symantec.™

Me code write good – The l33t skillz of the virus writer.

John Canavan

Symantec Security Response

Abstract

- We will take a look at the legacy of less than expert level virus writers, and examine the threat they continue to pose.

Background

- July 1962 , Mariner 1 space probe
- 1985-1987, Therac-25 radiation therapy machine.
- August 2003, power blackout affected the North Eastern Coast of the United States.

Bugs in viruses

•**Until recently, typically written by amateur fanatics, hacked together by script kiddies or as a form of experimentation by overly-curious fledgling coders with minimal testing.**

•**Case studies of bugs in well known viruses…**

- Overview
- Bugs
- Impact

The Morris Worm

•2 November 1988, Exploited flaws in *fingerd/gets* and *sendmail* in BSD-derived versions of UNIX

•Many machines gave in to the crippling load and failed completely as their swap space or process tables were exhausted

•Most problems due to flawed logic in propagation control routine.

The Morris Worm - Analysis

- Designed simply to spread to as many systems as possible
- The worm first attempted to spawn a remote shell, invoking /usr/ucb/rsh, /usr/bin/rsh, and /bin/rsh.
- If this failed the worm connected to the remote finger server daemon sending a 536 byte buffer overflow exploit string to execute an *execve("/bin/sh",0, 0)*. This attack only worked on vulnerable VAX machines, and caused a core dump on Suns.
- Finally the worm would attempt to exploit an SMTP vulnerability, setting debug on and sending:
  mail from: </dev/null>
  rcpt to: <"|sed -e '1,/^$/'d | /bin/sh ; exit 0">

The Morris Worm - Bugs

- Calls are made to functions with incorrect numbers of arguments
- Local variables are declared but never used
- Includes routines that are never referenced
- Others that will not be executed because of conditions that are never met.

The Morris Worm - Bugs

```
if ((random() % 7) == 3)
        return;
```

- Several worm processes infected a clean machine at once.
- Several worm processes starting at once, in the presence of an existing infection.
- A machine is slow or heavily loaded, which could cause the worm to exceed the timeouts imposed on the exchange of numbers.

The Morris Worm - Impact

- Propagated far faster than expected.
- Systems slowed significantly by infections.
- Administrators noticed slow machines and spotted worm quickly,
- With experts at work on a fix, solutions were available within hours.

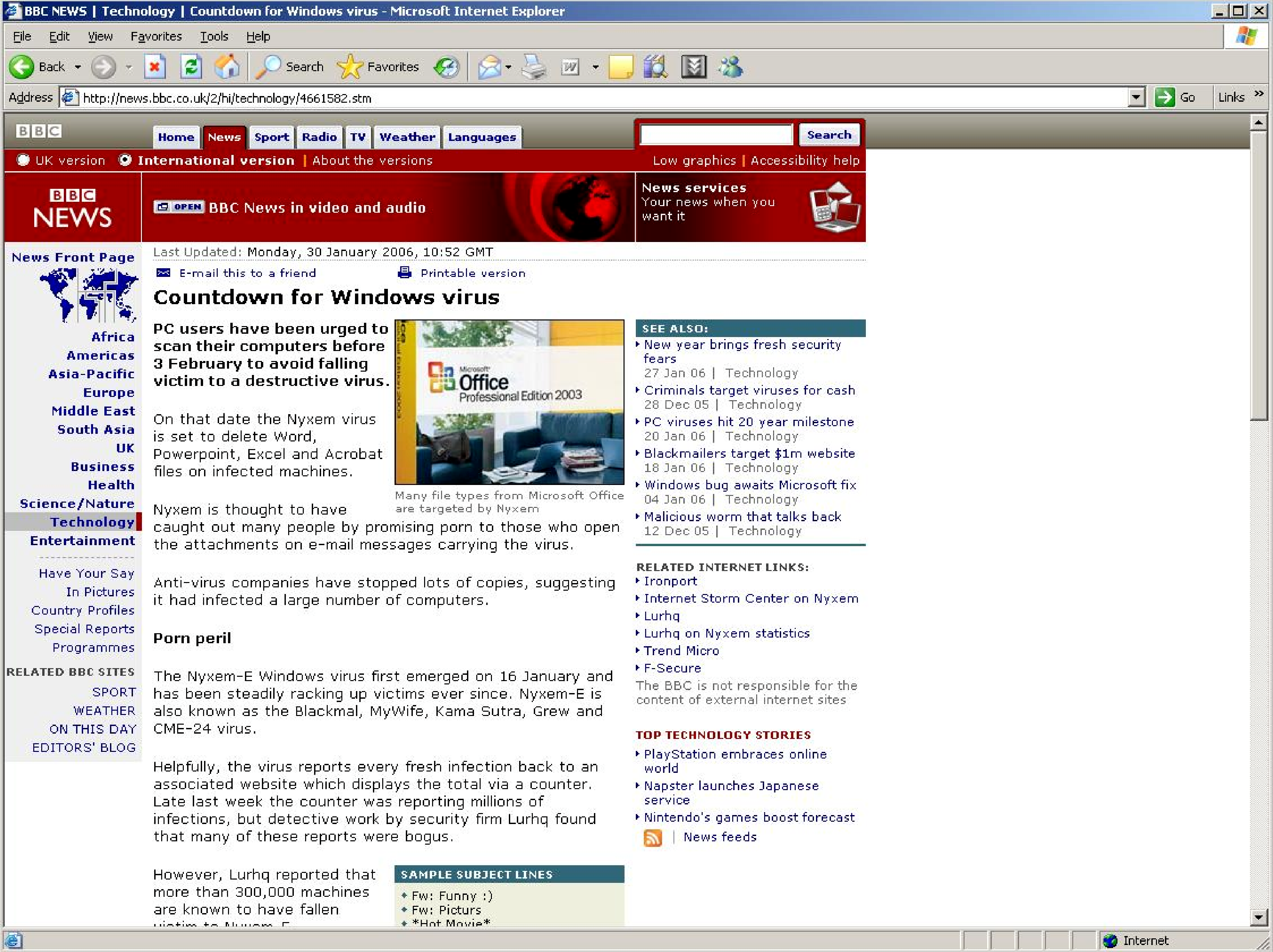
Kama Sutra - A wet blanket

- Late January 2006 - W32.Blackmal.E@mm (Nyxem,MyWife) mass-mails itself from infected hosts with a choice of 19 mail subjects.
- Contacted a web-based script which was intended to function as an infection counter.
- Estimations of up to 1.8million infected systems.
- Overwrite files with the following extensions on the 3rd of the month;

*.doc, *.xls, *.mdb, *.mde, *.ppt, *.pps, *.zip, *.rar, *.pdf, *.psd, *.dmp

With the following text:

DATA Error [47 0F 94 93 F4 F5]


BBC NEWS | Technology | Countdown for Windows virus - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://news.bbc.co.uk/2/hi/technology/4661582.stm
Go
Links
BBC
Home News Sport Radio TV Weather Languages
Search
○ UK version ● International version | About the versions
Low graphics | Accessibility help
BBC NEWS
OPEN BBC News in video and audio
News services
Your news when you want it
Microsoft Office Professional Edition 2003
Internet

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

Have Your Say
In Pictures
Country Profiles
Special Reports
Programmes

RELATED BBC SITES
SPORT
WEATHER
ON THIS DAY
EDITORS' BLOG

Last Updated: Monday, 30 January 2006, 10:52 GMT

E-mail this to a friend   Printable version

Countdown for Windows virus

PC users have been urged to scan their computers before 3 February to avoid falling victim to a destructive virus.

On that date the Nyxem virus is set to delete Word, Powerpoint, Excel and Acrobat files on infected machines.

Many file types from Microsoft Office are targeted by Nyxem

Nyxem is thought to have caught out many people by promising porn to those who open the attachments on e-mail messages carrying the virus.

Anti-virus companies have stopped lots of copies, suggesting it had infected a large number of computers.

Porn peril

The Nyxem-E Windows virus first emerged on 16 January and has been steadily racking up victims ever since. Nyxem-E is also known as the Blackmal, MyWife, Kama Sutra, Grew and CME-24 virus.

