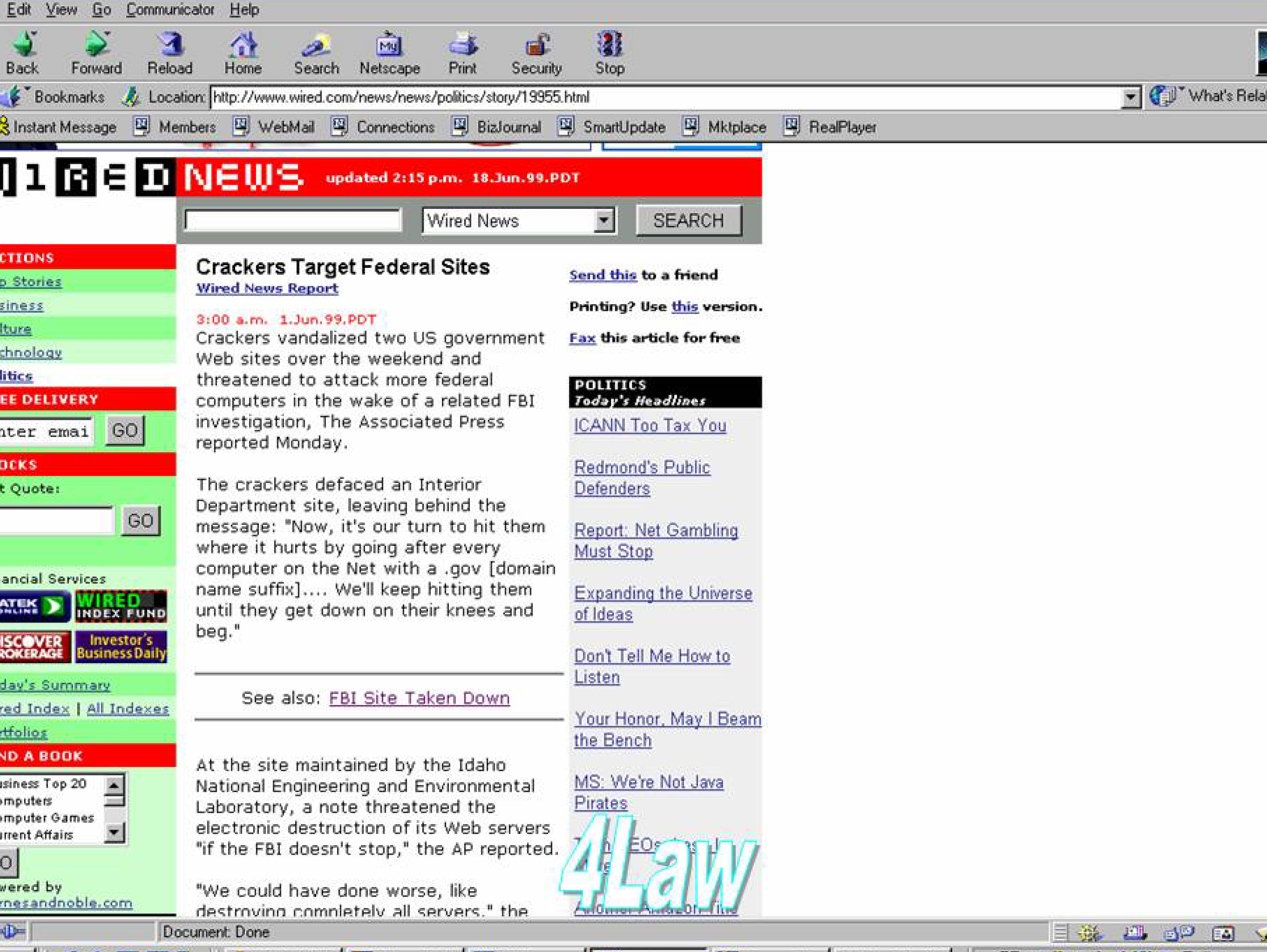
National Infrastructure Protection Center

SSA Scott K. Larson
FBI NIPC
Cyber Emergency
Support Team

UNCLASSIFIED

The Truth Is Out There
Paranormal Activity
Trust No One
Government Denies Knowledge
THE X FILES
The X files

4Law



CTIONS
p Stories
siness
lture
chnology
litics
EE DELIVERY
nter emai GO
OCKS
t Quote:
GO
ancial Services
ATEK ONLINE
WIRED INDEX FUND
ISCOVER ROKERAGE
Investor's Business Daily
day's Summary
red Index | All Indexes
rtfolios
ND A BOOK
usiness Top 20
mputers
mputer Games
urrent Affairs
O
wered by
rnesandnoble.com

Crackers Target Federal Sites

Wired News Report

3:00 a.m. 1.Jun.99.PDT

Crackers vandalized two US government Web sites over the weekend and threatened to attack more federal computers in the wake of a related FBI investigation, The Associated Press reported Monday.

The crackers defaced an Interior Department site, leaving behind the message: "Now, it's our turn to hit them where it hurts by going after every computer on the Net with a .gov [domain name suffix].... We'll keep hitting them until they get down on their knees and beg."

See also: FBI Site Taken Down

At the site maintained by the Idaho National Engineering and Environmental Laboratory, a note threatened the electronic destruction of its Web servers "if the FBI doesn't stop," the AP reported.

