

# The SAGATUG

# INTERFACE

Volume 23 Number 12

December, 2000

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

## Warning: New E-mail Worm's Surfaces

By John Calhoun.

A new, destructive email worm type virus called "W32.N\*vid\*d. According to the folks at Symantec, W32.N\*vid\*d is a mass mailing worm program.

However, the name of the worm does not actually have asterices in its name. To get past some brain-dead corporate email filters that can't differentiate between a discussion of a worm and the presence of an actual worm, I'm going to have to use a simple letter-substitution code in discussing this item: In the next paragraphs, when you see "\*" replace it with an "a."

The worm replies to all Inbox messages that contain a single attachment. This type of worm virus is called a Messaging Application Program Interface (MAPI) because it is able to distribute itself via any MAPI compliant email client, including Microsoft Outlook.

However, emails that are infected with this worm can be received by any email client. The worm utilizes the existing email subject line and body and attaches itself as N\*VID\*D.EXE. Due to the bugs in the code, after being executed, the worm causes your system to be unusable.

You can tell if you've been infected by using Regedit to search for this key: HKEY\_USERS\DEFAULT\Software\N\*vid\*d. **If you have that key, you've been infected.**

If the worm software works the way its creators intended, it also installs a blue eye icon in the system tray of your taskbar. If you place your mouse

pointer over the eye, a "tool tip" appears, stating:

Lo est\*mos mir\*ndo...

It does more, depending on what your actions are. The worm's damage can be repaired manually, although it's a pain; the better antivirus sites tell you how. (See link below, for example.)

The holidays are a fertile time for hackers and crackers: Keep your anti-virus definitions up to date, and be careful with any attachments you get with your e-mail.

For more info on this particular worm, visit the information pages of your anti-virus vendor, or check out

[http://www.symantec.com/avcenter/venc/data/w32.n\\*vid\\*d.html](http://www.symantec.com/avcenter/venc/data/w32.n*vid*d.html)

(but remember to change each astertisk to an "a" in the above url)

According to the FBI's National Infrastructure Protection Center (NIPC), the cyber crime investigative unit, has been tracking the Internet worm (W32N\*vid\*d@M) and currently assesses that it represents a low threat in the United States. Although there have been media reports of outbreaks of this worm in South Korea and Australia, NIPC's international counterparts have reported no significant outbreaks. Although Navidad does not contain a dangerous payload, it does modify the Windows registry file. The modification makes it impossible to execute most programs with an .exe attachment unless they were already running at the time of infection.

(Continued on page 2)

# Technical View of the Corporate Mind

By Anonymous

Here is a look into the corporate mind that is very interesting, educational, historical, completely true, and hysterical all at the same time:

The US standard railroad gauge (width between the two rails) is 4 feet, 8.5 inches. That's an exceedingly odd number. Why was that gauge used? Because that's the way they built them in England, and the US railroads were built by English expatriates.

Why did the English build them like that? Because the first rail lines were built by the same people who built the pre-railroad tramways, and that's the gauge they used.

Why did "they" use that gauge then? Because the people who built the tramways used the same jigs and tools that they used for building wagons which used that wheel spacing.

*(Continued from page 1)*

## **New "worm" virus**

"For every message found with an attachment, it constructs a separate email message using the identical subject line and body of the message and then forwards the binary .exe code to all the recipients (To and CC) of the found messages. In doing so, it swaps the .exe binary for the original attachment emailed to the user. Additional technical information for this worm will be made available in Cybernotes 23 posted on the NIPC's website on November 23, 2000, at <http://www.nipc.gov/cybernotes/cybernotes.htm>

Full descriptions and removal instructions are available at various anti-virus software firms' web sites, including the following:  
<http://www.symantec.com>    <http://www.nai.com>  
<http://www.trend.com>    <http://fsecure.com>  
<http://www.sophos.com>

As always, users are advised to keep their anti-virus software current by checking their vendors' web sites frequently and to stay apprised of warnings from NIPC, and other organizations.

The FBI asked everyone to please report any illegal or malicious activities to your local FBI office, or the NIPC, and to your law enforcement.

Okay! Why did the wagons have that particular odd wheel spacing? Well, if they tried to use any other spacing, the wagon wheels would break on some of the old, long distance roads in England, because that's the spacing of the wheel ruts.

So who built those old rutted roads? The first long distance roads in Europe (and England) were built by Imperial Rome for their legions.

The roads have been used ever since. And the ruts in the roads? Roman war chariots first formed the initial ruts, which everyone else had to match for fear of destroying their wagon wheels. Since the chariots were made for (or by) Imperial Rome, they were all alike in the matter of wheel spacing.

The United States standard railroad gauge of 4 feet, 8.5 inches derives from the original specification for an Imperial Roman war chariot. Specifications and bureaucracies live forever.

So the next time you are handed a specification and wonder what horse's butt came up with it, you may be exactly right, because the Imperial Roman war chariots were made just wide enough to accommodate the back ends of two war horses.

Thus, we have the answer to the original question.

Now the twist to the story. There's an interesting extension to the story about railroad gauges and horses' behinds.