Helpfully, the virus reports every fresh infection back to an associated website which displays the total via a counter. Late last week the counter was reporting millions of infections, but detective work by security firm Lurhq found that many of these reports were bogus.

However, Lurhq reported that more than 300,000 machines are known to have fallen victim to Nyxem-E

SAMPLE SUBJECT LINES
- Fw: Funny :)
- Fw: Picturs
- *Hot Movie*

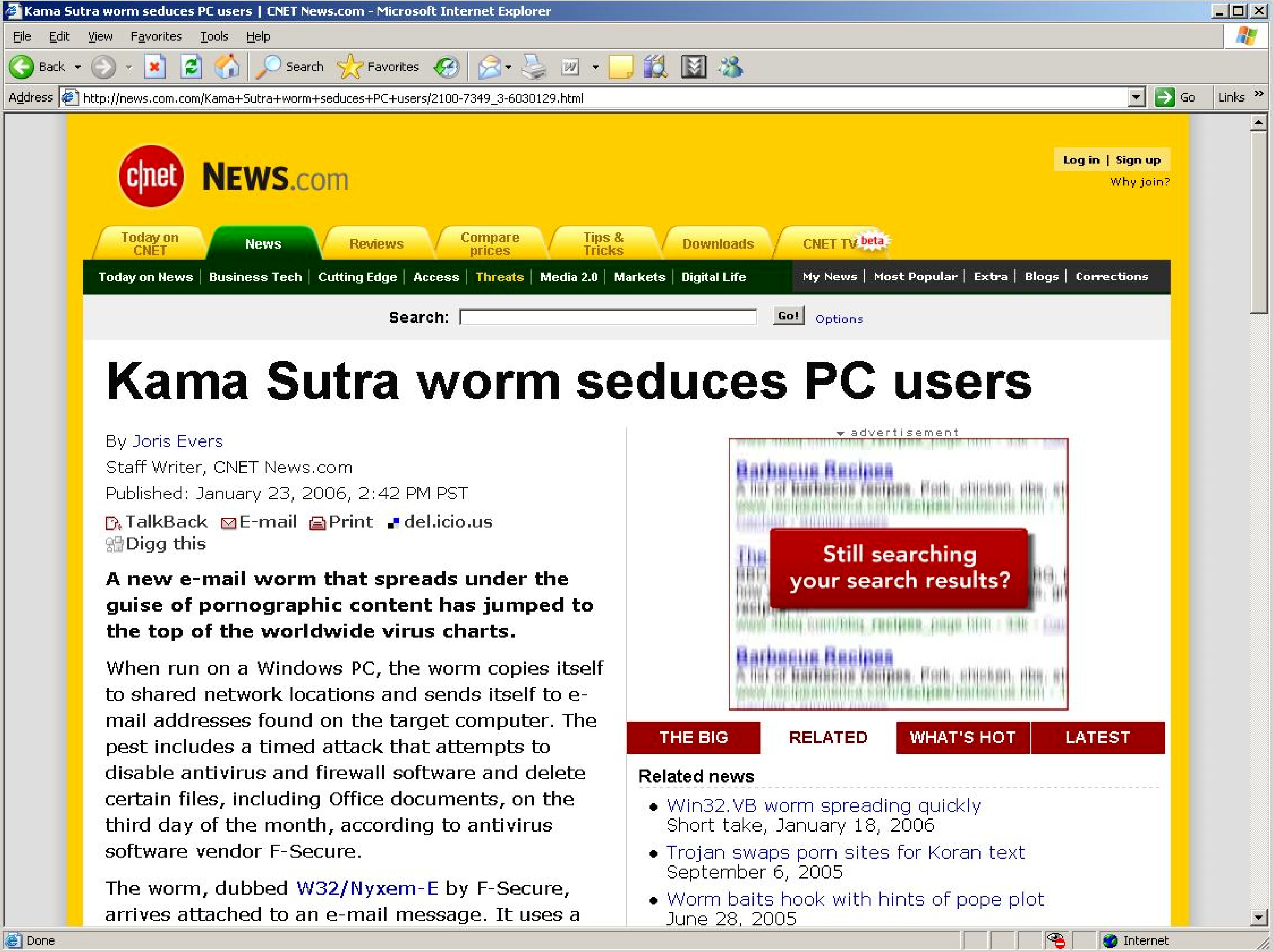
SEE ALSO:
- New year brings fresh security fears
  27 Jan 06 | Technology
- Criminals target viruses for cash
  28 Dec 05 | Technology
- PC viruses hit 20 year milestone
  20 Jan 06 | Technology
- Blackmailers target $1m website
  18 Jan 06 | Technology
- Windows bug awaits Microsoft fix
  04 Jan 06 | Technology
- Malicious worm that talks back
  12 Dec 05 | Technology

RELATED INTERNET LINKS:
- Ironport
- Internet Storm Center on Nyxem
- Lurhq
- Lurhq on Nyxem statistics
- Trend Micro
- F-Secure

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES
- PlayStation embraces online world
- Napster launches Japanese service
- Nintendo's games boost forecast

News feeds


Kama Sutra worm seduces PC users | CNET News.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://news.com.com/Kama+Sutra+worm+seduces+PC+users/2100-7349_3-6030129.html
Go
Links
Done
Internet

Kama Sutra worm seduces PC users

By Joris Evers
Staff Writer, CNET News.com
Published: January 23, 2006, 2:42 PM PST

TalkBack E-mail Print del.icio.us
Digg this

A new e-mail worm that spreads under the guise of pornographic content has jumped to the top of the worldwide virus charts.

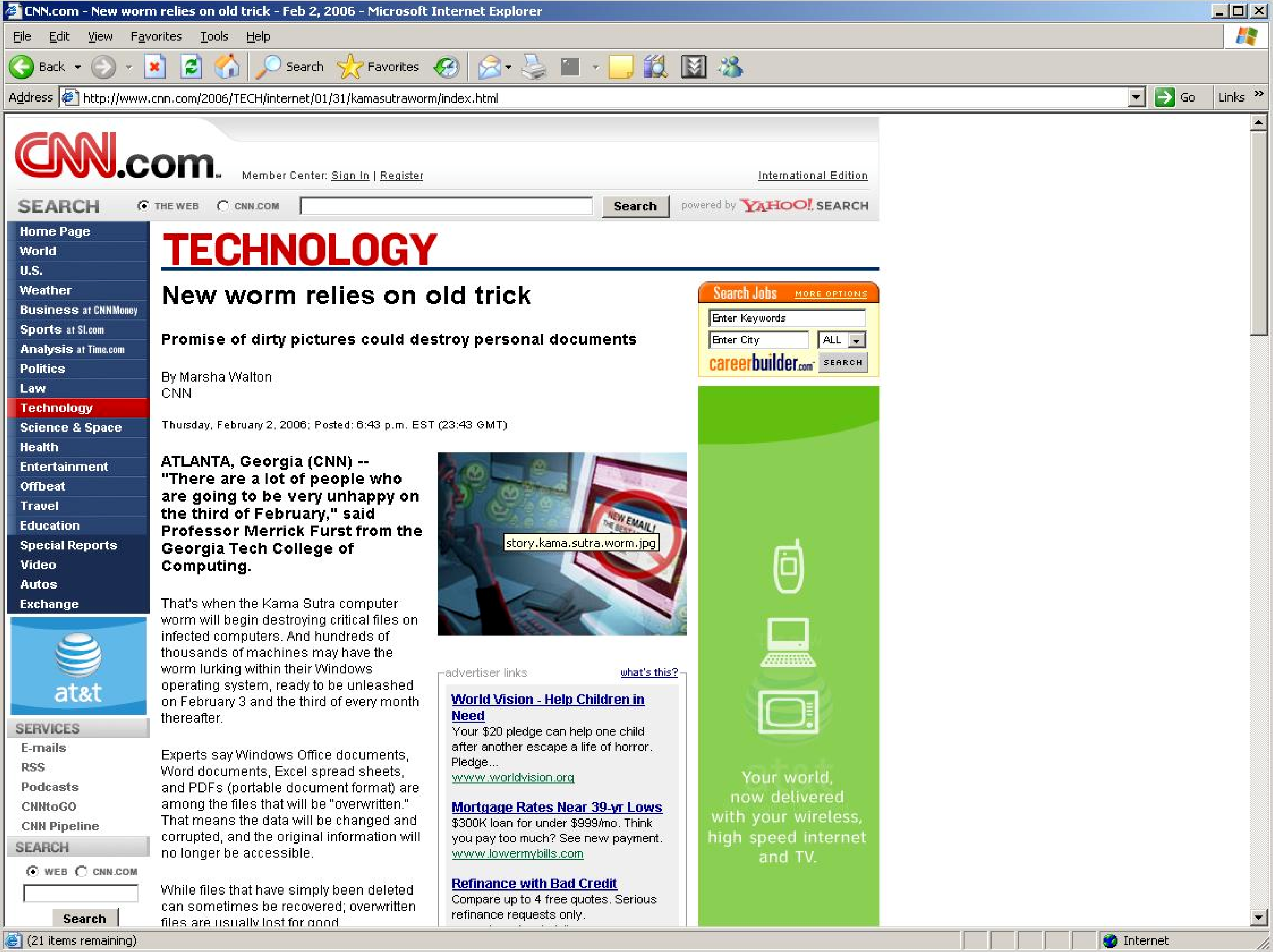
When run on a Windows PC, the worm copies itself to shared network locations and sends itself to e-mail addresses found on the target computer. The pest includes a timed attack that attempts to disable antivirus and firewall software and delete certain files, including Office documents, on the third day of the month, according to antivirus software vendor F-Secure.

