

The SAGATUG

INTERFACE

Volume 23 Number 8

August, 2002

The San Gabriel Valley Technology User's Group. The Club for TRSDOS and MS-DOS

Two New Viruses Found Last Week

According to the Symantec Corporation, one of the foremost virus protection software manufacturers, two new viruses were discovered last Friday, August 2. One is called "W32.Assarm@mm" and the other is named "Backdoor.Winshell",

The W32.Assarm@mm worm-type virus is a mass-mailing worm that sends messages in reply to all unread messages in the Microsoft Outlook Mailbox. The email messages are not sent if the day of the week is Monday or Thursday and the hour of the time of day is greater than 5. For example, if the time is 4:00 A.M. or 4:00 P.M., the message will be sent; if the time is 6:00 A.M. or 6:00 P.M., it will not be sent. The subject of the email message is "Re: <original message subject line>." The attachment varies.

a mass-mailing worm that sends messages in reply to all unread messages in the Microsoft Outlook Mailbox. The email messages are not sent if the day of the week is Monday or Thursday and the hour of the time of day is greater than 5. For ex-

ample, if the time is 4:00 A.M. or 4:00 P.M., the message will be sent; if the time is 6:00 A.M. or 6:00 P.M., it will not be sent. The subject of the

Continued on page 2

FBI: Threat to Websites and ISP's

August 05, 2002

Editor's Note: The following is reprinted from the FBI cybercrime agency, NIPC website, www.nipc.gov

"Heightened Awareness Warranted on August 5-6, 2002 By U.S. Website and ISP Administrators"

On the afternoon of August 05, 2002, the National Infrastructure Protection Center received credible, but nonspecific information that wide-scale hacker attacks against U.S. websites and Internet Service Providers (ISP) are being planned for later tonight, possibly emanating from Western Europe.

The purpose of this alert is to recommend that website and ISP administrators heighten their awareness of network traffic during this period and encourage them to report suspected malicious activities to their local FBI office <http://www.fbi.gov/contact/fo/fo.htm> or the NIPC and to other appropriate authorities. Recipients may report incidents online at <http://www.nipc.gov/incident/cirr.htm>, and can reach the NIPC Watch and Warning Unit at (202) 323-3205, (888) 585-9078, or nipc.watch@fbi.gov.

The NIPC intends to update this alert should it receive additional relevant information, including information provided to it by the user community.



Memory Jogger...

See you at the next SAGATUG meeting this Friday, August 9, 2002 from 7 to 10 p.m. at the Arcadia Park Senior Citizen's Center, 405 S. Santa Anita Ave. (See page four for directions and more upcoming events.)

email message is "Re: <original message subject line>." The attachment varies.

Type: Worm

Infection Length: 69,632 bytes

Systems Affected: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me

Systems Not Affected: Macintosh, Unix, Linux

The threat assessment of this worm is low to medium.

Damage

- Payload Trigger: Monday or Thursday after the hour of 5
- Payload: Displays a Message Box that will also hang the machine on Monday or Thursday after the hour of 5
- Large scale e-mailing: Replies to all unread messages in the Outlook Mailbox using MAPI

Distribution

Subject of email: Re: [Original Message Subject]

Name of attachment: "opinion.exe", or "images.exe", or "card.exe", or "click.exe", or "Game.exe", or "news_doc.exe", or "data.exe", or "click.exe", "Card.EXE", "bill.exe", "mp3.exe", "docs.exe", "humor.exe", "Flash.exe", "fun.exe", or "demo.exe", or one of 11 filenames containing Korean text.

Size of attachment: 69,632 bytes

As stated above, the worm sends messages in reply to all unread messages in the Microsoft Outlook Mailbox. The email messages are not sent if the day of the week is Monday or Thursday and the hour of the time of day is greater than 5.

Subject: Re: <original message subject line>

Message:

<infected computer's user name> wrote:

====

-<first line of original message>

-<second line of original message>

.

.-<(n-1)th line of original message>

-<nth line of original message>

followed by:

<infected computers user's email address>

followed by two lines of Korean text; then:

<infected computers user's email address>

followed by a line of Korean Text.

Attachment: The attachment is one of the following:

- Opinion.exe
- Images.exe
- Card.exe
- Click.exe
- Game.exe
- News_doc.exe
- Data.exe
- Click.exe
- Card.exe
- Bill.exe
- Mp3.exe
- Docs.exe
- Humor.exe
- Flash.exe
- Fun.exe
- Demo.exe

Backdoor.Winshell is the other virus found last is the other virus found last week. This one is a Trojan Horse virus, so called because it neither replicates or copies itself, but does damage or compromises the security of the computer. Typically it relies on someone emailing it to you, it does not email itself, it may arrive in the form of a joke

program or software of some sort.

Backdoor.WinShell is a server program that allows unauthorized access to the infected computer.

(Continued on page 3)

(Continued from page 2)

New Viruses

Protection can be achieved against both of these viruses with the use of two good programs, Intelligent Updater and Live Update.

