FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1466263-0

Total Deleted Page(s) = 3
Page 22 ~ Duplicate;
Page 23 ~ Duplicate;
Page 24 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXXX
```

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/13/2001

To: Charlotte **Attn:** SSA [redacted] b6
Squad 7 b7C
Counterterrorism SSA [redacted]
NIPC, CIU

From: Charlotte
Squad 7, Raleigh RA
Contact: SA [redacted] b3 b6 b7C b7E

Approved By: [redacted] DHG

Drafted By: [redacted] tjm TJM

Case ID #: [redacted]

Title: UNSUB(S);
STATE OF NORTH CAROLINA - VICTIM;
ANNA KOURNIKOVA VIRUS; VBS/SST VIRUS - FEBRUARY 2000;
[redacted]
OO: CE

Synopsis: Request above captioned matter be Opened and Assigned to SA [redacted] b6 b7C

Enclosures: (4) - Enclosed for FBIHQ are copies of four documents obtained on the Internet regarding the above captioned matter. One document from the web site: www.symantec.com, two documents from the web site: www.zdnet.com, and one document from the web site: www.cert.org.

2/15/01 L/T TJM

Details: On 02/12/00, [redacted] b6 b7C State of North Carolina, Office of Information Technology, P.O. Box 17209, Raleigh, NC 27619, telephone: [redacted] advised many of the State of North Carolina's computers have been infected by a computer virus/worm known as the Anna Kournikova virus or the vbs/sst virus. The infections have caused considerable damage to the mail servers of several State of North Carolina Agencies and Departments to include the Department of Insurance, the Department of Agriculture, the Department of Transportation, and the Governor's Office.

Information concerning this virus was located on the Internet at www.symantec.com and www.zdnet.com and is enclosed. This information subsequently propagated to NIPC's web page and www.cert.org. The CERT information is also enclosed.

O & A [redacted] DHG Case opened & assigned 2/15/01 b6 b7C

044TJM01.EC

To: Charlotte From: Charlotte
Re: [redacted] 02/13/2001

b3
b6
b7C
b7E

[redacted] will continue to effect the technical solutions to resolve this matter and quantify the scope of the damage.

It is requested this matter be O&A'd to SA [redacted]

[redacted]

To: Charlotte From: Charlotte
Re: [redacted] 02/13/2001 b3 b7E

LEAD(s):

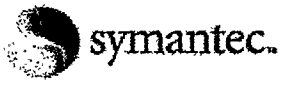
Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

For information of SSA [redacted] read and clear. b6 b7C

♦♦



security up

VBS.SST@mm

Discovered on: February 12, 2001
Last Updated on: February 12, 2001 at 10:10:59 AM PST

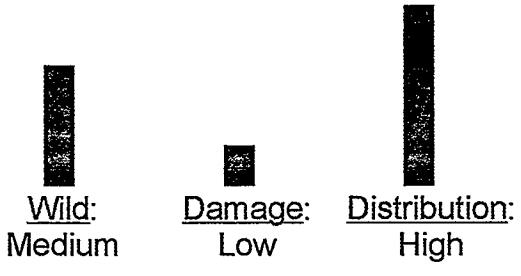
The Symantec AntiVirus Research Center (SARC) has confirmed a new mass-mailing worm. SARC is currently analyzing the worm. The worm is being reported in an attachment named ANNAKOURNIKOVA.JPEG.VBS. SARC recommends that you filter attachments with a VBS extension if you have not already done so.

Category: Worm

Aliases: ANNAKOURNIKOVA.JPEG.VBS

Virus definitions: Pending

Threat assessment:



Wild

- Number of infections: 0-49

Distribution

- Subject of email: Here you have, ;o)
- Name of attachment: AnnaKournikova.jpg.vbs

Technical description:

VBS.SST is a VBS email worm that has been encoded with a virus creation kit. The worm arrives as an attachment named AnnaKournikova.jpg.vbs When executed the worm emails itself to everyone in your address book. On January 26, the worm will attempt to spawn the web browser to an Internet address. This worm appears to have originated in the Netherlands

When run the virus creates the registry key

HKCU/Software/OnTheFly/

If the day is January 26, the virus attempts to spawn the web browser to http://www.dynabyte.nl

Next, the virus checks to see if the mass-mailing routine has been executed. If not, the worm emails everyone in the Outlook address book and creates the registry key HKCU/Software/OnTheFly/mailed

So, the worm does not email every address again. The worm sends the message with the subject Here you have, ;o)

The message body

Hi:
Check This!

and the attachment AnnaKournikova.jpg.vbs

The worm then remains running and if it is deleted attempts to recreate itself. Due to a bug in the code, the virus instead recreates itself as a zero-byte file.

Removal Instructions:

1. Delete all found infections. If exists, delete the zero-byte file.
2. Remove registry keys

Write-up by: Eric Chien

 *Tell a Friend about this Write-Up*

From Russia with love? Kournikova virus smashes Net

By *Robert Lemos*, ZDNN
February 12, 2001 10:59 AM PT
URL:

A virus posing as a photo of Russian tennis player Anna Kournikova spread aggressively on Monday, as major security companies rushed to update their antivirus software to detect the fast-spreading e-mail virus.