The worm, dubbed W32/Nyxem-E by F-Secure, arrives attached to an e-mail message. It uses a

THE BIG | RELATED | WHAT'S HOT | LATEST

Related news

- Win32.VB worm spreading quickly
Short take, January 18, 2006
- Trojan swaps porn sites for Koran text
September 6, 2005
- Worm baits hook with hints of pope plot
June 28, 2005


CNN.com - New worm relies on old trick - Feb 2, 2006 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.cnn.com/2006/TECH/internet/01/31/kamasutraworm/index.html
Go
Links
(21 items remaining)
Internet

CNN.com Member Center: Sign In | Register International Edition

SEARCH ● THE WEB ○ CNN.COM Search powered by YAHOO! SEARCH

Home Page
World
U.S.
Weather
Business at CNNMoney
Sports at SI.com
Analysis at Time.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Offbeat
Travel
Education
Special Reports
Video
Autos
Exchange

SERVICES
E-mails
RSS
Podcasts
CNNtoGO
CNN Pipeline

SEARCH
● WEB ○ CNN.COM
Search

TECHNOLOGY

New worm relies on old trick

Promise of dirty pictures could destroy personal documents

By Marsha Walton
CNN

Thursday, February 2, 2006; Posted: 6:43 p.m. EST (23:43 GMT)

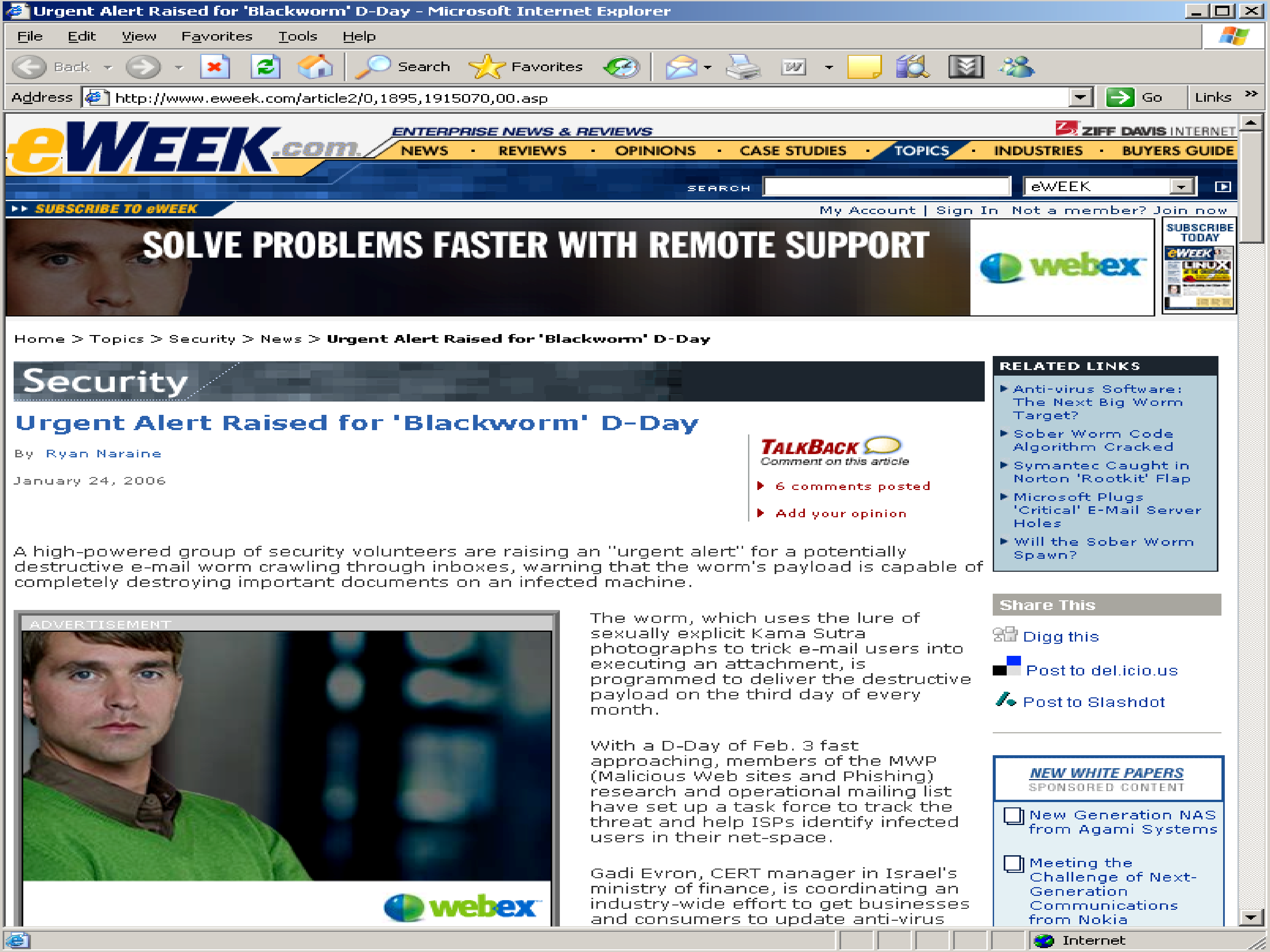
story.kama.sutra.worm.jpg

ATLANTA, Georgia (CNN) -- "There are a lot of people who are going to be very unhappy on the third of February," said Professor Merrick Furst from the Georgia Tech College of Computing.

That's when the Kama Sutra computer worm will begin destroying critical files on infected computers. And hundreds of thousands of machines may have the worm lurking within their Windows operating system, ready to be unleashed on February 3 and the third of every month thereafter.

Experts say Windows Office documents, Word documents, Excel spread sheets, and PDFs (portable document format) are among the files that will be "overwritten." That means the data will be changed and corrupted, and the original information will no longer be accessible.

