TEK THOTS

Electronic Newsletter

```
+-+-+-+ +-+-+-+-+-+
|T|e|k| |T|h|o|t|s|
+-+-+-+ +-+-+-+-+-+
```

TEK THOTS
Volume 4, Number 2
February 24, 1999
Published irregularly by Scott C. Holstad

```
=============================================================
```
Copyright Notice
Copyright (C) 1999 Scott C. Holstad
All enclosed material may be used for non-commercial purposes.
```
=============================================================
```

```
*************************************************************************
```
DISCLAIMER The views and analysis expressed in Tek Thots are the author's own, and do not
in any way reflect the views of EarthLink Network, Inc., the author's employer.
```
*************************************************************************
```

CONTENTS

-- News/Editorial
-- PC Thots
-- Web Development Thots
-- This Issue's Software-O-Rama
-- Stock Thots
-- Newbie Thots
-- Game Thots
-- Privacy/Security Thots

```
=============================================================
```

News/Editorial
----

*   Welcome to another issue of Tek Thots. Thanks to all of you expressing concern re my
health. I'm feeling largely better now. I appreciate all the email. I am really hoping
to get more issues out this year. One of the things I'm interested in is in allowing this
to become a forum for you - the reader. You'll note a couple of thots from readers in
this issue. If you know of a rumor, have a rant, are onto something hot, let me know, and
maybe I'll print it.

*   I do this once a year, so now's the time. I don't know how many of you are interested
in these things, but it always interests me: the domains of our readers. So, without
further ado, here are where you folks are coming from, in order from recent greatest to
least: com, net, edu, Canada, Germany, the US, the UK, org, the US Military, Australia,
Sweden, Japan, Israel, US Government, Mexico, Denmark, France, Ireland, Malaysia,
Netherlands, Belgium, Italy, Switzerland, Norway, UAE, New Zealand, Finland, Spain,
Latvia, Thailand, Greece, Croatia, Brazil, Chile, Singapore, Russia, Austria, Bermuda,
ARPAnet, India, Iceland, Nicaragua, Czech Republic, Argentina, Romania, Slovak Republic,
and Poland. There, now. Wasn't that tantalizing?

*   Man, how quickly things change. Yahoo bought Geocities. Mindspring bought Netcom (who
would have thought as recently as 1997!!!). The RBOCs are buying up each other and ISPs.
Consolidation, my friends, is the key word. Soon there will be fierce competition between
several very large companies in many of these technology industries.

* My buddy, Kent Filmore (kentf@earthlink.net), sent us this tidbit.

        Who ever might have said the entrepreneurial spirit is a thing
of the past in the computer industry is a short sighted person of
little knowledge. Recently the InternNIC has made public
something which they have seen occurring (probably) daily; domain
name claim staking.
        Without getting into the nuts and bolts of registering a
domain name, the basic principle has been "get the firstest with
the mostest" which has lead to a number of private individuals
ending up with domain names like "www.fordmotors.com" and
"www.cocacola.com". For the most part these are individuals who
register a well known brand name in the hopes of making a profit
by reselling the name to the appropriate company. The InterNIC
has no control (as of this writing) over who claims what name.
        The latest maelstrom in a mug centers on a Canadian high
school student, Abdul Traya, who has claimed the name
"appleimac.com". Naturally Apple claims the name infringes on
their trademark for their popular new Internet computer, the
iMac. It turns out that Apple has forgotten its
"built-in-a-garage" foundations as well as its vast imaginative
resources and pointed its legal department at this enterprising
youth. Good luck Abdul, and remember, 1984 may not be like
"1984", but 1999 will be a year YOU remember!

*   You Usenet and/or O'Reilly fans will appreciate the following site:
http://www.shmooze.net/~cmv/porn.php3

*   My buddy, Dennis Poledna (defragc@hotmail.com) wrote a little ditty for Tek Thots (and
you can too - just send something decent in and I'll look it over):

It does my piratical heart good to see the music industry going through paroxysms over the
MP3 format. So frightened are they by the thought of folks downloading music and then
burning it to CD that the music lobby is actually trying to get the Canadian government to
impose a CDN$2.50 "Royalty Fee" on each blank CDR sold in the Great White North.