"Compared to the 'Love Bug', it's spreading twice as fast," said Alex Shipp, antivirus technologist with British e-mail service MessageLabs. In the five hours since MessageLabs detected the infection, its users have received almost 2,900 copies of the infected e-mail sent from more than 290 different domains.

Also known as VBS/SST, the virus initially poses as an attachment--AnnaKournikova.jpg.vbs--included in a message with one of three similar subject lines: "Here you are ;-)," "here you have ;o)" and "here you go ;-)."

The virus uses the Visual Basic scripting language to infect Windows systems and then, on systems using Microsoft's Outlook e-mail program, mails itself out to the entire address book. The ability to mail itself out to a large number of Internet users classifies the virus as a worm.

The virus does not damage the systems it has infected, said Vincent Weafer, director of Symantec's AntiVirus Research Center.

And while the virus has only a few subject lines--which makes it easy for network administrators to filter it out before it ever reaches the desktop--it does use encryption to make it harder for antivirus software to detect it.

"Internally, it's highly polymorphic, which means it changes its signatures to hide itself from antivirus software," said Weafer. He said SARC has only seen 20 copies of the virus but expects it to spread quickly.

As of 11:15 a.m. PST, major antivirus software makers had either posted patches to detect the virus or were already detecting it with the latest version.

"We are working on detection right now," said Weafer.

Businesses that had detected the virus or had been infected by it kept the security companies busy early Monday. Symantec had received 20 calls from clients in the morning, Network Associates almost 50, Computer Associates nearly 25 and Trend Micro a dozen.

Antivirus software maker Trend Micro said the virus had hit many different types of companies.

"We have heard from a government agency that have seen 200 hits per hour," spokeswoman Susan Orbuch said. "Others include a banking institution, a major networking company, a beverage company and an insurance company. You are not just seeing it in one sector."

Several experts believe the worm to be the product of a so-called "virus creation kit," a program that lets any online vandal with rudimentary computer skills to point-and-click their way to creating malicious code.

Trend Micro's software detected the virus originally as VBS_KALAMAR, and believes that Kalamar is the name of the author of the virus creation kit.

Anna virus spreading fast

By *Robert Vamosi*, Help & How-To
February 12, 2001 9:32 AM PT
URL:

February 12, 2001, *revised*

There's a new virus spamming the world. Anna (a.k.a., VBS/SST, Kalamar, OnTheFly) has some of the same characteristics as the ILOVEYOU worm. Anti-virus software companies are still investigating this new worm. Anna is known to be a mass mailer; the number of infections worldwide has risen every hour. Anna uses listings found in the Microsoft Outlook address book to send copies of itself. The real danger from Anna is that it will overload e-mail servers with excess traffic. Anna currently ranks as a 7 on the ZDNet Virus Meter.

How It Works
The Anna virus arrives via e-mail with the following information:

Subject: Here you have, ;o)

Body: Hi: Check This!

Attachment: AnnaKournikova.jpg.vbs

Clicking on the attachment activates the worm. Once activated, Anna uses the Microsoft Outlook address book to mass e-mail itself to others. Anna then changes the Registry to include the following entry:

HKCUsoftwareOnTheFly

Also, Anna schedules itself to connect to a Dutch computer shopping Web site, www.dynabyte.nl, every January 26th.

Prevention

Here are the key steps for preventing the latest outbreak:

1. Download Microsoft's Outlook Security Patch. If you haven't already installed it, download the Outlook 98 Security Patch or the Outlook 2000 Security Patch (which requires the Office 2000 Service Release 1a). Please note that this patch does not include Outlook Express. Click here for help with installation, or for more information regarding this patch.

2. Turn off Windows Scripting Host. Recent virus outbreaks have exploited known vulnerabilities in Visual Basic Scripting under Windows. To limit your risk of infection, you should turn off Windows Scripting Host. For a complete discussion of the pros and cons of removing Windows Scripting Host, see this article.

3. "Don't open attachments!" One of the best ways to prevent virus infections is not to open attachments, especially when viruses such as [Fireburn] are being actively circulated. Even if the e-mail is from a known source, be careful. A few viruses take the mailing lists from an infected computer and send out new messages with its destructive payload attached. Always scan the attached files first for viruses. Unless it's a file or an image you are expecting, delete it.

4. Stay informed. Did you know that there are virus and security alerts almost every day? Keep up-to-date on breaking viruses and solutions by bookmarking our Viruses, Bugs, Security Alerts page.

5. Get protected. If you don't already have virus protection software on your machine, you should. If you're a home or individual user, it's as easy as downloading any of these five-star programs then following the installation instructions. If you're on a network, check with your network administrator first.

6. Scan your system regularly. If you're just loading anti-virus software for the first time, it's a good idea to let it scan your entire system. It's better to start with your PC clean and free of virus problems. Often the anti-virus program can be set to scan each time the computer is rebooted or on a periodic schedule. Some will scan in the background while you are connected to the Internet. Make it a regular habit to scan for viruses.