While files that have simply been deleted can sometimes be recovered; overwritten files are usually lost for good


Urgent Alert Raised for 'Blackworm' D-Day - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.eweek.com/article2/0,1895,1915070,00.asp
Go Links
eWEEK.com
ENTERPRISE NEWS & REVIEWS
ZIFF DAVIS INTERNET
NEWS · REVIEWS · OPINIONS · CASE STUDIES · TOPICS · INDUSTRIES · BUYERS GUIDE
SEARCH
eWEEK
SUBSCRIBE TO eWEEK
My Account | Sign In Not a member? Join now
SOLVE PROBLEMS FASTER WITH REMOTE SUPPORT
webex
SUBSCRIBE TODAY
Internet

Home > Topics > Security > News > **Urgent Alert Raised for 'Blackworm' D-Day**

Security

Urgent Alert Raised for 'Blackworm' D-Day

By Ryan Naraine

January 24, 2006

TALKBACK
Comment on this article

- 6 comments posted
- Add your opinion

A high-powered group of security volunteers are raising an "urgent alert" for a potentially destructive e-mail worm crawling through inboxes, warning that the worm's payload is capable of completely destroying important documents on an infected machine.

The worm, which uses the lure of sexually explicit Kama Sutra photographs to trick e-mail users into executing an attachment, is programmed to deliver the destructive payload on the third day of every month.

With a D-Day of Feb. 3 fast approaching, members of the MWP (Malicious Web sites and Phishing) research and operational mailing list have set up a task force to track the threat and help ISPs identify infected users in their net-space.

Gadi Evron, CERT manager in Israel's ministry of finance, is coordinating an industry-wide effort to get businesses and consumers to update anti-virus

RELATED LINKS

- Anti-virus Software: The Next Big Worm Target?
- Sober Worm Code Algorithm Cracked
- Symantec Caught in Norton 'Rootkit' Flap
- Microsoft Plugs 'Critical' E-Mail Server Holes
- Will the Sober Worm Spawn?

Share This

Digg this

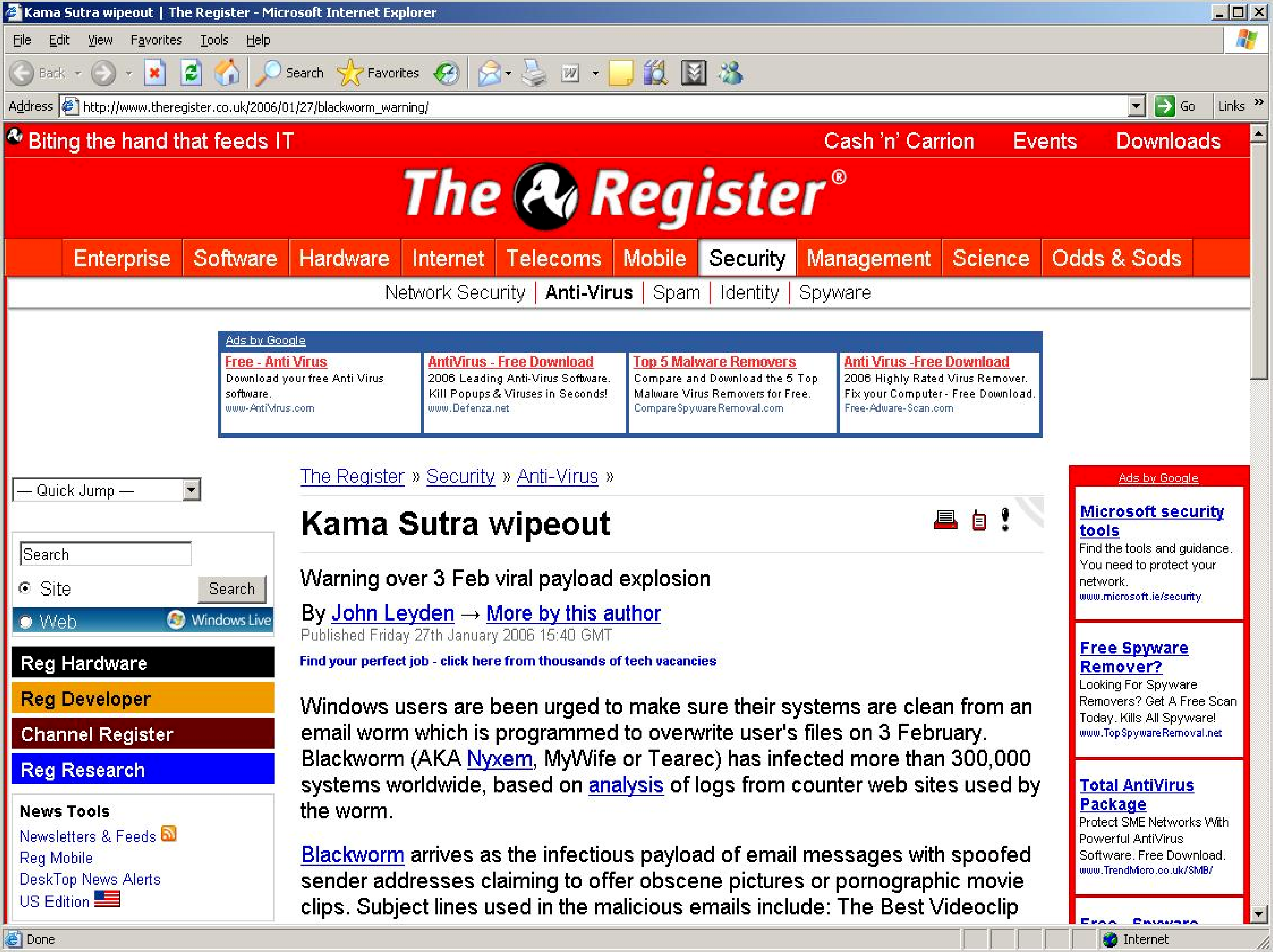
Post to del.icio.us

Post to Slashdot

NEW WHITE PAPERS
SPONSORED CONTENT

□ New Generation NAS from Agami Systems

□ Meeting the Challenge of Next-Generation Communications from Nokia



The Register » Security » Anti-Virus »

Kama Sutra wipeout

Warning over 3 Feb viral payload explosion

By John Leyden → More by this author

Published Friday 27th January 2006 15:40 GMT

Windows users are been urged to make sure their systems are clean from an email worm which is programmed to overwrite user's files on 3 February. Blackworm (AKA Nyxem, MyWife or Tearec) has infected more than 300,000 systems worldwide, based on analysis of logs from counter web sites used by the worm.

Blackworm arrives as the infectious payload of email messages with spoofed sender addresses claiming to offer obscene pictures or pornographic movie clips. Subject lines used in the malicious emails include: The Best Videoclip

W32.Blackmal.E@mm - Bug

```
L4:  On Error GoTo Next
L7:  On Error Resume at $+46
L9:  push &(Variant[-0054] = 1 As Integer)
L14:  push &[-001C]
L17:  push &[-0022]
L20:  With currentobject=this
L21:  call [currentobject.method 203], push Long result
L24:  Object[-0020] = pop (no addref on source)
L27:  With currentobject=[-0020]
L30:  call [currentobject.method 44] 117, check result
```

W32.Blackmal.E@mm - Impact

- Highly anticipated widespread damage never materialised.
- Media coverage raised awareness
- Systems with no floppy drive and using a single hard-drive partition not affected.

Osx.Leap

- Posted on “hacking” forum as pictures of Macbook Pro Internals.
- Later reposted on macrumours.com as Mac OS X “Leopard” screenshots.

- Creates an Input Manager called apphook.bundle in Library/InputManagers/
- Infects 4 most recently used apps.
- Sends copy of itself to iChat contacts.