When we see a Space Shuttle sitting on its launch pad, there are two big booster rockets attached to the sides of the main fuel tank. These are solid fuel rocket boosters, or SRBs. The SRBs are made by Thiokol at their factory in Utah.

The engineers who designed the SRBs might have preferred to make them a bit fatter, but the SRBs had to be shipped by train from the factory to the launch site. The railroad line from the factory had to run through a tunnel in the mountains. The SRBs had to fit through that tunnel. The tunnel is slightly wider than the railroad track, and the railroad track is about as wide as two horses' behinds.

So, the major design feature of what is arguably the world's most advanced transportation system was determined over two thousand years ago by the width of a Horse's Ass!

# Some Amusing Tech Support Stories

*This item reprinted with permission from The LangaList (a free email newsletter available at <http://www.langa.com/newsletter.htm>), Copyright (c) 2000 Langa Consulting*

Reader Paul Williams sends along these tech support stories, which are only funny if you're neither the caller nor the support technician.

Tech Support: "OK Bob, let's press the control and escape keys at the same time. That brings up a task list in the middle of the screen. Now type the letter 'P' to bring up the Program Manager."

Customer: "I don't have a 'P'."

Tech Support: "On your keyboard, Bob."

Customer: "What do you mean?"

Tech Support: "'P' on your keyboard, Bob."

Customer: "I'm not going to do that!"  
~~~~~  
Overheard in a computer shop:  
Customer: "I'd like a mouse mat, please."

Salesperson: "Certainly sir, we've got a large variety."

Customer: "But will they be compatible with my computer?"

~~~~~  
I once received a fax with a note on the bottom to fax the document back to the sender when I was finished with it, because he needed to keep it.

~~~~~  
Customer: "Can you copy the Internet for me on this diskette?"

~~~~~  
I work for a local ISP. Frequently we receive phone calls that go something like this: "Hi. Is this the Internet?"

~~~~~  
Some people pay for their online services with checks made payable to "The Internet."  
Customer: "So that'll get me connected to the Internet, right?"

Tech Support: "Yeah."

Customer: "And that's the latest version of the Internet, right?"

Tech Support: "Uhh...uh...uh...yeah."

~~~~~  
Tech Support: "All right...now double-click on the File Manager icon."

Customer: "That's why I hate this Windows - because of the icons --I'm a Protestant, and I don't believe in icons."

Tech Support: "Well, that's just an industry term sir. I don't believe it was meant to ..."

Customer: "I don't care about any 'Industry Terms'. I don't believe in icons."

Tech Support: "Well, ...why don't you click on the 'little picture' of a file cabinet...is 'little picture' OK?"

Customer: [click]

~~~~~  
Customer: "My computer crashed!"

Tech Support: "It crashed?"

Customer: "Yeah, it won't let me play my game."

Tech Support: "All right, hit Control-Alt-Delete to reboot."

Customer: "No, it didn't crash -- it crashed."

Tech Support: "Huh?"

Customer: "I crashed my game. That's what I said before. I crashed my spaceship and now it doesn't work."

Tech Support: "Click on 'File,' then 'New Game.'"

Customer: [pause] "Wow! How'd you learn how to do that?"

## SAGATUG Meeting

### Time and Place:

**7 to 10 p.m., Friday, December 8, 2000**  
**Arcadia Park Senior Citizen's Center**  
**405 South Santa Anita Avenue, Arcadia.**  
**(In the park just south of Huntington Drive)**  
**Meetings held second Friday every month**

### Upcoming Events:

#### TRW Swap Meet

Last Saturday, monthly, Manhattan Beach

#### Pomona Fairplex, December 30 & 31

(Bldgs. 6 & 7 LA Fair grounds, Gate 14) -  
Admission \$7 plus parking

#### Buena Park, December 16 & 17

at the Sequoia Conference Center, 7530  
Orangethorpe, (Beach Blvd exit from 91 Freeway)  
\$3 admission

**Reseda, December 9 & 10** at the Sherman Square  
Entertainment Center, 18430 Sherman Way.  
Admission \$3.

#### Glendora Seniors Computer Club

La Fetra Senior Citizens Center, 333 E. Foothill  
Blvd., Glendora, 2nd & 4th Wednesdays at 1 p.m.

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

### Club Officers and Board Members:

|                  |                                         |
|------------------|-----------------------------------------|
| President        | Royall Brown                            |
| Treasurer        | Bob Day, daybob@earthlink.net           |
| INTERFACE Editor | Bob Allen, boballen99@earthlink.net     |
| Past President   | Art Heywood, heywood@starquest.net      |
| Members at Large | Roy T. Beck, roybeck@ix.netcom.com      |
| Disk Librarian   | John Phillip, jphillip@pop.primenet.com |

### IN THIS ISSUE:

**Warning: New E-mail Worm' Surfaces..... 1**  
**Technical View of the Corporate Mind ..... 2**  
**Some Amusing Tech Support Stories ..... 3**

#### Deadline For The Newsletter

The deadline for the INTERFACE is the last Saturday of the month.

#### Republication:

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

**FIRST CLASS MAIL**