Virus Bulletin 2006 Montreal KEYNOTE

F-SECURE®

BE SURE.

Mikko Hypponen
Chief Research Officer
F-Secure Corporation

www.f-secure.com
www.hypponen.com
Simplified example

(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. \(\text{“R”}\) and \(\text{“G”}\) 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).

\[
\begin{align*}
g_{\alpha}(x) &= \begin{cases} 
    m_{\alpha}(x - \theta_{\alpha}) & \text{if } x > \theta_{\alpha} \\
    0 & \text{else} 
\end{cases}, \\
\end{align*}
\]

\[
\begin{align*}
g_{\alpha}(x) &= \begin{cases} 
    m_{\alpha}(x - \theta_{\alpha}) & \text{if } x > \theta_{\alpha} \\
    0 & \text{else} 
\end{cases}. \\
\end{align*}
\]

\[
I_{r}^{lat} = \sum_{s \in S} L_{s}^{xx} x_{s}
\]

\[
I_{y}^{lat} = \sum_{s \in S} L_{s}^{yy} y_{s}
\]

\[
\begin{align*}
I_{x} &= I_{x}^{0} + I_{x}^{lat} - I_{x}^{norm} \\
I_{y}^{lat} &= \sum_{s \in S} L_{s}^{xx} x_{s} \\
I_{y}^{lat} &= \sum_{s \in S} L_{s}^{yy} y_{s}
\end{align*}
\]

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

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

\[
\begin{align*}
\dot{x} &= -r_{x} x - g_{y}(y) + L_{0}^{xx} g_{x}(x) + I_{x} + \eta_{x} \\
y &= -r_{y} y + g_{x}(x) - I_{y} + \eta_{y}.
\end{align*}
\]
Hello
name:
Mikko Hypponen
CRO
Helsinki
300 PC viruses
Good
Evil
Canada!

eh
Mikko Hypponen
Data Fellows Ltd, Finland

MIKKO HYPÖNNEN
DATA FELLOWS, FINLAND

MIKKO HYPÖNNEN
DATA FELLOWS LTD, FINLAND
Keynote
Criminal investigation
For-profit botnet gang
Attacked us
Investigation
Several months
Busted
3 arrests
Excellent case study
Keynote
Tuesday, September 5, 2006

**Keynoting**

*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?

---

**F-Secure - September 5th Poll**

*What should Mikko’s VB Keynote presentation be?*

- A generic product sales pitch
- ...or tell us your suggestion:
What should Mikko's VB Keynote presentation be?

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

Submit
Brain
Stoned
Cascade
Yankee Doodle
Dark Avenger
Form
Omega

13th of September

1991
Michelangelo
V-Sign

C:\horror\vdemo\Q-V-SIGN.COM
C:\horror\vdemo\WALKER.COM
C:\horror\vdemo\ELVIRA-G.COM

1992
Type "Happy Birthday Joshi"!
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

1996
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
Marburg
RemoteExplorer
Funlove
ZippedFiles
Melissa
Bubbleboy
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
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 fizz out on its own. A worm is a virus that is self-replicating.
Annakournikova
[ aka VBSWG.ASDF ]
Badtrans
Sircam
admin
Klez
Bugbear
Mimail
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.
Code Red

http://www.caida.org/

Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD
Slapper
Slammer
Blaster
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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Transportation</th>
<th>Power</th>
<th>Infrastructure</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slammer</td>
<td>Air traffic control problems in USA</td>
<td>Infected a nuclear power plant in Ohio</td>
<td>911 phone services down in Seattle</td>
<td>Bank of America's ATM network down</td>
</tr>
<tr>
<td>Blaster</td>
<td>Air Canada flights grounded, CSX trains stopped</td>
<td>NY ISO power operator's network infected</td>
<td>Numerous RPC-based SCADA networks down</td>
<td>Several Windows-based ATM networks infected</td>
</tr>
<tr>
<td>Sasser</td>
<td>Railcorp trains stopped in Australia, Delta flight problems, delays with British Airways flights</td>
<td>Hong Kong government's department of energy networks infected</td>
<td>Infected: Two hospitals in Sweden, EU commission, Heathrow airport, Coastguard UK</td>
<td>Several banks shutting down offices because of internal infections</td>
</tr>
</tbody>
</table>
Fizzer