Guardian Unlimited Technology | Technology | Mac users face first Apple virus - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://technology.guardian.co.uk/online/security/story/0,,1712275,00.html
Go
Links
Sign in · Register
Go to: Guardian Unlimited home
Go
Guardian Unlimited
Read today's paper · Jobs
Search:
Go
● Guardian Unlimited ○ Web
technology
Home | Technology blog | Ask Jack blog | Gamesblog | Games | Opinion | Innovations | Inside IT | Gameszone
Computer security
Search
● Online articles
○ Ask Jack
Go
Go to ...
Special report: computer security
Computer security: archived articles
Done
Internet

3.30pm

Mac users face first Apple virus

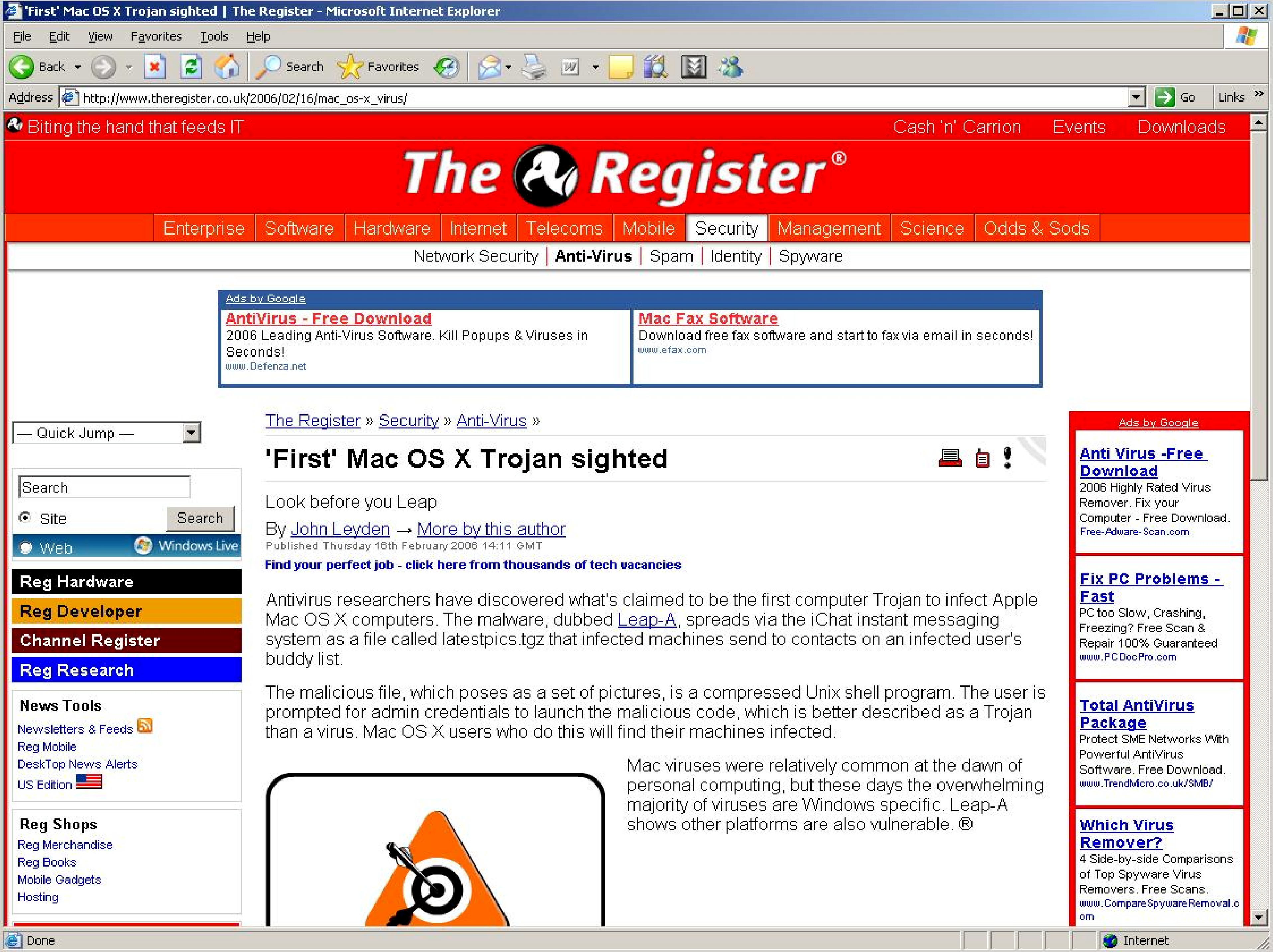
Bobbie Johnson
Friday February 17, 2006
Guardian Unlimited

Users of Apple computers were today being warned to protect themselves after the existence of a new kind of worm virus emerged.

The Leap-A worm, which spreads through instant messaging program iChat, is thought to be the first virus for the Apple platform. It poses as a series of pictures which, when opened, allows the worm through a security loophole in order to implant itself in other programs.

Experts say it is easy for users to protect themselves, but that the arrival of malicious code should be a wake-up call to Mac users, who have been unaffected by viruses until now.

"The Leap-A worm isn't in itself a significant threat, but it should act as a helpful reminder that malware [malicious software] can be written for any


'First' Mac OS X Trojan sighted | The Register - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.theregister.co.uk/2006/02/16/mac_os-x_virus/
Go Links
Biting the hand that feeds IT
Cash 'n' Carrion Events Downloads
The Register®
Enterprise Software Hardware Internet Telecoms Mobile Security Management Science Odds & Sods
Network Security Anti-Virus Spam Identity Spyware
— Quick Jump —
Search
Site Search
Web Windows Live
Reg Hardware
Reg Developer
Channel Register
Reg Research
News Tools
Newsletters & Feeds
Reg Mobile
DeskTop News Alerts
US Edition
Reg Shops
Reg Merchandise
Reg Books
Mobile Gadgets
Hosting
Done
Internet

The Register » Security » Anti-Virus »