This kind of move is only in keeping with the proud tradition of an industry that killed
DAT and that continues to charge US$16.50 for CDs even though the media costs have dropped
below US$1.00.

A number of artists are now going around the industry by distributing their music in MP3

format from their Web sites. Some are free, some try-and-buy. This is the wave of the
future and music industry intransigence has guaranteed that this wave (Or MP3, to be exact.)
will sweep them away.

==

PC Thots
----

*   Intel Links Alleged Pentium Flaw To Software

(Reuters) -
        Intel Corp. said Wednesday an alleged flaw in its new Pentium's
serial number system designed to keep personal computers secure
from interference by "hackers" was related to the chip's software,
not any physical problem with the chip.

        Intel said it is still in talks with the German magazine, Computer Technology,
which Tuesday alleged a flaw in the software Intel provided for turning off the serial
number, to determine what, if anything is wrong with its system.

        Intel provided an "on-off" system in response to privacy concerns
over the issuance of serial numbers which could be used to track
users in cyberspace. The German magazine said it found a way to
thwart that Pentium software and void the "on-off" switch without a user's knowledge.

        "What is at issue here is not a chip flaw. There is no flaw in the Pentium III
processor with respect to the processor serial number," said Intel spokesman Tom Waldrop.
"What is being discussed with the German magazine is a possible software hack."

        Intel has maintained that its new serial numbers are "an important step" toward
combating malicious hackers. At a developer's conference in Palm Springs, Calif. this week
to launch the new Pentium III chips, Intel underscored the importance of creating a secure
environment for Internet commerce, which it said will grow into a $1 trillion business
over the next few years.

        The serial numbers, Waldrop said, will make personal computers
"less hackable" and "more secure and private."

        "All software ultimately is hackable and today's Internet security is essentially
all software and it is all hackable," said Waldrop. "What we are doing today is
introducing into the equation is a processor serial number that brings more of a hardware
element, that's more resilient and less hackable and has more reliability."

        Waldrop said that if the software that controls the serial numbers is found to be
defective, Intel will work on a "patch" or other software fix.

        But he said there have been no allegations of a defect in the chip itself. Five
years ago, when the original Pentium chip was released, a flaw in the way the chip handled
certain math equations led to a recall that cost Intel hundreds of millions of dollars,
but the chip went on to become one of the most successful products in the history of the
high-tech industry.

==

Web Development Thots
----

*   Director 7 Shockwave Internet Studio has just come out (for a measly 1K - ouch!) By all
accounts, while being a decent package, it's bloatware, and you'll definitely need the
dreaded manual (200 pages). The Aftershock application is nifty (well, handy), and there
are many great features - just be prepared for the time suck it'll take you to learn to
use this program.

*   Tetranet Software (http://www.tetranetsoftware.com/) has just released LinkBot Pro 4.0
and it's hot. Does a damn good job, and it's a big improvement over 3.0. One of the cool
things about Tetranet is that if your site isn't big enough for the Pro version, you can
get a freebie "Express" version. Check it out.

==

This Issue's Software-O-Rama
----

*   I found a cute little semi-useless piece of software call Corkboard
(http://www.pcdynamics.com/corkboard/) recently. It's partial screen saver, partial
memo/sticky pad reminder. The cool thing about it is that it has SO many objects that you
can use.

 You can customize it, play with it, have different versions of it. And, it's FREE. So,
if you're interested (and even if you're not), give it a whirl.

==

Stock Thots
----

*   You all know I'm a braggart, but I would like to point out that I said - pre-IPO -
Amazon.com and Yahoo.... I also told some friends of mine Geocities too. The only one
I've been wrong on has been SRS Labs. 3 out of 4 ain't bad.

*   Anyone care to speculate on Ebay...?

==

Newbie Thots

Telnet Fundamentals

        You probably know that the Internet is basically an international collection of
networked computers - networked networks. Well, when you're online, have you ever wanted
to look at the contents of the remote computer to which you are connected? You can't do
this, unfortunately, with every computer out there, but you can make a "remote connection"
to certain computers, logging onto these computers and essentially using them as your own.
The protocol that allows you to do this is called "Telnet."