Virus definitions from **Intelligent Updater™** virus definitions have undergone full quality assurance testing by Symantec Security Response. They are posted on U.S. business days (Monday through Friday). They must be downloaded from the Symantec Security Response Web site and installed manually.

Users that benefit most from downloading and installing the Intelligent Updater™ virus definitions daily are corporate network administrators, as well as end-users that practice potentially risky Internet behavior (eg., clicking on email attachments from unknown senders or attachments included in unexpected emails, downloading files from newsgroups or suspicious Web sites, etc).

LiveUpdate™ is the easiest way to obtain virus definitions and product updates. These virus defi-

nitions have undergone full quality assurance testing by Symantec Security Response and are posted to the LiveUpdate™ servers one time each week (usually Wednesdays) unless there is a major virus outbreak. There are three stages in the LiveUpdate™ process:

LiveUpdate™ downloads a list of available updates, matches them to the programs that you have installed, determines if any updates apply to those programs, and presents you with a list of updates that are available for you to apply.

- **NOTE:** If you are using Automatic LiveUpdate™, and have it set to the default settings, it will download virus definitions (only) without prompting when they are available.
- It downloads the updates that you select.
- After downloading the update files, LiveUpdate™ automatically installs the virus definitions and updates.

The overall threat from this virus is considered to be low, according Semantec.

Part of Front Page 2002 Article Was Garbled Last Month

The Front Page 2002 article in the *Interface* In column one, page two in the July issue was a little garbled as a result of converting the text to two columns. Reprinted in the next column is the listing of the table of data provided by the website counter the way it should read. I also reprinted the text before that so you can see the context.

You may think that a counter is there solely for the ego of the Webmaster - not necessarily. It does quite a bit more than just count. It tells me if anyone is actually USING the site for one thing.

The other is that it actually keeps track of "stats" from the visitors. What kind of stats? It tells me the following info for EACH visitor: the date and time they visited the site; what browser they used; what operating system they used; their IP address; and where they were referred from. The following is the info I get when someone finds and

accesses our site from the APCUG.org (Association of Personal Computer User Groups) user group locator tool:

Date/Time

06 May 2002 / 10:22:43 AM

Hostname IP

205.160.160.14

OS

OS Icon

Browser

Browser Icon

Referrer: <http://cdb.apcug.org/rdrem.asp?EID=3181&ML=0>

**Next SAGATUG Meeting
Time and Place:**

7 to 10 p.m., Friday, August 9, 2002
**Arcadia Park Senior Citizen's Center, 405 South
 Santa Anita Avenue, Arcadia.**
(In the park just south of Huntington Drive)
Meetings are on the second Friday of every month

Club Officers and Board Members:

President	Art Molz, art1sam@juno.com
Vice President	Royal Brown
Treasurer	Bob Day, trebor543yad@earthlink.net
INTERFACE Editor	Bob Allen, boballen99@earthlink.net
Past President	Art Heywood, heywoodm@worldnet.att.net
Members at Large	Roy T. Beck, roybeck@ix.netcom.com
Webmaster, SAGATUG.org	John Calhoun, johnpc@sagatug.org

Upcoming Events:

Manhattan Beach, last Saturday, monthly,
TRW Swap Meet, Admission Free.

Santa Ana, last Sunday of each odd month,
ACP, 1310 E. Edinger, Admission Free.

Pomona Swap Meet 3rd Saturday, monthly, at Cal
Poly Pomona, 3801 W. Temple Ave., Admission Free

Pomona Fairplex, August 17 & 18, 2002 (Sat.,
Sun.) Bldgs. 6 & 7 at LA Fair grounds, Gate 14, Ad-
mission \$7, plus parking.

Burbank, August 31 & September 1, 2002 (Sat. &
Sun.), Hilton Burbank Airport & Convention Center,
2500 Hollywood Way, Burbank, CA 91505. 10 a.m.
to 5 p.m. \$5 admission

Costa Mesa, October 19 & 20, 2002 (Sat. & Sun.),
Orange County Fair and Exposition Center, 88 Fair
Drive, Costa Mesa, CA 92626, 10:00 a.m. to 5:00p.m.,
\$5 admission

Santa Monica, November 30 & December 1, 2002,
Santa Monica Civic Auditorium, 1855 Main Street,
Santa Monica, CA 90401

IN THIS ISSUE:

Two New Viruses Found Last Week..... 1
 FBI: Threat to Websites and ISP's 1
 Memory Jogger 1
 Part of Front Page 2002 Article Garbled 3
 Upcoming Events..... 4

Deadline for the Newsletter

The deadline for the INTERFACE is the last Sat-
urday of the month.

Republication:

Articles may be republished if credit is given to
the author and the San Gabriel Valley Technology
User's Group.

**Please visit the new SAGATUG website
at www.sagatug.org There you will
find photos of the meeting site maps to
the meeting, articles from other sources
and an archive of the *SAGATUG Inter-
face*.**

SAN GABRIEL VALLEY TECHNOLOGY USER'S GROUP
PO Box 661213
Arcadia, California 91066-1213

FIRST CLASS