'First' Mac OS X Trojan sighted

Look before you Leap

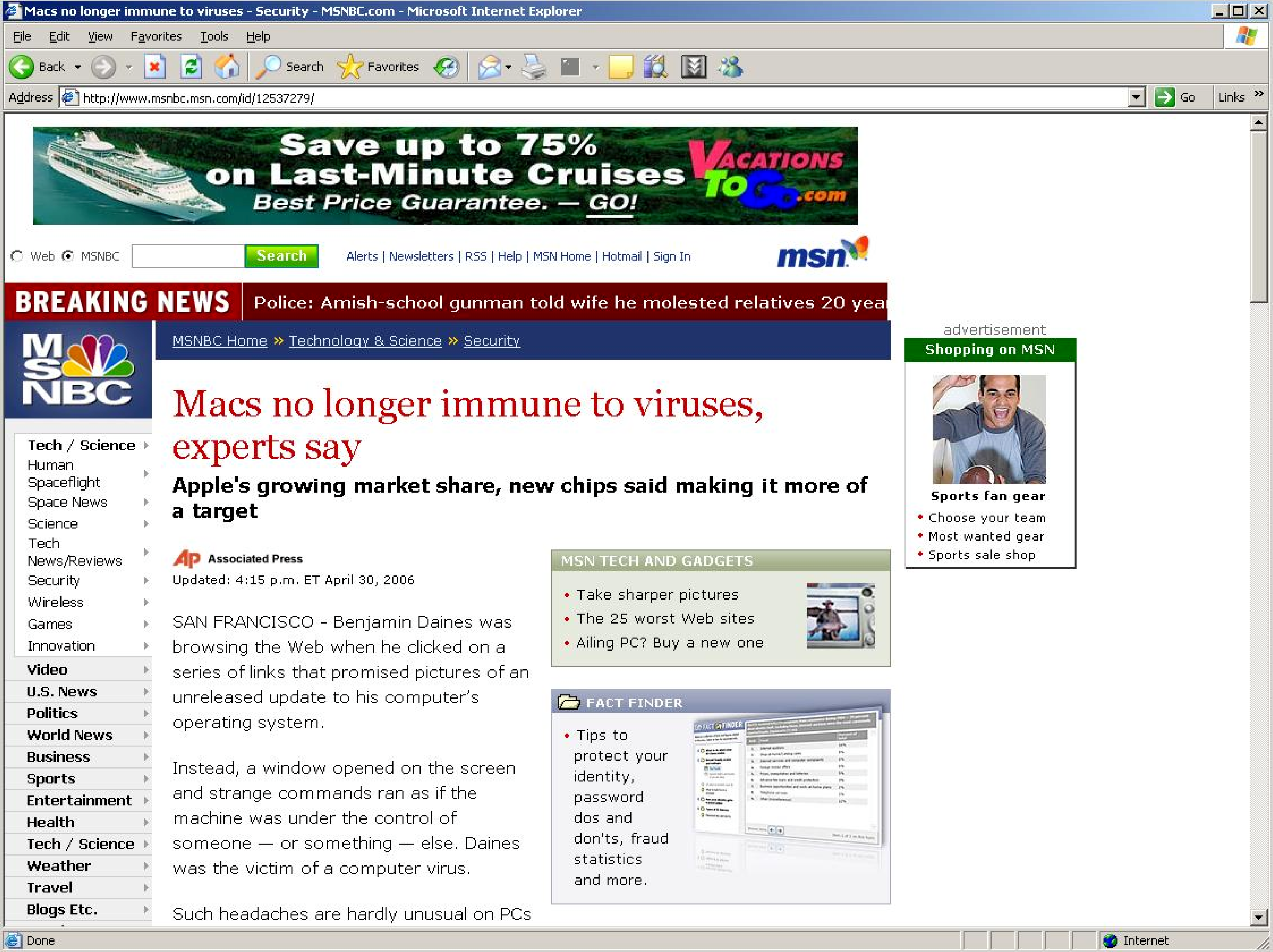
By John Leyden → More by this author

Published Thursday 16th February 2006 14:11 GMT

Antivirus researchers have discovered what's claimed to be the first computer Trojan to infect Apple Mac OS X computers. The malware, dubbed Leap-A, spreads via the iChat instant messaging system as a file called latestpics.tgz that infected machines send to contacts on an infected user's buddy list.

The malicious file, which poses as a set of pictures, is a compressed Unix shell program. The user is prompted for admin credentials to launch the malicious code, which is better described as a Trojan than a virus. Mac OS X users who do this will find their machines infected.

Mac viruses were relatively common at the dawn of personal computing, but these days the overwhelming majority of viruses are Windows specific. Leap-A shows other platforms are also vulnerable. ®


Macs no longer immune to viruses - Security - MSNBC.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.msnbc.msn.com/id/12537279/
Go
Links
Done
Internet

○ Web ● MSNBC
Search
Alerts | Newsletters | RSS | Help | MSN Home | Hotmail | Sign In
msn

BREAKING NEWS Police: Amish-school gunman told wife he molested relatives 20 yea

MSNBC Home » Technology & Science » Security
Tech / Science
Human Spaceflight
Space News
Science
Tech News/Reviews
Security
Wireless
Games
Innovation
Video
U.S. News
Politics
World News
Business
Sports
Entertainment
Health
Tech / Science
Weather
Travel
Blogs Etc.

Macs no longer immune to viruses, experts say

Apple's growing market share, new chips said making it more of a target

AP Associated Press

Updated: 4:15 p.m. ET April 30, 2006

SAN FRANCISCO - Benjamin Daines was browsing the Web when he clicked on a series of links that promised pictures of an unreleased update to his computer's operating system.

Instead, a window opened on the screen and strange commands ran as if the machine was under the control of someone — or something — else. Daines was the victim of a computer virus.

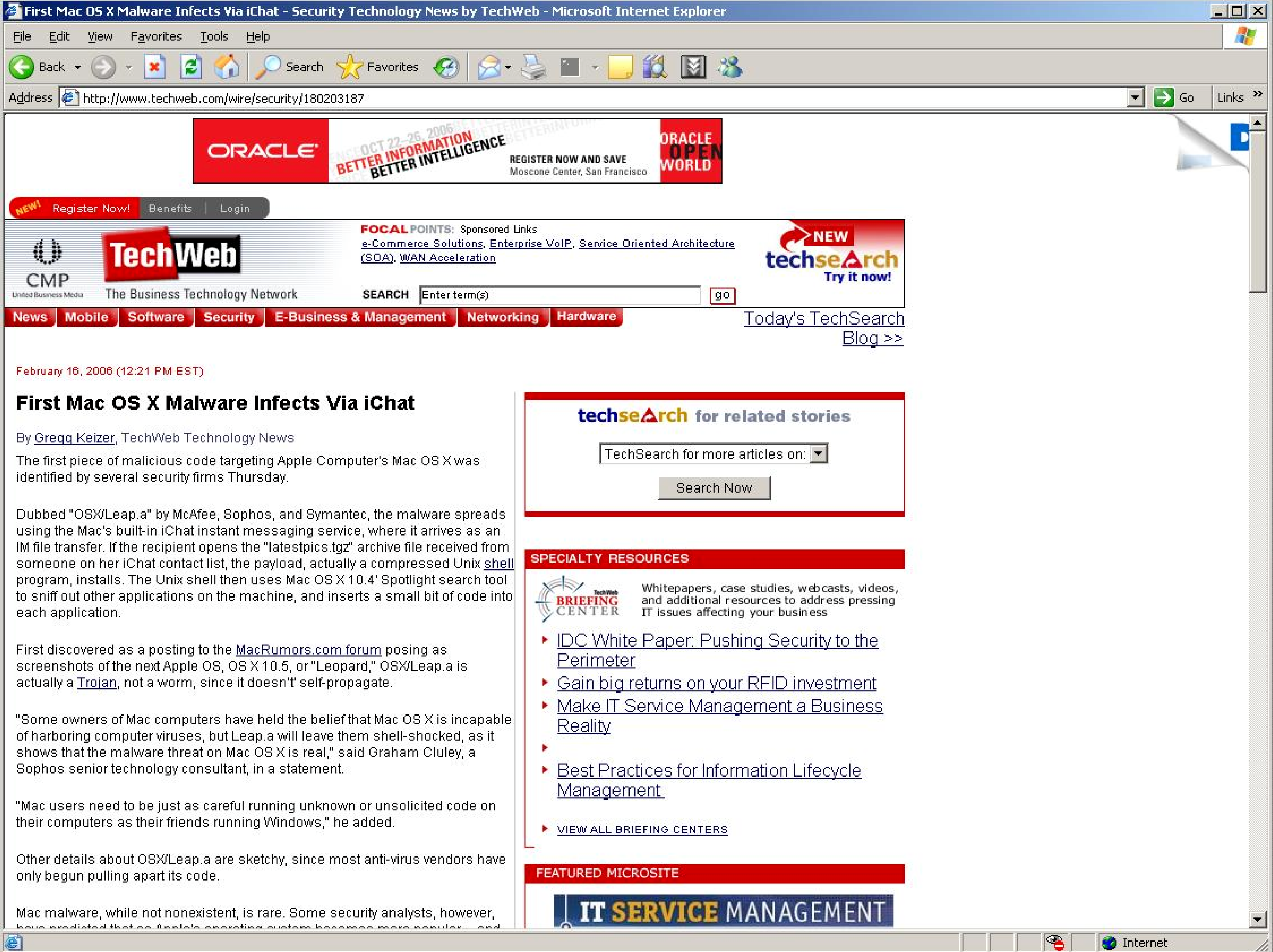
Such headaches are hardly unusual on PCs

MSN TECH AND GADGETS

- Take sharper pictures
- The 25 worst Web sites
- Ailing PC? Buy a new one

FACT FINDER

- Tips to protect your identity, password dos and don'ts, fraud statistics and more.


First Mac OS X Malware Infects Via iChat - Security Technology News by TechWeb - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.techweb.com/wire/security/180203187
Go
Links
Internet

NEW! Register Now! | Benefits | Login

CMP United Business Media

TechWeb
The Business Technology Network

FOCAL POINTS: Sponsored Links
e-Commerce Solutions, Enterprise VoIP, Service Oriented Architecture (SOA), WAN Acceleration

SEARCH Enter term(s) go

NEW techsearch Try it now!

News | Mobile | Software | Security | E-Business & Management | Networking | Hardware

Today's TechSearch Blog >>

February 16, 2006 (12:21 PM EST)

First Mac OS X Malware Infects Via iChat

By Gregg Keizer, TechWeb Technology News

The first piece of malicious code targeting Apple Computer's Mac OS X was identified by several security firms Thursday.

Dubbed "OSX/Leap.a" by McAfee, Sophos, and Symantec, the malware spreads using the Mac's built-in iChat instant messaging service, where it arrives as an IM file transfer. If the recipient opens the "latestpics.tgz" archive file received from someone on her iChat contact list, the payload, actually a compressed Unix shell program, installs. The Unix shell then uses Mac OS X 10.4' Spotlight search tool to sniff out other applications on the machine, and inserts a small bit of code into each application.