7. Update your anti-virus software. Now that you have virus protection software installed, make sure it's up-to-date. Some anti-virus protection programs have a feature that will automatically link to the Internet and add new virus detection code whenever the software vendor discovers a new threat. You can also download updates from ZDNet Updates.com.

To stay up-to-date on the latest virus alerts and solutions, bookmark our Virus Protection Guide.

Related:

Advisories

Summaries

Vendor-Initiated Bulletins

Subscribing to the CERT Mailing List

Current Activity

Incident Notes

Vulnerability Notes

CERT® Advisory CA-2001-03 VBS/OnTheFly (Anna Kournikova) Malicious Code

Original release date: February 12, 2001
Last revised: February 12, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Users of Microsoft Outlook who have not applied previously available security updates.

Overview

The "VBS/OnTheFly" malicious code is a VBScript program that spreads via email. As of 7:00 pm EST(GMT-5) Feb 12, 2001, the CERT Coordination Center had received reports from more than 100 individual sites. Several of these sites have reported suffering network degradation as a result of mail traffic generated by the "VBS/OnTheFly" malicious code.

This malicious code can infect a system if the enclosed email attachment is run. Once the malicious code has executed on a system, it will take the actions described in the Impact section.

I. Description

When the malicious code executes, it attempts to send copies of itself, using Microsoft Outlook, to all entries in each of the address books. The sent mail has the following characteristics:

- **SUBJECT:** "`Here you have, ;o)`"
- **BODY:**

```
Hi:
Check This!
```

- **ATTACHMENT:** "`AnnaKournikova.jpg.vbs`"

Users who receive copies of the malicious code via electronic mail will probably recognize the sender. We encourage users to avoid executing code, including VBScripts, received through electronic mail, regardless of the sender's name, without prior knowledge of the origin of the code or a valid digital signature.

It is possible for the recipients to be be tricked into opening this malicious attachment since file will appear without the .VBS extension if "Hide file extensions for known file types" is turned on in Windows.

II. Impact

When the attached VBS file is executed, the malicious code attempts to modify the registry by creating the following key:

HKEY_CURRENT_USER\Software\OnTheFly="Worm made with Vbswg 1.50b"

Next, the it will then place a copy of itself into the Windows directory.

C:\WINDOWS\AnnaKournikova.jpg.vbs

Finally, the malicious code will attempt to send separate, infected email messages to all recipients in the Windows Address Book. Once the mail has been sent, the malicious code creates the following registry key to prevent future mailings of the malicious code.

HKEY_USERS\.DEFAULT\Software\OnTheFly\mailed=1

The code's propagation can lead to congestion in mail servers that may prevent them from functioning as expected.

Beyond this effect, there does not appear to be a destructive payload associated with this malicious code. However, historical data has shown that the intruder community can quickly modify the code for more destructive behavior.

III. Solution

Update Your Anti-Virus Product

It is important for users to update their anti-virus software. Some anti-virus software vendors have released updated information, tools, or virus databases to help combat this malicious code. A list of vendor-specific anti-virus information can be found in Appendix A.

Apply the Microsoft Outlook E-mail Security Update

To protect against this malicious code, and others like it, users of Outlook 98 and 2000 may want to install the Outlook E-mail Security update included in an Outlook SR-1. More information about this update is available at

http://office.microsoft.com/2000/downloaddetails/Out2ksec.htm

You may also find the following document on Outlook security useful

http://www.microsoft.com/office/outlook/downloads/security.htm

The Outlook E-mail security update provides features that can prevent attachments containing executable content from being displayed to users. Other types of attachments can be so that they must be saved to disk before they can be opened (or executed). These features may greatly reduce the chances that a user will incorrectly execute a malicious attachment.

Filter the Virus in Email

Sites can use email filtering techniques to delete messages containing subject lines known to contain the malicious code, or can filter attachments outright.

Exercise Caution When Opening Attachments

Exercise caution when receiving email with attachments. Users should disable auto-opening or previewing of email attachments in their mail programs. Users should never open attachments from an untrusted origin, or that appear suspicious in any way. Finally, cryptographic checksums should also be used to validate the integrity of the file.

IV. General protection from email Trojan horses and viruses

Some previous examples of malicious files known to have propagated through electronic mail include:

Melissa macro virus - discussed in CA-99-04 http://www.cert.org/advisories/CA-1999-04.html

False upgrade to Internet Explorer - discussed in CA-99-02 http://www.cert.org/advisories/CA-1999-02.html

Happy99.exe Trojan Horse - discussed in IN-99-02 http://www.cert.org/incident_notes/IN-99-02.html

CIH/Chernobyl virus - discussed in IN-99-03 http://www.cert.org/incident_notes/IN-99-03.htm

In each of the above cases, the effects of the malicious file are activated only when the file in question is executed. Social engineering is typically employed to trick a recipient into executing the malicious file. Some of the social engineering techniques we have seen used include

- Making false claims that a file attachment contains a software patch or update
- Implying or using entertaining content to entice a user into executing a malicious file
- Using email delivery techniques that cause the message to appear to have come from a familiar or trusted source
- Packaging malicious files in deceptively familiar ways (e.g., use of familiar but deceptive program icons or file names)

The best advice with regard to malicious files is to avoid executing them in the first place. CERT advisory CA-1999-02.html and the following CERT tech tip discuss malicious code and offers suggestions to avoid them.

