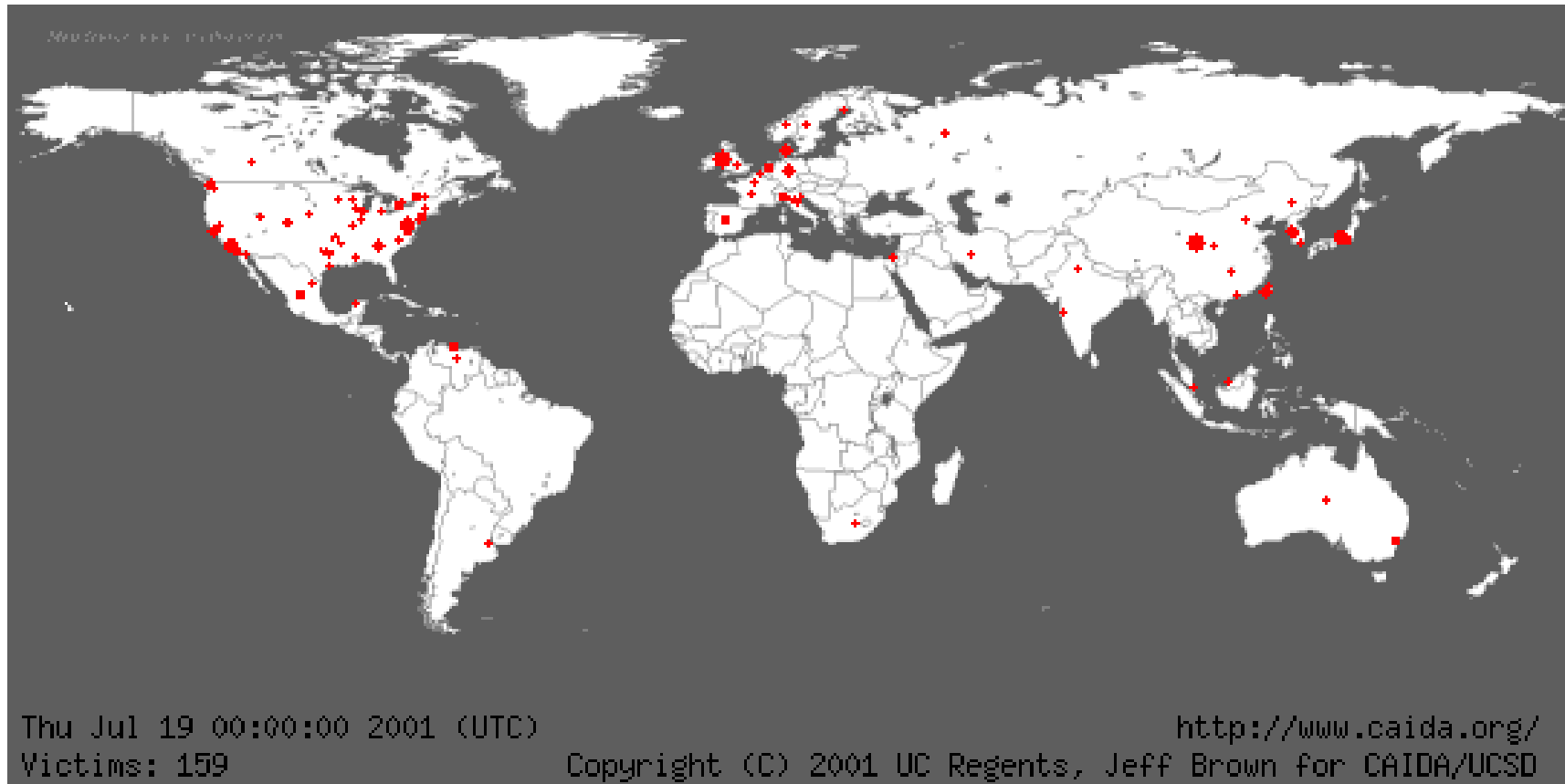
Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

[Contact Us](#) | [Legal](#) | [TRUSTe](#)

©2003 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#) | [Accessibility](#)