First discovered as a posting to the MacRumors.com forum posing as screenshots of the next Apple OS, OS X 10.5, or "Leopard," OSX/Leap.a is actually a Trojan, not a worm, since it doesn't' self-propagate.

"Some owners of Mac computers have held the belief that Mac OS X is incapable of harboring computer viruses, but Leap.a will leave them shell-shocked, as it shows that the malware threat on Mac OS X is real," said Graham Cluley, a Sophos senior technology consultant, in a statement.

"Mac users need to be just as careful running unknown or unsolicited code on their computers as their friends running Windows," he added.

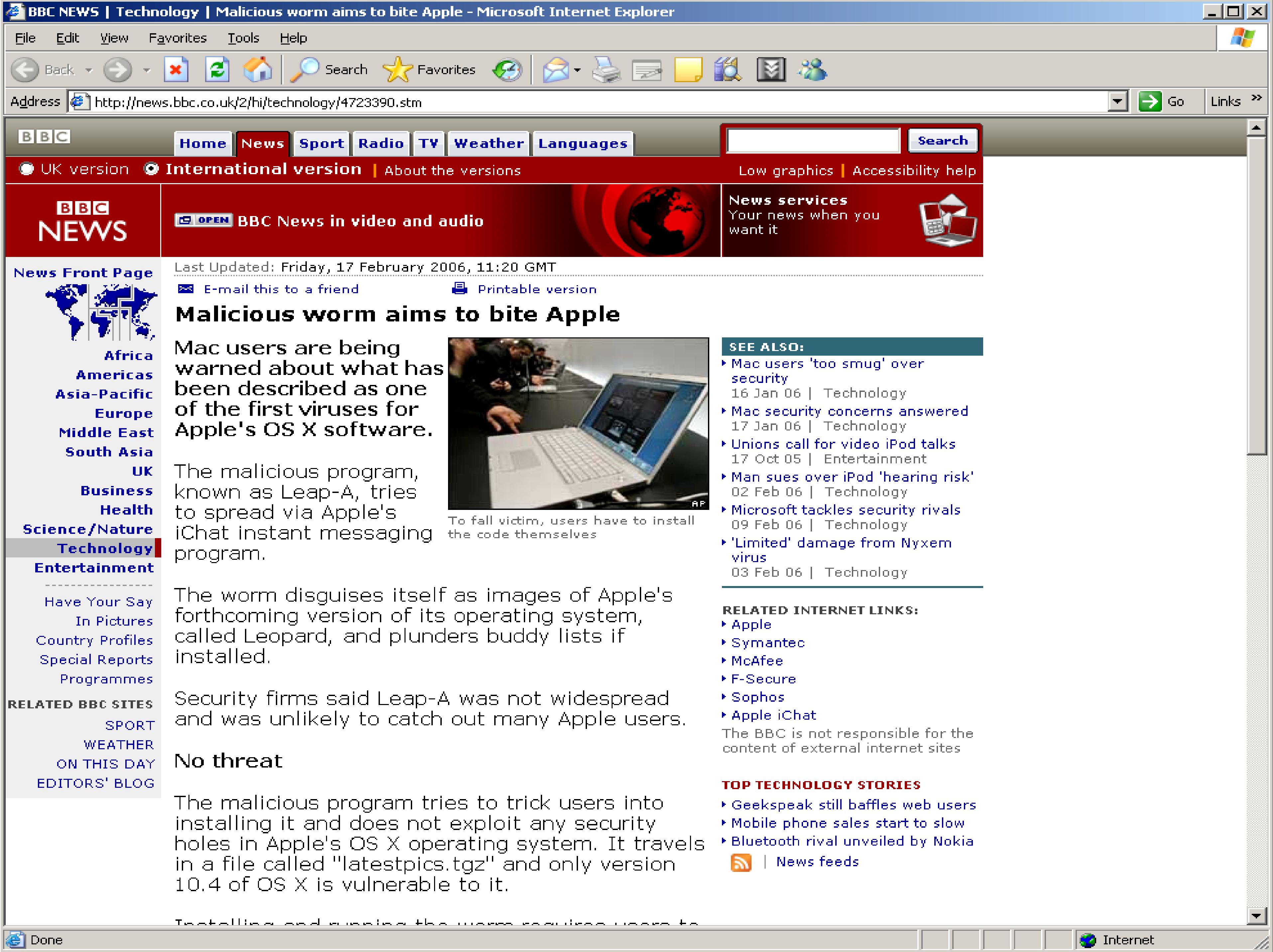
Other details about OSX/Leap.a are sketchy, since most anti-virus vendors have only begun pulling apart its code.

Mac malware, while not nonexistent, is rare. Some security analysts, however, have predicted that as Apple's operating system becomes more popular -- and

techsearch for related stories

TechSearch for more articles on:

Search Now


BBC NEWS | Technology | Malicious worm aims to bite Apple - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://news.bbc.co.uk/2/hi/technology/4723390.stm
Go
Links
Done
Internet

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

Have Your Say
In Pictures
Country Profiles
Special Reports
Programmes

RELATED BBC SITES
SPORT
WEATHER
ON THIS DAY
EDITORS' BLOG

Last Updated: Friday, 17 February 2006, 11:20 GMT

E-mail this to a friend | Printable version

Malicious worm aims to bite Apple

Mac users are being warned about what has been described as one of the first viruses for Apple's OS X software.

To fall victim, users have to install the code themselves

The malicious program, known as Leap-A, tries to spread via Apple's iChat instant messaging program.

The worm disguises itself as images of Apple's forthcoming version of its operating system, called Leopard, and plunders buddy lists if installed.

Security firms said Leap-A was not widespread and was unlikely to catch out many Apple users.

No threat

The malicious program tries to trick users into installing it and does not exploit any security holes in Apple's OS X operating system. It travels in a file called "latestpics.tgz" and only version 10.4 of OS X is vulnerable to it.

Installing and running the worm requires users to

SEE ALSO:
- Mac users 'too smug' over security
  16 Jan 06 | Technology
- Mac security concerns answered
  17 Jan 06 | Technology
- Unions call for video iPod talks
  17 Oct 05 | Entertainment
- Man sues over iPod 'hearing risk'
  02 Feb 06 | Technology
- Microsoft tackles security rivals
  09 Feb 06 | Technology
- 'Limited' damage from Nyxem virus
  03 Feb 06 | Technology

RELATED INTERNET LINKS:
- Apple
- Symantec
- McAfee
- F-Secure
- Sophos
- Apple iChat

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES
- Geekspeak still baffles web users
- Mobile phone sales start to slow
- Bluetooth rival unveiled by Nokia

News feeds

Osx.Leap - Bug

```
__text:00002D68 38 63 00 04          addi   %r3, %r3, 4    # size_t
__text:00002D6C 48 00 09 B5           bl     _malloc_stub
```

•the *snprintf* call will result in only “/..” and a trailing terminating null character to be appended to the string

•iChat code may corrupt the file so that it appears larger than it actually is.

Osx.Leap - Impact

- iChat bugs limited spread.
- Damage once infected was increased by rendered applications useless once infected.

Sobig, Sobad

- Early January 2003, with a total of 6 variants released over the following 8 months.
- Named for the large size of its code.
- Initial purpose was to spread a proxy server Trojan the author had put together the previous year.

Sobig - Bugs

- Sobig opens with a bug in the first line of code. Is this a record?
- Sobig.A converts the current date to *yyyy.mm.d* format, and compares it against *2003.1.23*
- To prevent multiple copies of the worm executing at the same time, Sobig uses a named event.
- Sobig.F Network share Enumeration.