http://www.cert.org/advisories/CA-1999-02.html

Tech tip: Protecting yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond

Appendix A. - Vendor Information

Appendix A. Anti-Virus Vendor Information

Aladdin Knowledge Systems

http://www.aks.com/home/csrt/valerts.asp#AnnaK

Command Software Systems, Inc.

http://www.commandcom.com/virus/vbsvwg.html

Computer Associates

http://ca.com/virusinfo/virusalert.htm#vbs_sstworm

F-Secure

http://www.f-secure.com/v-descs/onthefly.shtml

Finjan Software, Ltd.

http://www.finjan.com/attack_release_detail.cfm?attack_release_id=47

McAfee

http://www.mcafee.com/anti-virus/viruses/vbssst/default.asp

Dr. Solomon, NAI

http://vil.nai.com/vil/virusSummary.asp?virus_k=99011

Sophos

http://www.sophos.com/virusinfo/analyses/vbsssta.htm

Symantec

http://www.symantec.com/avcenter/venc/data/vbs.sst@mm.html

Trend Micro

http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_KALAMAR.A

You may wish to visit the CERT/CC's Computer Virus Resources Page located at:

http://www.cert.org/other_sources/viruses.html

This document was written by Cory Cohen, Roman Danyliw, Ian Finlay, John Shaffer, Shawn

Hernan, Kevin Houle, Brian B. King, and Shawn Van Ittersum.

This document is available from: http://www.cert.org/advisories/CA-2001-03.html

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

February 12, 2001: Initial release

0002 MRI 00020/044

OO AFO FBICE ALO

DE RUCNFB #0001 0440316

ZNR UUUUU

O 130027Z FEB 01

FM DIRECTOR FBI [redacted]

b3
b7E

TO ZEN/AIG 4505/IMMEDIATE/

ALL FBI FIELD OFFICES/IMMEDIATE/

ALL LEGATS/IMMEDIATE/

BT

UNCLAS

CITE: //1332//

PASS: NSA FOR ZKZK 00 ZSL DE; WHITE HOUSE SITUATION ROOM PLEASE PASS TO EOP SECURITY OFFICE; NIPC TO FEDCIRC AND CARNEGIE MELLON CERT. FBI FIELD OFFICES PLEASE PASS TO RESPECTIVE INFRAGARD AND KEY ASSET MEMBERS.

SUBJECT: NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC) ASSESSMENT QUOTE ANNA KOURNIKOVA VBS/SST VBS VIRUS UNQUOTE (ASSESSMENT 01-001) 12 FEBRUARY 2001.

BASED UPON INVESTIGATIONS AND INFORMATION FROM OTHER SOURCES, THE QUOTE ANNA KOURNIKOVA UNQUOTE MASS-MAILING WORM/VIRUS IS

FOR INFO OF THE FILE

[redacted]

b3
b6
b7C
b7E

[redacted]

SEARCHED
FOIMS
INDEXED

QUOTE ANNA KOURNIKOVA UNQUOTE MASS-MAILING WORM/VIRUS IS SPREADING RAPIDLY THROUGHOUT THE INTERNET. ALTHOUGH IT IS PROPAGATING RAPIDLY, IT IS SEEN AS A LOW THREAT DUE TO ITS APPARENTLY NON-DESTRUCTIVE PAYLOAD. ALTHOUGH IT DOES NOT INFECT FILES ON THE VICTIM'S SYSTEMS, THIS MASS-MAILING WORM CAN POTENTIALLY CLOG EMAIL SERVERS BECAUSE OF THE VOLUME IT GENERATES. ADMINISTRATORS ARE ADVISED TO ADJUST THEIR FILTERING SOFTWARE TO BLOCK ATTACHMENTS WITH THE NAME OF ANNA KOURNIKOVA.JPG.VBS. ADDITIONALLY, USERS SHOULD NOT OPEN ANY EMAILS OR ATTACHMENTS WITH THE ANNA KOURNIKOVA.JPG.VBS NAME.

VBS/SST.WORM IS A VISUAL BASIC SCRIPT WORM THAT SPREADS VIA E-MAIL BY USING THE MAPI APPLICATIONS SUCH AS MICROSOFT OUTLOOK AND OUTLOOK EXPRESS. THE WORM ARRIVES ATTACHED TO AN E-MAIL MESSAGE THAT HAS THE SUBJECT LINE: QUOTE HERE YOU HAVE, ;0) UNQUOTE THE MESSAGE BODY CONTAINS THE FOLLOWING TEXT: QUOTE HI: CHECK THIS! UNQUOTE THE ATTACHMENT TO THE E-MAIL MESSAGE IS A VISUAL BASIC SCRIPT FILE NAMED: QUOTE ANNAKOURNIKOVA.JPG.VBS UNQUOTE. WHEN THE ATTACHED PROGRAM (THE WORM CODE) IS EXECUTED, IT COPIES ITSELF TO THE WINDOWS DIRECTORY. IT THEN ADDS THE FOLLOWING DIGITAL SIGNATURE TO THE REGISTRY KEY: QUOTE HKCU\SOFTWARE\ONTHEFLY\WORM MADE WITH VBSWG 1.50B UNQUOTE. THE

WORM THEN PROCEEDS TO SEND ITSELF OUT TO ALL ADDRESSES FOUND IN THE MICROSOFT OUTLOOK APPLICATION.