Code Red

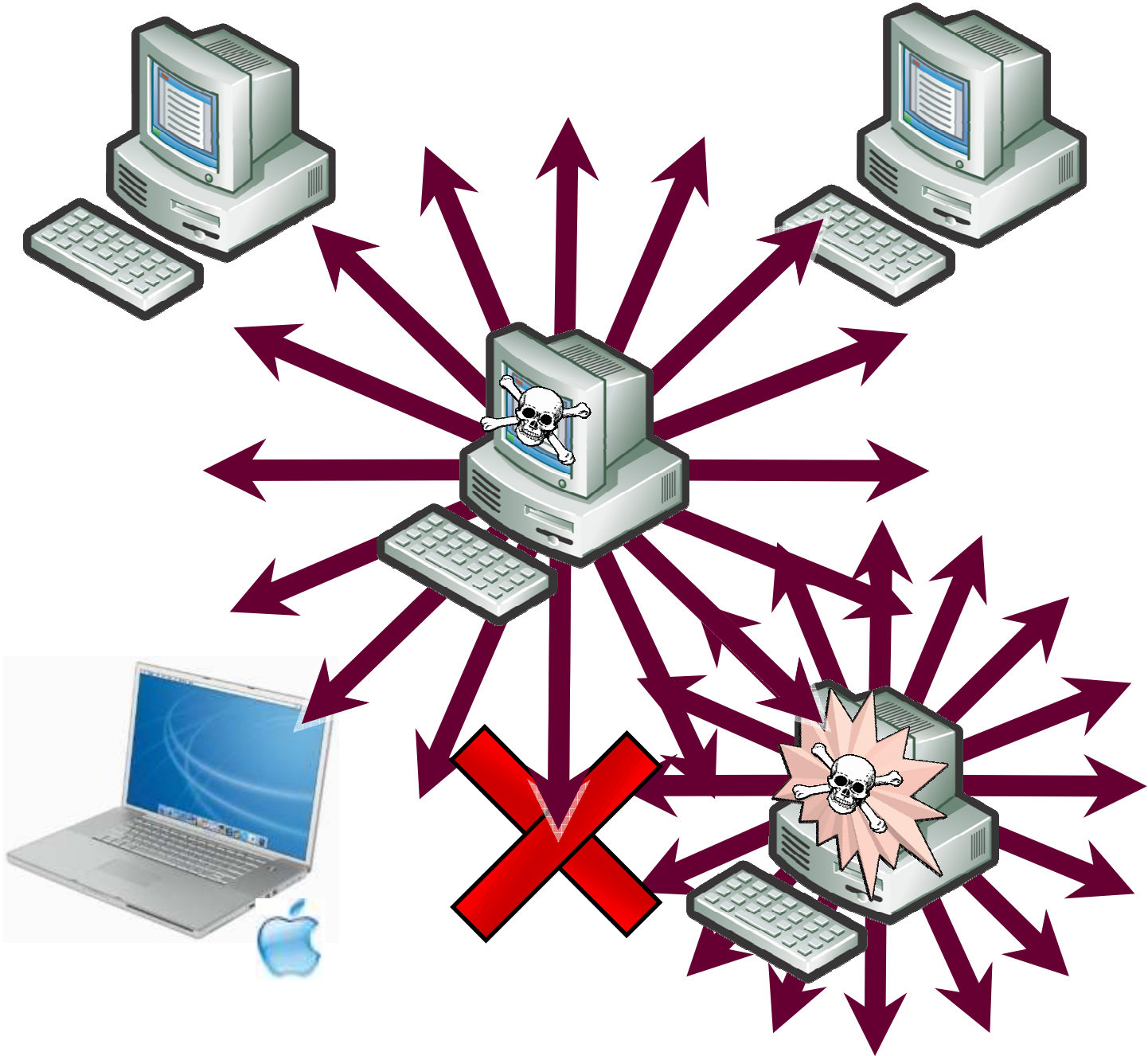


Slapper

Slammer

Blaster

Sasser



System Shutdown

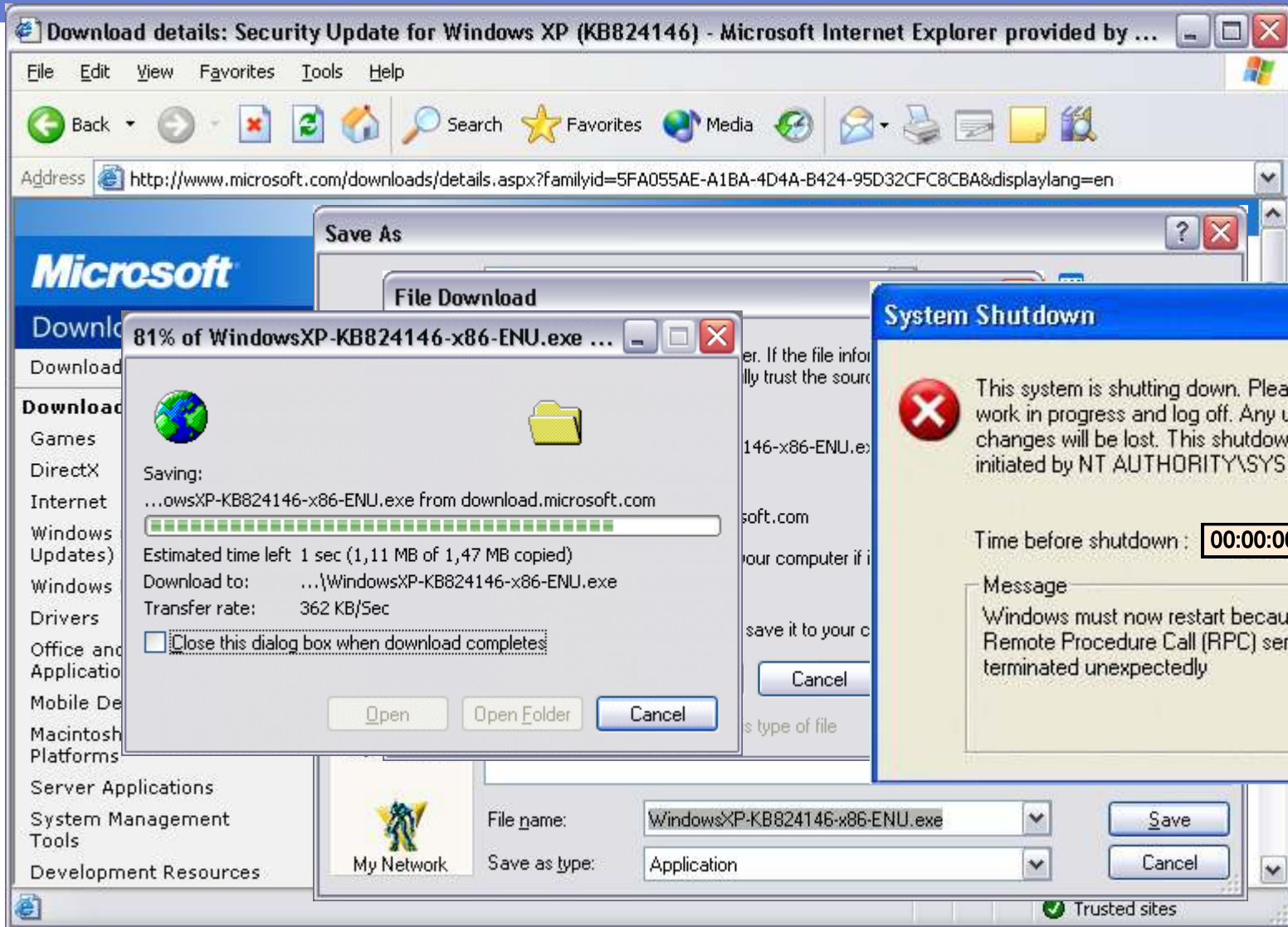


This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