Sobig - Bugs

```
•.shrink:00409517    push   ds:lpazTrayX    ; lpName
•.shrink:0040951D    push   esi             ; bInitialState
•.shrink:0040951E    push   1               ; bManualReset
•.shrink:00409520    push   esi             ; lpEventAttributes
•.shrink:00409521    call   ds:CreateEventA
•.shrink:00409527    mov    edi, ds:WaitForSingleObject
•.shrink:0040952D    push   esi             ; dwMilliseconds
•.shrink:0040952E    push   eax             ; hHandle
•.shrink:0040952F    mov    [ebp+hOwnEvent], eax
•.shrink:00409532    call   edi ; WaitForSingleObject
•.shrink:00409534    test   eax, eax
•.shrink:00409536    jnz    short ok_1
•.shrink:00409538    or     esi, 0FFFFFFFFh
•.shrink:0040953B    jmp    done
```

Sobig – Bugs

```
.shrink:00409540 ok_1:                        ; CODE XREF: WinMain(x,x,x,x)+AA_j
.shrink:00409540             push   [ebp+lpData]    ; char *
.shrink:00409543             call   _strlen
.shrink:00409548             test   eax, eax
.shrink:0040954A             pop    ecx
.shrink:0040954B             jz     no_commandline
.shrink:00409551             mov    ebx, [ebp+hOwnEvent]
.shrink:00409554             push   ebx             ; hEvent
.shrink:00409555             call   ds:SetEvent
.shrink:0040955B             lea    eax, [ebp+CommandLine]
.shrink:00409561             push   eax             ; lpWSAData
.shrink:00409562             push   202h            ; wVersionRequested
.shrink:00409567             call   WSAStartup
.shrink:0040956C             test   eax, eax
.shrink:0040956E             jz     short ok_2
```

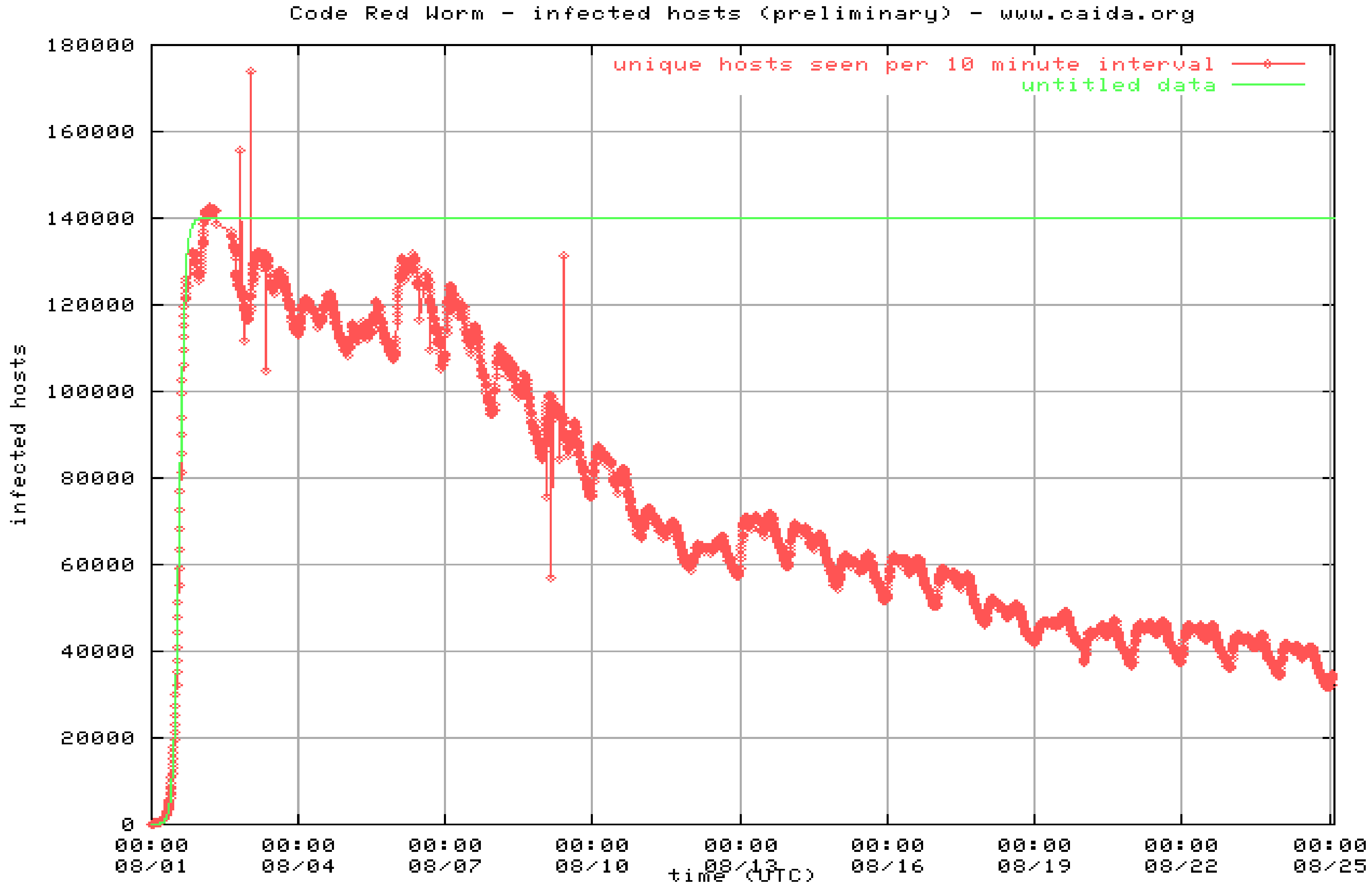
Sobig - Impact

- Many small bugs indicate a lack of proper testing.
- Nevertheless, the Sobig family spread very successfully, and Sobig.F became one of the biggest viral threats in 2003.

Code Red

- Static seed used when generating target IP address.

Code Red


Code Red Worm - infected hosts (preliminary) - www.caida.org
unique hosts seen per 10 minute interval
untitled data
infected hosts
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
00:00 08/01
00:00 08/04
00:00 08/07
00:00 08/10
00:00 08/13
00:00 08/16
00:00 08/19
00:00 08/22
00:00 08/25
time (UTC)

Code Red

- Static seed used when generating target IP address.
- Crippled the spread of the worm.
- Infected same machines over and over.
- Denial of Service due to the amount of data being transferred between the addresses generated.

W32.Lovgate.A@mm

- Bug or feature? After setting up the variable szPassword1 as “xyz123”, the worm proceeds to check the password received as follows…

VBS.SST@mm

```
Set opentextfile=
filesystemobject.opentextfile(wscript.scriptfullname, 1)
opentextfilereadall= opentextfile.readall
opentextfile.Close
Do
  If Not
(filesystemobject.fileexists(wscript.scriptfullname)) Then
    Set createfile=
filesystemobject.createtextfile(wscript.scriptfullname,
True)
    createfile.writeopentextfilereadall
    createfile.Close
  End If
Loop
```

VBS.Pet_Tick.N

```
Set gd=fso.OpenTextFile(cible.path,1)
If gd.readline <> "<Lover>" Then
htmorg=gd.Readall
gd.Close
Set gd=fso.OpenTextFile(cible.path,2)
gd.WriteLine "<dilan>"
gd.Write(htmorg)
gd.WriteLine document.body.createtextrange.htmltext
```

W32.Beagle.BH@mm

- This variant adds a value corresponding to its filename to the following registry keys, in what appears to be an attempt to ensure they are executed on startup…

W32.Netsky.D@mm

- When looking for files to extract email addresses from Netsky.D does the following…

W32.Mytob.MK@mm

•Sets the registry run key;

```
"WINDOWS" = "\jif.exe"
```

•However, the worm does not create a copy of itself as jif.exe in the system path so the attempt to execute the file on boot will fail.

The Professional Era

- Increases in the effectiveness of code released.
- More advanced techniques being used more often.
- More targeted attacks - developed for a specific environment.

Conclusions

- If blackboxing, assume threat may function as intended, perhaps on differing systems.
- Provide as much information as possible in the early stages of analysis.
- A bug can make a difference between a threat that is critical and one that is not.
- Acting on the information we provide costs customers money.

Questions?

Thanks.

john_canavan@symantec.com