THE ANTI-VIRUS SOFTWARE INDUSTRY IS AWARE OF THIS WORM AND HAS CREATED A SIGNATURE FILE TO DETECT AND REMOVE IT. FULL DESCRIPTIONS AND REMOVAL INSTRUCTIONS CAN BE FOUND AT VARIOUS ANTI-VIRUS SOFTWARE FIRMS WEB SITES, INCLUDING THE FOLLOWING:

HTTP://WWW.SYMANTEC.COM

HTTP://WWW.VIL.NAI.COM (MCAFEE)

HTTP://WWW.ANTIVIRUS.COM (TREND MICRO)

HTTP://WWW.FSECURE.COM

HTTP://WWW.SOPHOS.COM

AS ALWAYS, USERS ARE ADVISED TO KEEP THEIR ANTI-VIRUS SOFTWARE CURRENT BY CHECKING THEIR VENDOR'S WEB SITES FREQUENTLY FOR NEW UPDATES, AND TO CHECK FOR ALERTS DISSEMINATED BY NIPC, CERT/CC, AND ~~OTHER~~ COGNIZANT ORGANIZATIONS.

PLEASE REPORT ANY ILLEGAL OR MALICIOUS ACTIVITIES TO YOUR LOCAL FBI OFFICE OR THE NIPC, AND TO YOUR MILITARY OR CIVILIAN COMPUTER INCIDENT RESPONSE GROUP, AS APPROPRIATE. INCIDENTS MAY BE REPORTED ONLINE AT WWW.NIPC.GOV/INCIDENT/CIRR.HTM.

BT

#0001

NNNN

End of Data
02/12/01 Lis[redacted]ummary Response [redacted]NI050MK
22:25:43
Type X, x, or / to view Full Response, then press Enter.

. Name: [redacted] b3
M/R : M Case ID: [redacted] Serial: b7E
Race: X Sex: X DOB/Event: ID Info:
Misc: [redacted] Entry Date: 10/25/2000 Class Level: ~~SN~~

. Name: [redacted]
M/R : R Case ID: [redacted] Serial: [redacted]
Race: X Sex: X DOB/Event: ID Info:
Misc: Entry Date: 06/29/1999 Class Level: ~~SN~~

Command . . > ..... +
F1=Help F3=Exit F4=Prompt F12=Cancel

Routing Slip
FD-4 (Rev. 8-8-89)

Date 2/12/01

b6
b7C

TO: ☐ Director
Att.:

☐ SAC
☐ ASAC
☐ Supv.
☐ Agent
☐ OSM
☐ Rotor
☐ Steno
☐ Typist
☐ M
Room

FILE #

Title

RE:

☐ Acknowledge
☐ Assign ☐ Reassign
☐ Bring file
☐ Call me
☐ Correct
☐ Deadline
☐ Delinquent
☐ Discontinue
☐ Expedite
☐ File

☐ For Information
☐ Handle
☐ Initial & return
☐ Leads need attention
☐ Mark for indexing
☐ Open case
☐ Prepare lead cards
☐ Prepare tickler
☐ Recharge file ☐ serial
☐
☐ Send to

☐ Return assignment card
☐ Return file ☐ serial
☐
☐ Return with action taken
☐ Return with explanation
☐ Search and return
☐ See me
☐ Type

* on the internet.

SAC DUANE

See reverse side

Office

*U.S. Government Printing Office: 2000 — 461-077/31702

New Virus: Now Anna Loves You

by Michelle Delio

1:00 p.m. Feb. 12, 2001 PST

A new worm is making its way through e-mail boxes, and it seems to be spreading more rapidly than last year's Love Bug, which infected 15 million computers and is regarded as the worst e-mail virus ever.

The new e-mail worm, known as "Onthefly" and "Anna Kournikova," sends itself in an e-mail with the subject "Here you have, ;o)" -- and carries a message that reads, "Hi: Check This!"

The e-mail contains a Visual Basic scripted attachment that is titled "Anna Kournikova."

TECHNOLOGY

Sponsored by Brightpod

Today's Headlines
3:20 p.m. Feb. 12, 2001 PST

New Virus: Now Anna Loves You

Human Mutations: Blame Men

Human Genome Showdown

Researchers Cut Gene Estimate

DNA Junkyard Yielding Gold

Gene Map: Help or Hype?

Soot to Blame for Global Warming?

Keeping Up With the

See also:
Infected? Here's What to Do
New Love: A Whole Lot of Nothing?
'Love Bug' Virus Running Amok
Now *That* Was a Nasty Worm
Follow the trail of the Love Bug

Kournikova is an international tennis star -- and she's also one of the most downloaded celebrities on the Internet.

"She's a very good looking woman. Every guy in the world is going to click on that attachment," said Andrew Antipass, a systems administrator at Tekserve, a security firm.