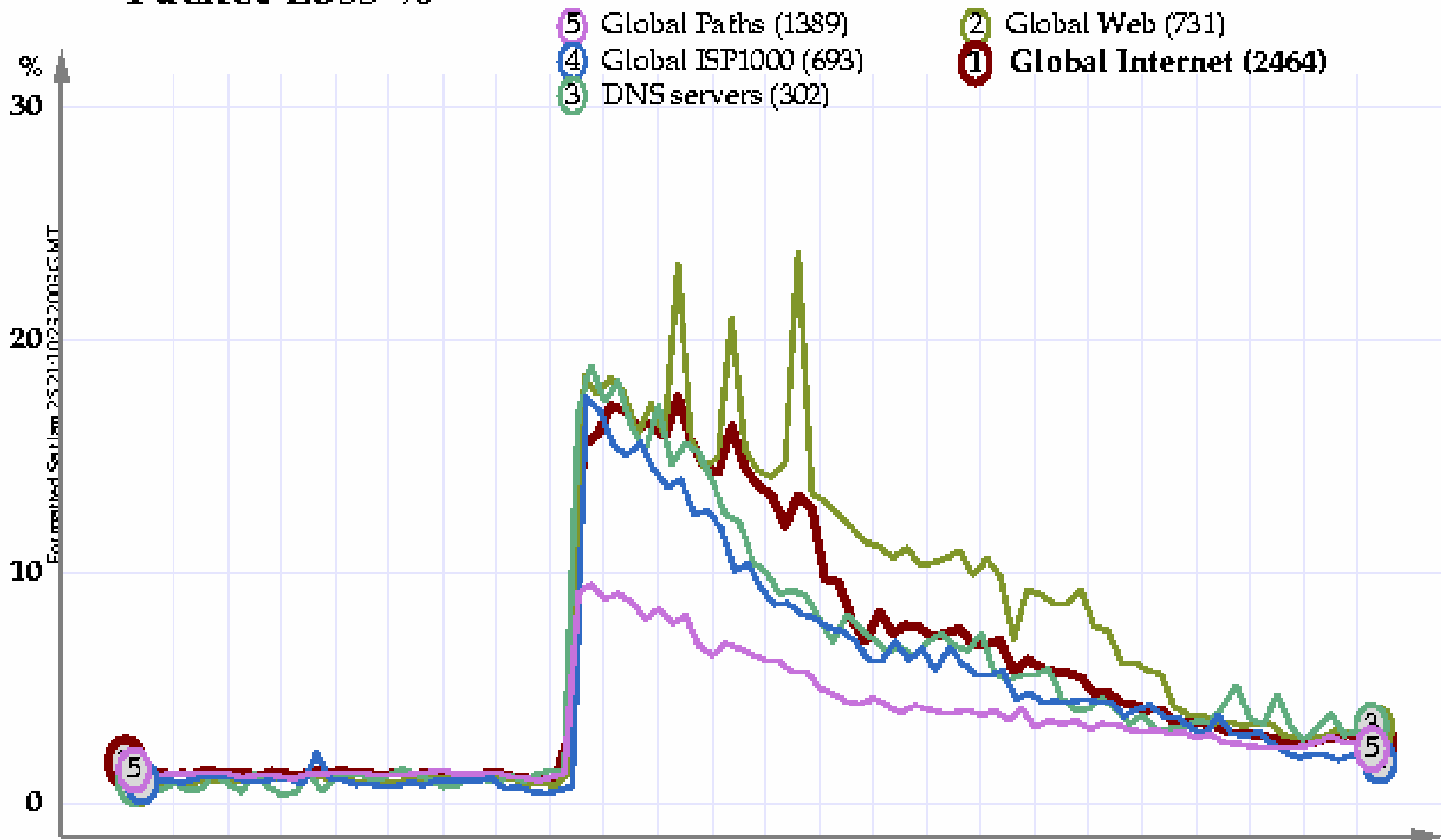
Time before shutdown : 00:00:58

Message

Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly



Packet Loss %



Timezone ()