        Telnet works by allowing you to use a standard Internet connection to send
commands to this distant computer to which you're attempting to connect. What's the
point, you may ask? With telnet, you can access numerous databases, government agency
files, library catalogs, ISPs, bulletin board systems (BBS's), and other information that

is NOT found on the Web. Cool!

        In order to utilize telnet, you need a telnet application (traditionally called a
"terminal emulator"). There are a number of software sites on the Net where you can
obtain such software. Tucows (http://tucows.tierranet.com/) is a great software
repository for PCs and Macs. You can find telnet programs under their "Network Tools"
area. Some PC telnet programs I have had success with include "CRT" and "QVT/Term."
However, my favorite - and the one I've been using for years - is EWAN, and this one's
harder to find. You can obtain it at the following Web site:
http://www.lysator.liu.se/~zander/ewan.html. A nice, comfy Mac telnet program is "NCSA
Telnet."

        After you've procured a telnet application, you'll need to set it up and put it to
work for you. For the purposes of this article, I'll be using EWAN 1.052 for the PC and
NCSA Telnet 2.6 for the Mac.

        Ideally, your terminal emulation program should be set to VT100. (This "video
terminal" setting guarantees the compatibility of your computer screen - otherwise, you
may just see garbage.) EWAN users should choose Configuration under the Operations menu,
click on Emulation, and then select DEC-VT100.

        NCSA Telnet users may also want to set their terminal emulation to VT100. To do
this, go to the Edit menu, select the Preferences option, click on New, and then VT100.

        In order to telnet, you need to know the address of the site you wish to visit.
Typically, this is little more than the domain name (the Internet address) of the site
(such as "earthlink.net"). You may also want to pre-configure the domain names of sites
you intend to visit regularly. Let's use a specific example for the remainder of this
article.

        PC users: When EWAN is opened, a Connect to site screen appears over the main
terminal window. Choose New, then type in a name for the connection in the Name field -
for this article, let's go with Library of Congress. Next, in the Network address of host
name field, type in the actual IP number or host name of the site you wish to visit - in
this case, type locis.loc.gov. Make sure the Telnet option is checked for the Service
(port). (If you choose Custom, you'll typically input the number 23, as this is the
standard telnet port number.) When you're done, click OK. The next time you want to
connect to the remote computer, choose Library of Congress, and your connection should be
established.

        Mac users: Well, it's pretty much the same thing. Using NCSA Telnet, choose
Preferences from the Edit menu, and click on Sessions. Select New, and then input the
connection name you want in the Alias field - again, for our purposes, input Library of
Congress. Next, type locis.loc.gov in the Hostname field. Finally, ensure that the Port
field is 23. That should be it! Now, when you too want to visit the Library of Congress,
simply choose Open Connection from the File menu, and Library of Congress from the
Host/Session Name field.

        Now, let's actually telnet to the Library of Congress. Open your telnet
application and select Library of Congress. When your connection is established, you'll
be greeted with a UNIX-like interface, which gives you a menu and some basic information.
Type in 1 (for the Library of Congress Card Catalog), and press Return/Enter. You'll then
be given catalog choices. Why don't we choose 3: Books catalogued since 1975. Now you
can search by title, author, subject, and more! When you want to leave a telnet session,
you can usually type quit or exit at the prompt and your session will terminate. Here,
however, we need to return to the main menu. Then, typing the number 12 allows us to
exit.

        "Great," you say, "But now that the Web has come along, isn't telnet just another
outdated, useless Internet protocol like gopher?" Well, think about this: the Web has
only been around for a few years, and not everything is available there (yet). You can

still find a LOT of info in text-based databases that haven't yet migrated to the Web.
For instance, if you're interested in seeing the contents are various library card
catalogs, you can explore the holdings of university libraries, such as the University of
Tennessee (telnet opac.lib.utk.edu) or California State University, Long Beach (telnet
coast.csulb.edu), among others - you can't always do that on the Web! Sometimes you would
be surprised at what else you can telnet to - places such as various NASA sites or
weather sites - an endless array of telnetable databases.