The worm doesn't seem to be doing any harm to infected computers. In other words, it's a lot like Kournikova at a Grand Slam tournament: She arrives with great fanfare, attracts lots of attention, then does nothing.

But because of the anticipated huge numbers of e-mails being generated by the virus, the only danger appears to be the possibility that it will overload and crash e-mail servers.

E-Joneses

News Flash: Floppies Are Not Dead

You Can't Hide Your Lying Eyes

Follow Your E-Mail Everywhere

Implant Achieves Female Orgasm

Emphysema's Breath of Fresh Air?

The Greatest Hacks of All Time

The Internet: It's Full of Holes

Projects With Power to Burn

When the attachment is clicked, the worm sends itself via e-mail to all addresses found in a user's Outlook address book. The virus also uses encryption to hide itself, to make it harder for antiviral software to detect it.

"Early propagation reports indicate that this virus is spreading faster than many of the biggest viruses we saw last year," said Mikko Hypponen of F-Secure.

Network Associates antiviral firm McAfee currently ranks the risk from this worm as high, and lists as worm-warning signs the "Presence of the file "c:WINDOWSAnnaKournikova.jpg.vbs" on a user's hard drive.

The company also wryly notes that a deluge of complaints about virus-sending e-mails from people whose names are in your Outlook address book would be another good tip-off that you are infected.

McAfee said that it has had protection for this worm since last August, and said that its users who had updated their software would be protected. F-secure's products also protect against the worm.

The virus activates itself on Jan. 26, 2002, when it opens up the Web page of a Dutch computer shop, which apparently has no connection with the worm.

The encryption used by the worm's writer has made it difficult to detect what, if any, damage the worm is intended to do to infected machines. Some experts said that the link to a Danish website is puzzling.

"Normally you would expect a worm that reaches out to a website to be attempting to download code from that site. Virus writers have used this technique in the past to bolster their viruses damage in the past," Antipass said .

"But that doesn't appear to be the case here. I suspect its an odd attempt at crashing the Danish website when all these computers are supposed to attempt to connect to it next January."

Security firm MessageLabs is warning that it

has already seen more than 3,000 copies of the virus in the last four hours.

Alex Shipp from MessageLabs said that the company "saw the first copy at 13:30(GMT) and now, just four hours later, we've seen more than 2,900 copies come in. We are still analyzing the code - some virus software picks it up - most doesn't."

The worm appears to be a variant of Love Bug, which was capable of damaging the contents of computer hard drives. Outlook users should not open the e-mail, but should select it by holding down the shift key and the press delete to permanently remove the e-mail(s) from your system.

Microsoft advises Outlook users to download and install the Outlook security patch for Office 2000 or a Office 98.

"The patch will effectively protect Outlook users from the Anna Kournikova e-mail worm and others like it," said Alton Kwok, Microsoft program manager.

Antipass said that the real danger will probably come in the next two weeks, as worm writers reengineer the code, altering it to make it more vicious.

"Keep an eye out for a blitz of wormy mail over the next few weeks," antipass said. "But don't get hysterical. As always, if you don't click on any attachments, you won't have any problems. If people would learn to think before they click, these problems would cease to exist."

Have a comment on this article? Send it.
Printing? Use this version.
E-mail this to a friend.

Related Wired Links:

EBay E-mail Makes Users 'Bidder'
Jan. 9, 2001

Critics Blast MS Security
May. 16, 2000

Their Email *Does* Love You
May. 9, 2000

Hey Spyder: Love You, Too

May. 5, 2000

How The Slimy Worm Works
May. 4, 2000

Who Caught the Bug First?
May. 4, 2000

Techies: Victims of 'Love'
May. 4, 2000

This 'Virus' Is an Apparition
Apr. 10, 2000

[redacted]

b6
b7C
b7E

From: [redacted]
To:

Sent: Tuesday, February 13, 2001 4:07 PM
Attach: [redacted]
Subject: Our experience yesterday

We sent an email to the NC Alert lists that include NC agencies, community colleges, libraries, K12, universites, local/county governments, etc on our list. Not all are yet on the distribution. But I'd estimate about 200 are at this time. Our alert went out 32 minutes after the DOD announced their problem occurred. Given the time to investigate and make preliminary calls, I'd say we were hit approximately at the same time.

Here's a good article from the UK that tells how the virus was created:

This story was printed from ZDNet UK,
located at http://www.zdnet.co.uk/news/

Virus Alert: How the Anna virus was created

By Robert Vamosi
Tue, 13 Feb 2001 09:10:09 GMT
URL: http://www.zdnet.co.uk/news/2001/6/ns-20923.html

6/7/01
TJ

She was made from a toolkit

Whoever wrote the Anna virus didn't have to work very hard.

Every day there are hundreds of new viruses that fail to infect another user, often because of programming bugs. According to Trend Micro, Anna's
author avoided all that heartbreak and simply used an existing virus toolkit available on the Internet. VBS Worm Generator (VBSWG) 1.50b is a standalone application that allows script kiddies, (malicious users with very little programming skills), to create their own successful viruses.