(c) Copyright 2003 Matrix NetSystems, Inc. www.matrixnetsystems.com

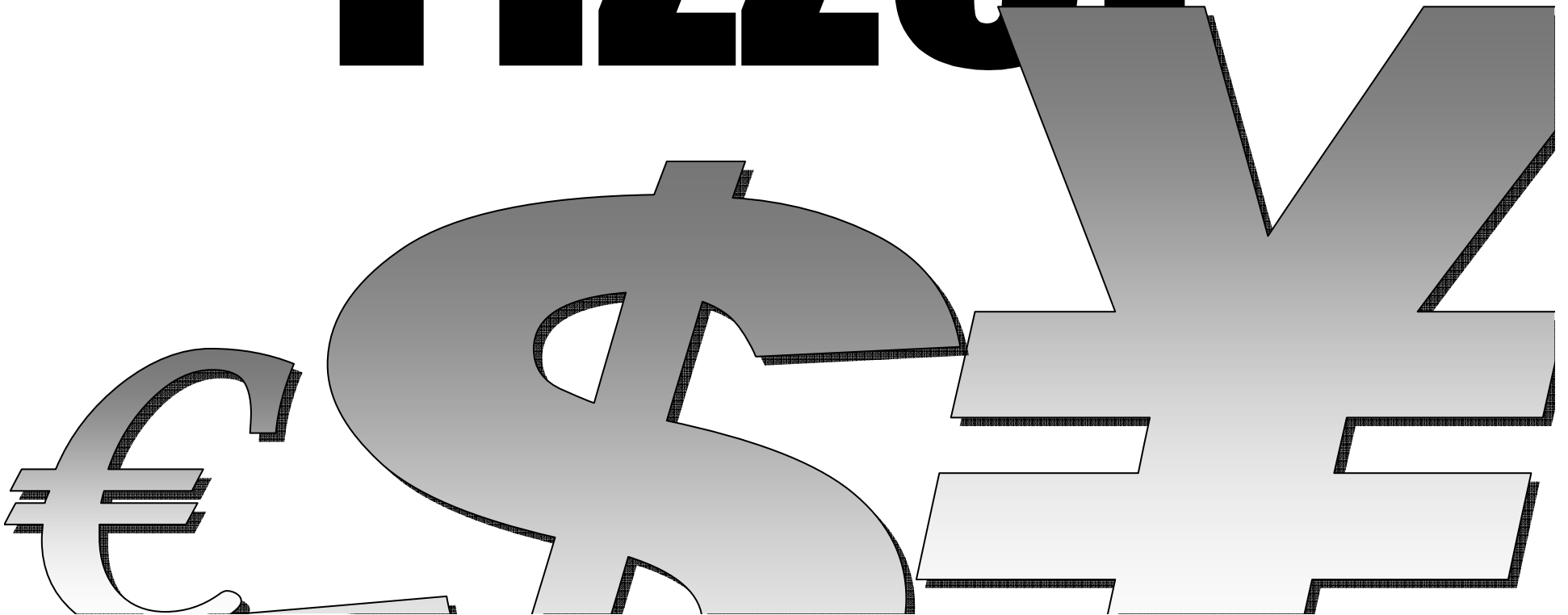
| | | | | | | | | | | | | |
|-----|--------|------|-------|-------|--------|-------|-------|-------|-------|-------|-------|-------|
| GMT | Jan 24 | Jan | 02:00 | 04:00 | 06:00 | 08:00 | 10:00 | 12:00 | 14:00 | 16:00 | 18:00 | 20:00 |
| EST | Jan 24 | 7 PM | 9 PM | 11 PM | Jan 25 | 3 AM | 5 AM | 7 AM | 9 AM | 11 AM | 1 PM | 3 PM |



OOPS

| Name | Transportation | Power | Infrastructure | Banks |
|----------------|--|---|---|--|
| Slammer | Air traffic control problems in USA | Infected a nuclear power plant in Ohio | 911 phone services down in Seattle | Bank of America's ATM network down |
| Blaster | Air Canada flights grounded, CSX trains stopped | NY ISO power operator's network infected | Numerous RPC-based SCADA networks down | Several Windows-based ATM networks infected |
| Sasser | Railcorp trains stopped in Australia, Delta flight problems, delays with British Airways flights | Hong Kong government's department of energy networks infected | Infected: Two hospitals in Sweden, EU commission, Heathrow airport, Coastguard UK | Several banks shutting down offices because of internal infections |

Fizzer





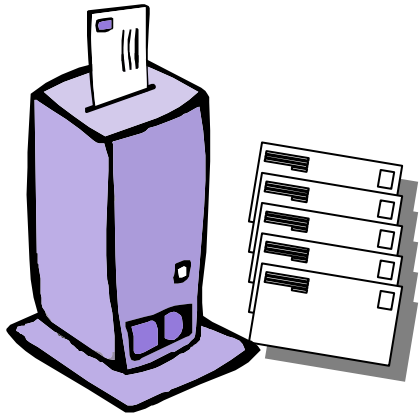
SPAM[®]



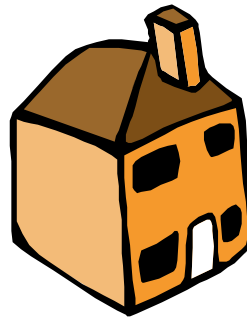
GAME PLAY
LEFT TO RIGHT
OR
RIGHT TO LEFT
Only Highest Win Paid Per
With Consecutive Wins
Starting From Far Left Or
Far Right Reel, Only One

WIN UP TO
500

Spam through Proxy

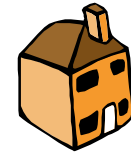


Enlarge-Your-Penis
Enterprises Inc.
(Spammer)



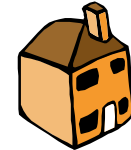
Peter
(infected computer)

?#%\$!?