        Some ISPs even let you telnet to their site to edit your Web sites directly on
their Web server, saving you the hassle of FTPing new files every time you want to make
one little change, such as a word or date. However, not every site supports this program,
as some ISPs view this as a security risk. Check with your ISP to find out what their
policy is on this issue.

        Simply because some sites won't give you telnet access shouldn't stop you from
enjoying the benefits this application can provide. Telnet is easy to use - in fact, if
you ever need help in a telnet session, you can typically type help or "?" at the prompt
for aid. So, grab a telnet app and try it out. You'll find there are other cool Internet
applications out there and many, many interesting telnet sites.

==

Game Thots
----

*   EA. Their NCAA Football 98 destroyed 3 computers. Don't know why. NCAA Football 99
caused the Blue Screen of Death on two. Don't know why. I wrote them a nasty letter,
alleging they owed me a new PC after the disastrous affairs, claiming their code sucked.
I cc'd all the bigwigs. Would you believe I actually got numerous calls from these
people!!! And they had me ship my PC to them, they fixed it, and installed the games,
which work. THAT, my friends, is customer service. That is a good way of establishing
and maintaining brand and company loyalty. More power to EA!!!

==

Privacy/Security Thots
----

*   With thanks from the Journal of Electronic Defense:

Director of Central Intelligence (DCI) George J. Tenet has, in a series of speeches to
industry and in Congressional testimony, tried to increase awareness of and interest in
threats to the commercial and security aspects of information warfare (IW) threats. "We
are building an information infrastructure - the most complex systems the world has ever
known - on an insecure foundation. Protecting our critical information infrastructure is
an issue that requires attention from us all. Our national security and our economic
wellbeing depend upon it," Tenet said.

"Protecting our critical information systems and the data on them will be key to our
survival as the world's leading economic power and as the world's leader in information
technology," he emphasized. Echoing a point made strongly at the Association of Old Crows
National Convention in Virginia Beach, the DCI noted that national security also relies on
information technology and information systems, since more than 95 percent of all defense
telecommunications travel on commercial circuits and networks.

        "The informationwarfare threat is real and it is growing," Tenet told his
audiences. In testimony before the Senate Select Committee on Intelligence as well as the

Senate Governmental Affairs Committee, the DCI noted that the intelligence community has identified several countries that have governmentsponsored IW programs and several others working to develop them.

Potential attackers include national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers and aggrieved or disloyal insiders. Each of these adversaries is motivated by different objectives and constrained by different levels of resources, technical expertise, access to the target and risk tolerance, but all can conduct cyber attacks and are a threat to our critical infrastructure.

Foreign military writings discuss the importance of disrupting the flow of information in combat; but the battlespace of the future will extend to our domestic information infrastructure, such as electric power grids and telecommunications networks.

The role of the intelligence community is to provide adequate warning of these cyber threats to our nation's security decisionmakers in Washington and at military command posts overseas.

Through existing mechanisms, threat information can be passed to the private sector. Cyber threats are a difficult intelligence target. They are cheap and require little infrastructure; the technology required is dual use, and they are exceptionally easy to conceal. In addition, intrusiondetection technology is still in its infancy. When attacks are detected, the source of the attack is often disguised so they are difficult to trace. "These are enormous challenges," Tenet said, "but the intelligence community is taking them on by focusing analytical and collection resources on this threat."

*   Also, from JED, an interesting tidbit:

BVR Systems (Givatayim, Israel) has developed a fifthgeneration aircombatmaneuveringinstrumentation (ACMI) system. Dubbed the EHUD, the company's latest ACMI system possesses a number of improved capabilities over its previous version. These include enhanced navigation capabilities, a patented multichannel, autoroaming datalink communications system, Windows NT(tm)based software, improved processing power - 3 Pentium processors replace the 486 processor used in the fourthgeneration system - and a minimized Removable DataStorage card. The card, used for trainingflight debriefing, has a greater memory capacity for longer recording time and higherresolution terrain data of flight areas. Also part of the system is the company's unique anticollision warning system based on the Global Positioning System

*   The Secrecy & Government Bulletin has this one:

Pentagon Removes Unclassified Info from the Web

The golden age of public access to government information may have already come and gone, as defense agencies adopt new measures to restrict the online availability of many types of unclassified information in an effort to address the novel challenges posed by the Internet.