The US National Infrastructure Protection Center (NIPC) states that VBSWG
1.50b is a tool that originated in Buenos Aires, Argentina. It creates VBS worms that infect Windows systems with Microsoft VB5 runtimes or Windows Scripting Host 5.0. This includes users of Windows 95 SE, 98, and
98 SE.

FOR INFO OF THE FILE
[redacted] TJ

b3
b6
b7C
b7E

[redacted] 3/01

According to Susan Orbuch, director of Communications for Trend Micro, the firm has seen about half a dozen other viruses created from this same
toolkit. She said the author of the Anna virus is probably a Dutch script
kiddie who goes by the name "OnTheFly". If the day is 26 January, the Anna virus will attempt to connect to a Dutch computer Web site called Dynabyte.

The toolkit, however, takes some of the fun out of writing one's own virus. Using the pop-up interface, anyone with malicious intent can type in a name, an author, and an attachment. One can also specify how the virus is to spread, either by email attachments sent via Outlook or via a
direct connection to mIRC or Pirch.

The toolkit also allows a script kiddie to specify up to four payloads (in other words, what the virus/worm will do on an infected computer). These payloads may launch immediately with activation of the virus, or they may lie dormant until a specificed "trigger date".

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/20/2001

To: Charlotte **Attn:** SSA [redacted]

From: Charlotte
Squad 7, Raleigh Resident Agency
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] jm

b3
b6
b7C
b7E

Case ID #: [redacted] (Pending)
(Pending)
(Pending)
(Pending)
(Pending)
(Pending)
(Pending)

Title: [redacted]
Effect of PENTTBOMB Investigation

Synopsis: Due to the investigative efforts expended on the PENTTBOMB investigation (Major Case 182) and associated International Terrorist matter, no investigation has been conducted concerning the above listed cases since 09/11/01.

Details: Following the September 11, 2001 terrorist attack on the United States, SA [redacted] has been assigned to addressing Leads and Rapid Start matters associated with the PENTTBOMB investigation (Major Case 182). Considerable effort has been spent concerning the investigation of [redacted] Additionally, an International Terrorist matter developed as a spinoff of PENTTBOMB consumed significant resources in the Raleigh RA to include significant time spent by SA [redacted] addressing this matter.

b6
b7C

As a result of the aforementioned investigative efforts, no investigation has been conducted concerning the above listed cases since 09/11/01.

[redacted]

b3
b7E

To: Charlotte Fr[redacted]: Charlotte
Re: [redacted] 11/20/2001

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHARLOTTE

AT CHARLOTTE, NC

Read and clear.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/21/2002

To: Charlotte **Attn:** SSA [redacted]

From: Charlotte
Squad 7, Raleigh Resident Agency
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] jm

Case ID #: [redacted] (Pending)
Pending)
Pending)
Pending)
Pending)
Pending)
Pending)

b3
b6
b7C
b7E

Title: [redacted]
Effect of PENTTBOMB Investigation

Synopsis: Due to the investigative efforts expended on the PENTTBOMB investigation (Major Case 182) and associated International Terrorist matter, minimal or no investigation has been conducted concerning the above listed cases since 09/11/01.

Details: Following the September 11, 2001 terrorist attack on the United States, SA [redacted] has been assigned to addressing Leads and Rapid Start matters associated with the PENTTBOMB investigation (Major Case 182). Considerable effort has been spent concerning the investigation of [redacted] SA [redacted] led a team of SA's whose focus was on [redacted] and his possible association with terrorists to include those involved in the September 11, 2001 terrorist attacks on the United States. On December 13, 2001, [redacted] submitted to a polygraph examination which indicated [redacted]

b6
b7C
b7E

As a result of the aforementioned investigative efforts, minimal or no investigation has been conducted concerning the above listed cases since 09/11/01.