Ed

?#%\$!?



Bob

?#%\$!?



Lisa

?#%\$!?



Jack

?#%\$!?



Mary



Old enemy



Chen-Ing Hau



Joseph McElroy



Jeffrey Lee Parson



New enemy



Jeremy Jaynes



Jay Echouafni



Andrew Schwarmkoff



Good

Evil

Sobig

Mydoom

Bagle

2004

Netsky

The Virus

Weeks 2004

From: random@address.johndoe.com
 To: samples@f-secure.com
 Subject: Hello
 Date: Mon, 26 Jan 2004 14:07:48 -0800

The message contains Unicode characters and has been sent as a binary attachment.



From: andevy@terra.com.br
 To: mikko.hypponen@datafellows.fi
 Subject: something for you
 Date: Sat, 21 Feb 2004 12:59:26 -0300
 X-Spam-Checker-Version: SpamAssassin 2.60-fsc12082003_1 (1.212-2003-09-23-exp) on dfmail.f-secure.com
 X-Spam-Status: No, hits=1.5 required=4.5 tests=MICROSOFT_EXECUTABLE, MSGID_HAS_NO_AT_NO_REAL_NAME autolearn=no version=2.60-fsc12082003_1
 X-Spam-Level: *
 X-OriginalArrivalTime: 21 Feb 2004 15:51:07.0617 (UTC) FILETIME=[84F68D10:01C3F892]

that is bad

 [talk.txt.scr](#)

| | | | |
|-----------------------|-----------------|-----------------------|-----------------|
| Fri 23.1.2004: | Bagle.A | Mon 8.3.2004: | Netsky.J |
| Tue 27.1.2004: | Mydoom.A | Mon 8.3.2004: | Netsky.K |
| Mon 16.2.2004: | Netsky.A | Tue 9.3.2004: | Bagle.L |
| Mon 16.2.2004: | Mydoom.E | Wed 10.3.2004: | Netsky.L |
| Tue 17.2.2004: | Bagle.B | Thu 11.3.2004: | Netsky.M |
| Wed 18.2.2004: | Netsky.B | Tue 11.3.2004: | Bagle.M |
| Tue 24.2.2004: | Mydoom.F | Thu 13.3.2004: | Bagle.N |
| Wed 25.2.2004: | Netsky.C | Thu 13.3.2004: | Bagle.O |
| Fri 27.2.2004: | Bagle.C | Sat 15.3.2004: | Bagle.P |
| Sat 28.2.2004: | Bagle.D | Mon 17.3.2004: | Netsky.O |
| Sat 28.2.2004: | Bagle.E | Tue 18.3.2004: | Bagle.Q |
| Sun 29.2.2004: | Netsky.D | Thu 18.3.2004: | Bagle.R |
| Mon 1.3.2004: | Bagle.F | Thu 18.3.2004: | Bagle.S |
| Mon 1.3.2004: | Bagle.G | Thu 18.3.2004: | Bagle.T |
| Mon 1.3.2004: | Netsky.E | Sun 21.3.2004: | Netsky.P |
| Tue 2.3.2004: | Bagle.H | Fri 26.3.2004: | Bagle.U |
| Tue 2.3.2004: | Bagle.I | Mon 29.3.2004: | Bagle.V |
| Tue 2.3.2004: | Netsky.F | Mon 29.3.2004: | Netsky.Q |
| Tue 2.3.2004: | Bagle.J | Wed 31.3.2004: | Netsky.R |
| Wed 3.3.2004: | Mydoom.G | Mon 5.4.2004: | Netsky.S |
| Wed 3.3.2004: | Bagle.K | Mon 5.4.2004: | Bagle.W |
| Wed 3.3.2004: | Mydoom.H | Tue 6.4.2004: | Netsky.T |
| Thu 4.3.2004: | Netsky.G | Thu 8.4.2004: | Netsky.U |
| Fri 5.3.2004: | Netsky.H | Tue 13.4.2004: | Mydoom.I |
| Sun 7.3.2004: | Netsky.I | Wed 14.4.2004: | Netsky.V |
| | | Thu 15.4.2004: | Netsky.W |
| | | Fri 16.4.2004: | Mydoom.J |
| | | Mon 19.4.2004: | Netsky.X |