€ $ ¥
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
<table>
<thead>
<tr>
<th>Date</th>
<th>Virus Name</th>
<th>Date</th>
<th>Virus Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thu 11.3.2004</td>
<td>Netsky.M</td>
<td>Thu 11.3.2004</td>
<td>Netsky.M</td>
</tr>
<tr>
<td>Sat 15.3.2004</td>
<td>Netsky.P</td>
<td>Thu 18.3.2004</td>
<td>Bagle.Q</td>
</tr>
<tr>
<td>Thu 18.3.2004</td>
<td>Bagle.R</td>
<td>Thu 18.3.2004</td>
<td>Bagle.S</td>
</tr>
<tr>
<td>Fri 26.3.2004</td>
<td>Bagle.U</td>
<td>Mon 29.3.2004</td>
<td>Bagle.V</td>
</tr>
<tr>
<td>Mon 29.3.2004</td>
<td>Bagle.V</td>
<td>Mon 29.3.2004</td>
<td>Bagle.W</td>
</tr>
<tr>
<td>Mon 31.3.2004</td>
<td>Bagle.W</td>
<td>Mon 5.4.2004</td>
<td>Bagle.U</td>
</tr>
<tr>
<td>Mon 5.4.2004</td>
<td>Bagle.U</td>
<td>Thu 6.4.2004</td>
<td>Bagle.T</td>
</tr>
<tr>
<td>Tue 17.2.2004</td>
<td>Bagle.B</td>
<td>Thu 13.3.2004</td>
<td>Bagle.O</td>
</tr>
<tr>
<td>Tue 24.2.2004</td>
<td>Mydoom.F</td>
<td>Mon 17.3.2004</td>
<td>Netsky.O</td>
</tr>
<tr>
<td>Fri 27.2.2004</td>
<td>Bagle.C</td>
<td>Fri 27.2.2004</td>
<td>Bagle.C</td>
</tr>
<tr>
<td>Sat 28.2.2004</td>
<td>Bagle.D</td>
<td>Sat 28.2.2004</td>
<td>Bagle.D</td>
</tr>
<tr>
<td>Sun 29.2.2004</td>
<td>Netsky.D</td>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
<tr>
<td>Mon 1.3.2004</td>
<td>Bagle.F</td>
<td>Mon 1.3.2004</td>
<td>Bagle.G</td>
</tr>
</tbody>
</table>

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

2005
"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
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 аккаунтов и установка лимитов (срок действия аккаунта, 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

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
versionkdaseliplim.com
ertinmdesachlion.com
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

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.

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

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.

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

CHECK NOW
Bancos
# Brazilian Busts

<table>
<thead>
<tr>
<th>Operation</th>
<th>2001</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;Cash net&quot;</td>
<td>&quot;Cavalo de trolja I&quot;</td>
<td>&quot;Cavalo de trolja II&quot;</td>
<td>&quot;Pegasus&quot;</td>
<td>&quot;Scan&quot;</td>
</tr>
<tr>
<td>Arrests</td>
<td>17</td>
<td>27</td>
<td>64</td>
<td>85</td>
<td>63</td>
</tr>
<tr>
<td>Money stolen</td>
<td>$46,000,000</td>
<td>$14,000,000</td>
<td>$110,000,000</td>
<td>$33,000,000</td>
<td>$4,700,000</td>
</tr>
</tbody>
</table>
**bank accounts for sale**

<table>
<thead>
<tr>
<th>tabbot</th>
<th>Posted: Jan 27 2006, 12:29 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verified for Bank Accounts</strong></td>
<td></td>
</tr>
<tr>
<td>Logins</td>
<td></td>
</tr>
<tr>
<td><strong>Group:</strong> Verified Vendor</td>
<td></td>
</tr>
<tr>
<td>Posts: 14</td>
<td></td>
</tr>
<tr>
<td>Member No.: 3407</td>
<td></td>
</tr>
<tr>
<td>Joined: 24-January 06</td>
<td></td>
</tr>
</tbody>
</table>

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

---

bank accounts for sale
icq 258-954-710
www.accs-info.com
<claatrass> what accounts you have and the value
<hacker_xero> i have chase accts with wire enabled
<claatrass> what's the value
<hacker_xero> balances 21k, 44k, 30k
<claatrass> how much for all three
<hacker_xero> $500
<claatrass> ok
I will take down any website that you want for $50 per day. I am experienced at this and am known for taking down many sites in the past. If you wish to take part in my services, send me an email to microcrew777@yahoo.com or send $50 X the number of days you wish to take down a site to my e-gold account Account 2994988 (--MC--) and include the website in the memo field.

This is a great deal on DDOS attacks and cannot be beat by anyone!
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...
Good
Evil
How on earth can we handle all these?
Future?
Wi-Fi viruses
Hitting Windows laptops
Sniffing WLAN traffic
Inserting itself into TCP/IP frames
Uses

web exploits
Good
Evil
Good will prevail
Thanks to Lawrence Lessig