♦♦

FILE

b3
b7E

[redacted]

Ø53TJMØ1.EC

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/19/2002

To: Charlotte **Attn:** SSA [redacted]
Squad 7

From: Charlotte
Squad 7, Raleigh RA
Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted] tjm TJM

Case ID #: [redacted] (Pending)

Title: UNSUB(S);
STATE OF NORTH CAROLINA - VICTIM;
ANNA KOURNIKOVA VIRUS, VBS/SST VIRUS - FEBRUARY 2000;
[redacted]
OO: CE

(X) TJM

Synopsis: Request above captioned matter be reassigned to TFA [redacted]

b6
b7C

Details: Per previous discussion with SSA [redacted] it is requested this matter be transferred to TFA [redacted]

♦♦

Case reassigned 3/24/03

Reassign TFA [redacted] DHG

b6
b7C

[redacted]

b3
b7E

353 TJM 03. EC

FD 801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/09/2003

To: Cyber **Attn:** Computer Investigations Unit, Room 11887 Computer Investigations and Infrastructure Threat Assessment Center (CID/NSD)

From: Charlotte

Approved By: [redacted]

Drafted By: [redacted] tjm

b3
b6
b7C
b7E

Case ID #: [redacted] (Pending)

Title: UNSUB(S);
STATE OF NORTH CAROLINA - VICTIM;
ANNA KOURNIKOVA VIRUS, VBS/SST VIRUS - FEBRUARY 2000;
[redacted]
OO: CE

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED: 02/12/2001

CASE CLOSED:

- ☐ No action due to the state/local prosecution (Name/Number)
- ☐ USA Declination
- ☐ Referred to Another Federal Agency (Name/Number)
- ☐ Placed in unaddressed work
- ☐ Closed administratively
- ☐ Conviction

COORDINATION: FBI Field Office:
Government Agency:
Private Corporation:

VICTIM

Company Name/Government Agency:
State of North Carolina
Address/location: Office of Information Technology

[redacted]

b3
b7E

254TJM02.801

To: Cyber From: Charlotte
Re: [redacted] 09/09/2003

b3
b7E

P.O. Box 17209
Raleigh, NC 27619

Purpose of System: Various Department's Networks
Highest classification of information stored in system:
Unclassified

System Data:
Hardware/configuration (CPU): Desktops
Operating System: Various
Software: Various

Security Features:
Security Software Installed: X yes Virus/firewall
X no (Some systems)
Logon Warning Banner: X yes X no

INTRUSION INFORMATION

Access for intrusion: X Internet connection ☐ Dial-up number
☐ LAN(insider)
If Internet: Internet Address:
Network Name:

Method:
Technique(s) used in intrusion

Path of intrusion:
addresses: 1. Internet 2. Victim
country: 1. Unknown 2. US
facility: 1. Unknown 2. State of NC systems (various)

Subject:
Age:
Sex:
Alias(es):
Race:
Education:
Motive: Virus widespread on Internet
Group Affiliation:
Employer:
Known Accomplices:
Equipment Used: Unk
Hardware/configuration (CPU): Unk
Operating System: Unk
Software: Unk

Impact:
Compromise of classified information: ☐ yes X no

b3
b7E

Estimated number of computers affected: multiple

Estimated dollar loss to date: Unk

Category of Crime:

Impairment:
- ☐ Malicious code inserted
- X Denial of Service
- X Destruction of information /software
- ☐ Modification of information /software

Theft of Information:
- ☐ Classified information compromised
- ☐ Unclassified information compromised
- ☐ Passwords obtained
- ☐ Computer processing time obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

Intrusion:
- ☐ Unauthorized access
- ☐ Exceeding authorized access

REMARKS

♦♦

Menu
Technology(s) Used:

Top Screen *Secondary Screen*

Protocol Attacks:

- ☐ IP
  - ☐ spoofing attack
    - ☐ source routing
- ☐ TCP
  - ☐ sequence number attack
- ☐ UDP
  - ☐ spoofing attack
  - ☐ flooding
- ☐ FTP
  - ☐ vulnerable version
  - ☐ SITE EXEC
  - ☐ overload FTP buffer
  - ☐ anonymous FTP
- ☐ Telnet
  - ☐ highjacking
  - ☐ packet sniffing
- ☐ TFTP
- ☐ r commands
  - ☐ rsh
  - ☐ rlogin
- ☐ SMTP
  - ☐ vulnerable version
    - ☐ spoofing
    - ☐ embedded postscript attack
    - ☐ trojan horse attack
    - ☐ syslog attack
    - ☐ flooding
    - ☐ MIME
- ☐ HTTP
  - ☐ flooding
  - ☐ Telnet to HTTP port
- ☐ gopher
- ☐ X11 window
- ☐ DNS
  - ☐ vulnerable version
  - ☐ flooding
- ☐ SNMP
- ☐ FSP
- ☐ NFS

Other Attacks:

To: Cyber From: Charlotte
Re: [redacted] 09/09/2003

b3
b7E

- ☐ Worm
- ☐ Social engineering
- ☐ Scavenging and reusing
- ☐ Masquerading
- ☐ Scanning
- ☐ Trojan Horse
- X Other - Virus

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2006

To: Charlotte **Attn:** [redacted]

From: Charlotte
Raleigh Resident Agency
Contact: TFA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted] 0116

Drafted By: [redacted] sja

Case ID #: [redacted] (Pending)
(Pending)
(Pending)
(Pending)

Title: Resignation of Task Force Agent

Synopsis: Due to the resignation of Task Force Agent [redacted] [redacted] the above captioned cases should be closed.

b6
b7C
b7E

Reference: [redacted]

Details: Due to the resignation of Task Force Agent [redacted] [redacted] this Electronic Communication will summarize the status of the above captioned cases. Task Force Agent [redacted] will be working as a Special Agent for the Defense Criminal Investigative Service, Southeast Field Office, Ft. Lauderdale Resident Agency and can be contacted at [redacted] after June 1, 2006.

b6
b7C

[redacted]

This investigation involved the infection by the Anna Kournikova virus of the State of North Carolina computer systems. All leads have been exhausted in this investigation and it is recommended that the case be closed administratively.

b3
b7E

[redacted]

b6
b7C
b7E

Close #4 0116

Case closed 6/5/2006

[redacted]

b3
b7E

1435JA01.EC

To: Charlotte From: Charlotte
Re: [redacted] 05/23/2006

b3
b7E

[redacted]

b6
b7C
b7E

♦♦