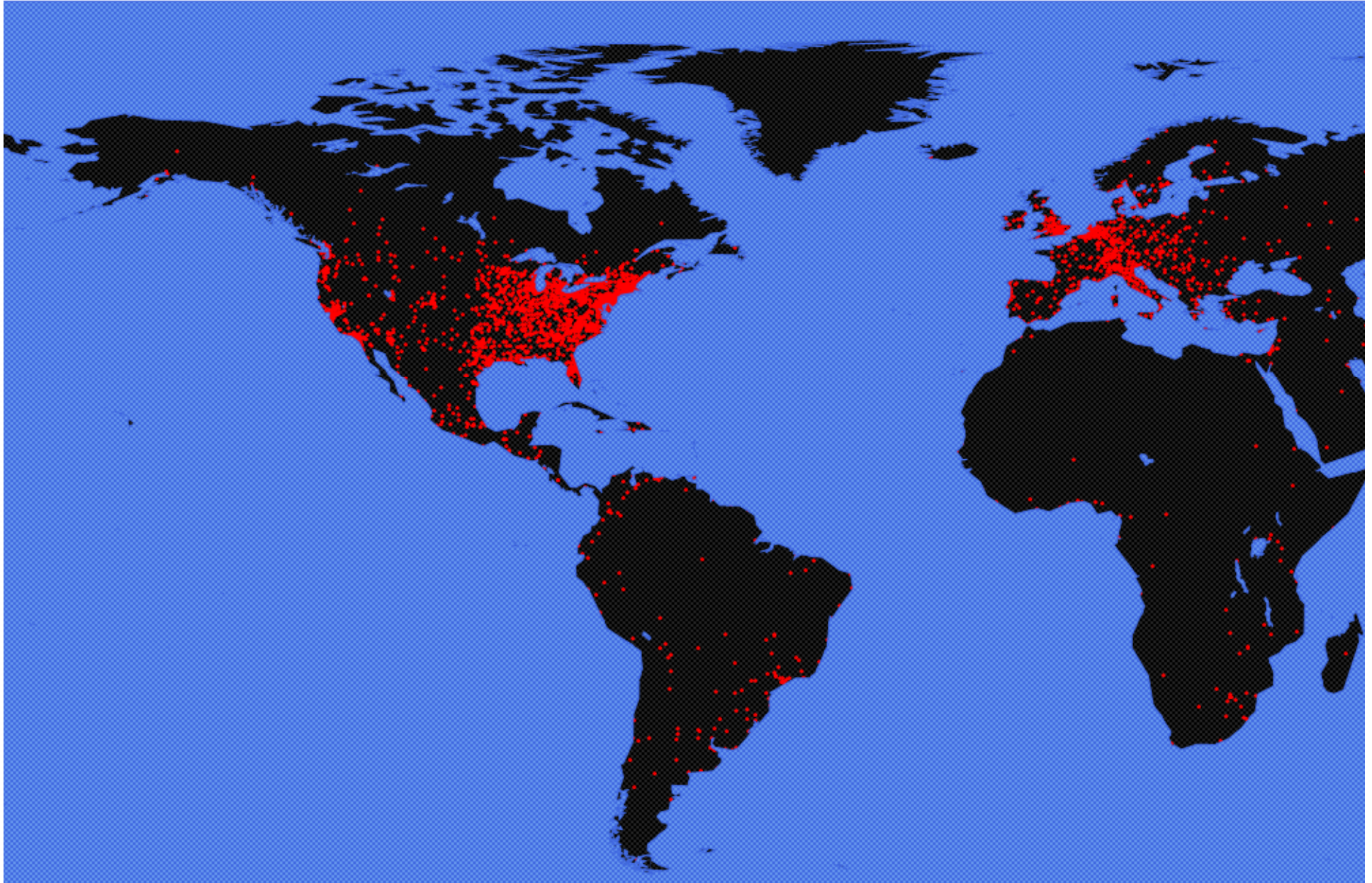
*"Most people don't even know what a rootkit is,
so why should they care about it?"*

- Thomas Hesse, President, Global digital business, Sony BMG

Nyxem



Nyxem.E (Blackworm)



Haxdoor

A311 Death это профессиональная система удалённого администрирования с кучей возможностей.

Помните, что постоянное совершенствование средств защиты требует постоянный приток новых технологий тестирования ТОЛЬКО **свежее spyware** способно обеспечить уровень функциональности, адекватный текущим потребностям.

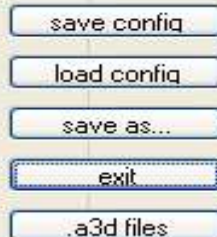
--==;==--

- ♦ **!!! теперь возможен заказ с ПРОФЕССИОНАЛЬНОЙ админкой для организации сокс-сервиса**

- СВЕЖАЯ GEO база (IP to country-state-city)
 - система аккунтов и установка лимитов (срок действия аккунта, количество взятых проксей)
 - вывод соксов для пользователей в поштучном виде типа 197.59.***.***
 - поиск и фильтрация по соксам
 - в цену входит установка на сервер
- цена 250 \$

посмотреть скриншоты

*** установка производится ТОЛЬКО на технически подготовленные сервера



about

All information on this site is given exclusively in the educational purposes.

All programs are intended only for testing and revealing vulnerability on personal computers and corporate networks.

WareZOV

sadujadesion.com
yuhadefunjinsa.com
jaxedunnjsatunheri.com
gadesunheranwui.com
vertionkdaseliplim.com
ertinmdesachlion.com

Spysheeriff



HOME



Is your computer infected?

FREE SCAN

Key features

- **Intelligent Threat Scanner**
Performs an user-controlled or automatic threat scan with optional threat removal.
- **Application Firewall**
Controls running of each and every program on your PC. Rules-based system gives you a powerful tool to restrict or allow this or that application to run once or permanently.