Following a new Pentagon policy promulgated in November, military agencies are quietly withdrawing many hundreds of pages of unclassified electronic documents from the world wide web, or placing them under access controls that prevent the general public from viewing them.

As recently as last summer, official Pentagon policy concerning the world wide web still dictated that "Information will be made fully and readily available, consistent with statutory requirements, unless its release is precluded by current and valid security classification."

But the new policy now states that even unclassified information "should not be accessible
to the general public" on the Web unless it is "specifically cleared and marked as
approved for public release."

"This is a wartime information policy," observed John Pike, who has monitored the
disappearance of numerous web pages. "All kinds of program information is being withdrawn.
Almost anything that discloses what an agency actually does, beyond a brief mission
statement, is going away."

The new policy reflects a profound anxiety among defense officials about the power of the
Internet, especially its capacity for aggregation and "data mining," and the potential
vulnerabilities that may create. Deputy Secretary of Defense John J. Hamre warned in a
September 24 memo that "the Web can ... provide our adversaries with a potent instrument
to obtain, correlate and evaluate an unprecedented volume of aggregated information
regarding DoD capabilities, infrastructure, personnel and operational procedures."

Unfortunately, in the exercise of their duties, Pentagon officials have elided the
difference between classified and unclassified information. The new policy seems
predicated on the notion that classified information may be latent in any and all
unclassified information, waiting to be extracted by a clever analyst. This is a
significant expansion of the traditional argument ("mosaic" theory) that compilations of
unclassified information can sometimes be classified.

Bill Leonard, director of security programs for the assistant secretary of defense (C3I),
defended the new policy. "We had a number of instances where people overlooked the first W
in World Wide Web, and posted information that should not have received global
distribution. In no way, shape, or form was there ever any intent to restrict legitimate
public access to government information." However, he told S&GB on January 12, "It's
possible that some individuals down the line have misinterpreted the policy, and have
overreacted to it" by withdrawing more information than necessary from disclosure.

There appears to be a significant discrepancy between DoD's severe new limits on web
publication and the more forthcoming disclosure requirements of the FOIA. In an effort to
recover access to some portion of the suppressed information, FAS has filed several FOIA
requests for copies of selected web pages that have been withdrawn from public access. To
the extent that the requests are successful, the recovered pages will be re-hosted on the
FAS web site.

*   Check out the following URL which Dan Farmer so triumphantly has been passing around:

ACLU wins - top of:

        http://www.aclu.org/features/f101698a.html

Off to celebrate!

dan

*   A worm has been wandering around the Net via Usenet and email: W32/Ska, otherwise known
as Happy99.exe. IF you get this as an email attachment, please do not execute (open) it.
Although this file does not behave like a standard virus, it has some nasty side effects.
A large problem which has been noticed is that after opening the attachment, outgoing
email messages are sent twice with happy99.exe attached to the second message.

How do you know if your computer has been affected? Using the Find command from the Start
menu, search for Files or Folders. Enter "ska" in the first box (labeled "Named"), then
click the Find Now button. If the Find results show any of the following file

s, your computer is infected:

```
ska.exe
ska.dll
liste.ska
wsock32.ska
```

These are the steps that need to be taken to undo the effect of this file.

1) Delete files ska.exe, ska.dll, and wsock32.dll.
2) Rename wsock32.ska to wsock32.dll.
3) After deleting and renaming these files, you should reboot your machine.
4) Delete liste.ska

```
===============================================================
```

SUBSCRIPTION INFO

To Subscribe: Send email to sch@well.com. In the subject line, write "subscribe tek
thots." In the message area, write your email address.

To Unsubscribe: : Send email to sch@well.com. In the subject line, write "unsubscribe
tek thots." In the message area, write your email address.

At this point and until further notice, the email list will be handled manually.

```
===============================================================
```

Online versions of this electronic newsletter will be archived at:
http://www.well.com/user/sch/tekthots.html.

Copyright (C) 1999 Scott C. Holstad
ASCII Tek Thots logo courtesy Teri Osato

Click on [image] to return to Tek Thots.