9 OUT OF 10 PC's ARE INFECTED
With Spyware that can't be detected by your Anti-Virus
Download our award winning Anti-Spyware Software



Designed for MS Windows™ 95, 98, NT, ME, 2K, XP

Check if you're infected

DOWNLOAD

FREE SCAN

Your computer is infected when

- Your computer has slowed down
- Your Internet connection speed has decreased
- You have downloaded music or software from the Web
- You get popups and annoying ads when you're online or sometimes even offline
- Your default home page has been changed to the one you didn't ask for
- You have an extra toolbar installed, and you don't know where it came from
- You receive more spam emails than ever

If the answer to one of these questions is "Yes", then you are probably infected.

CHECK NOW

What is Spyware?

- Spyware, like a virus, is a malicious software planted on your PC by a third party in order to secretly monitor what you do online.
- Once your browsing habits are analyzed, you are flooded with endless Commercials, Popups and Spam from inside your PC!
- Spyware also dramatically slows down your computer and Internet connection speeds.
- Spyware collects your private information and steals your identity, passwords, credit card details and other financial data.
- The presence of the infection is hidden, and is not revealed even by Anti Virus or Firewall programs.

Bancos

Brazilian Busts

| Operation | 2001 "Cash net" | 2003 "Cavalo de troija I" | 2004 "Cavalo de troija II" | 2005 "Pegasus" | 2006 "Scan" |
|-------------------------|----------------------------|--|---|---------------------------|------------------------|
| Arrests | 17 | 27 | 64 | 85 | 63 |
| Money stolen | \$46,000,000 | \$14,000,000 | \$110,000,000 | \$33,000,000 | \$4,700,000 |

ARTICLE 19 OF UNIVERSAL DECLARATION OF HUMAN RIGHTS

Pages: (3) [1] 2 3 (Go to first unread post)

AddReplu

NewTopic

NewPoll

bank accounts for sale

Track this topic | Email this topic | Print this topic

tabbot

Posted: Jan 27 2006, 12:29 AM

Quote

Verified for Bank Accounts Logins

any US bank accounts for sale
Balance from 3k and above -40\$
Regular Brokerage accounts from 3k and above - 70\$
Lots of different brokerage accounts from 3k and above with signature - 100\$
In stock accounts from other countries: CA, AU, NZ, FR, TR etc. - price negotiable
Also I can check for other countries that interest you, please drop links to my icq

Group: Verified Vendor
Posts: 14
Member No.: 3407
Joined: 24-January 06

bank accounts for sale
icq 258-954-710
www.accs-info.com

PM

Email

ICQ



#darkmarket

```
<claatrass>    what accounts you have and the value  
<hacker_xero> i have chase accts with wire enabled  
<claatrass>    whats the value  
<hacker_xero> balances 21k, 44k, 30k  
<claatrass>    how much for all three  
<hacker_xero> $500  
<claatrass>    ok
```





> Registration

> FAQ

> Contact

> How it works

Home

Contact Us

Outsource Line

Great opportunity for everyone!



Outsource Line

"If it weren't for Outsource Line I wouldn't be in business today. It's that simple."
President, Packaging Company

Company's News

>> **05.12.04**

Each day brings new customers! Today we got our happy 100-th customer!

>> **21.10.04**

Finally we have made new design. Enjoy.

>> **12.10.04**

We opened a new office in Spain.

[Read more](#)

> **You guys are really the greatest!!!!...**

It works great this way!
Thanks a lot for all the great support!!!

Registration:

Thank you for the shown interest about our proposal. At the moment we have a number of vacancies of GENERAL ASSISTANT in many countries and territories. We'd like to give you some information about what exactly our company doing and how would you help us. But just before that I'd like to tell you that for this job we are NOT going to ask you do ANY initial investments or send ANY kind of initial payments. And another thing to mention here that this is part-time home-based job that will require just about 5 or less hours weekly. So you can happily stay at your current position if you have any and just if you'll see a good potential to grow with us you can start work harder.

Basic methods of domestic payments we are receiving from our customers are: domestic wire transfers, cashier's checks, money orders and some others. For most of those methods it will take a long time and often significant additional charges to receive them outside the country where the payment was initiated.

Your responsibilities will include receiving these payments into your bank account and transfer them to us with the way we'll inform you. You will get 6-8% from total transferred amount as your wages.

This is fully home-based flexible hours part-time job with just minimal



>> **You have a company that cares about more than just the bottom line** and that is rare to find in this day and age.
Marc & Diane Injejikian

...thank you very much for all your support and for looking into this for me. Thats how support should be.

Thanks
Spencer Boydell-Butt

Good

Evil

**How on earth can
we handle all
these?**



© 2005 Mikael Albrecht

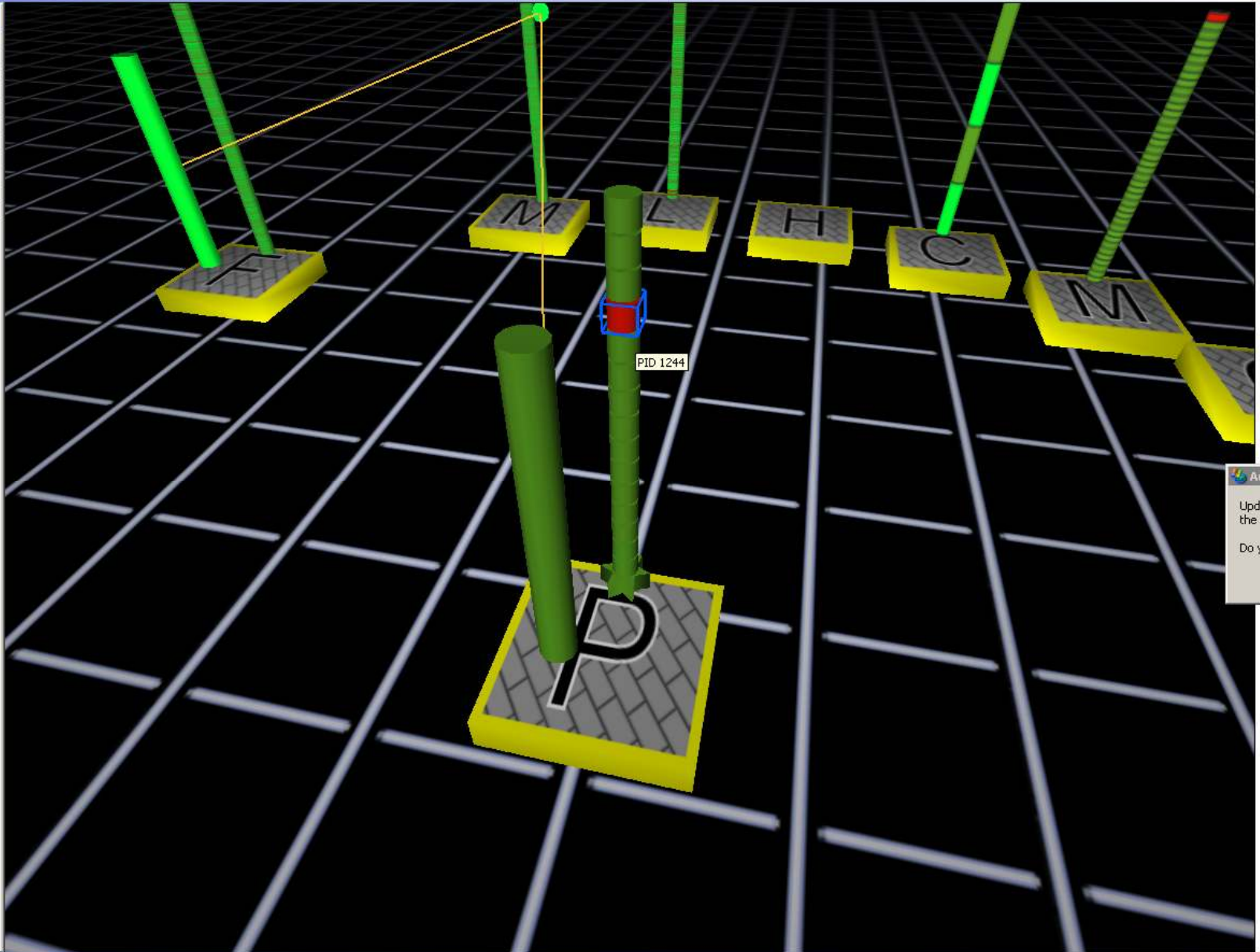
F-Secure MAViz

File Edit Navigate View Snapshots Help

snapshot_breplibot_c.xml

| Properties | |
|----------------|--------------------------|
| Type | Module |
| Name | wintrust.dll at 0x76C300 |
| Anomaly score | 2 |
| PID | 848 |
| Module size | 188416 |
| Module address | 0x76C30000 |

| Neighbors | |
|-----------|------------------------------|
| File | wintrust.dll |
| Process | PID 848 |



Filters Sorters



Future?





Wi-Fi viruses

**Hitting Windows
laptops**

Sniffing WLAN traffic

Inserting itself into TCP/IP frames

**Uses
web exploits**



Good

Evil

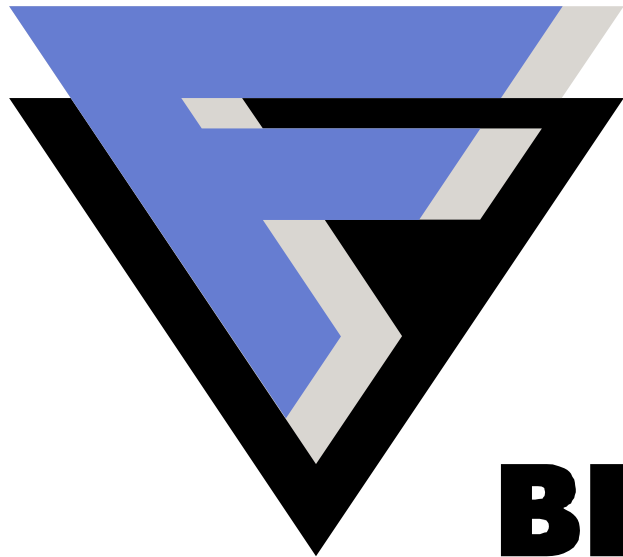


Good

will

prevail

F-SECURE®



BE SURE.

Mikko Hypponen
Chief Research Officer
F-Secure Corporation

www.f-secure.com

www.hypponen.com

Thanks to Lawrence Lessig