"We could have done worse, like destroying completely all servers," the

Send this to a friend

Printing? Use this version.

Fax this article for free

POLITICS
Today's Headlines

ICANN Too Tax You

Redmond's Public Defenders

Report: Net Gambling Must Stop

Expanding the Universe of Ideas

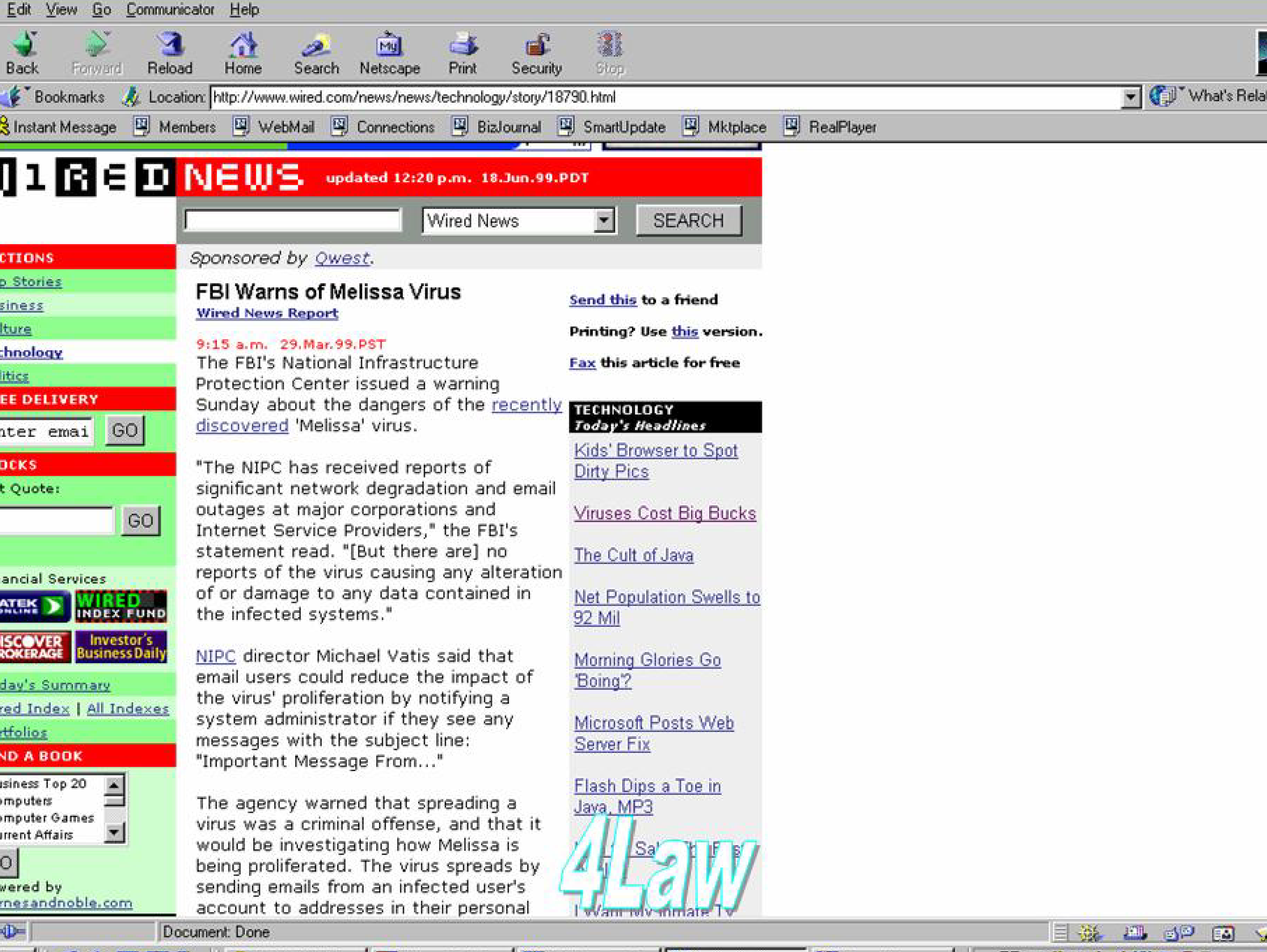
Don't Tell Me How to Listen

Your Honor, May I Beam the Bench

MS: We're Not Java Pirates

[illegible] CEOs [illegible]

[illegible]



Sponsored by Qwest.

FBI Warns of Melissa Virus

Wired News Report

9:15 a.m. 29.Mar.99.PST

The FBI's National Infrastructure Protection Center issued a warning Sunday about the dangers of the recently discovered 'Melissa' virus.

"The NIPC has received reports of significant network degradation and email outages at major corporations and Internet Service Providers," the FBI's statement read. "[But there are] no reports of the virus causing any alteration of or damage to any data contained in the infected systems."

NIPC director Michael Vatis said that email users could reduce the impact of the virus' proliferation by notifying a system administrator if they see any messages with the subject line: "Important Message From..."

The agency warned that spreading a virus was a criminal offense, and that it would be investigating how Melissa is being proliferated. The virus spreads by sending emails from an infected user's account to addresses in their personal

Send this to a friend

Printing? Use this version.

Fax this article for free

TECHNOLOGY
Today's Headlines

Kids' Browser to Spot Dirty Pics

Viruses Cost Big Bucks

The Cult of Java

Net Population Swells to 92 Mil

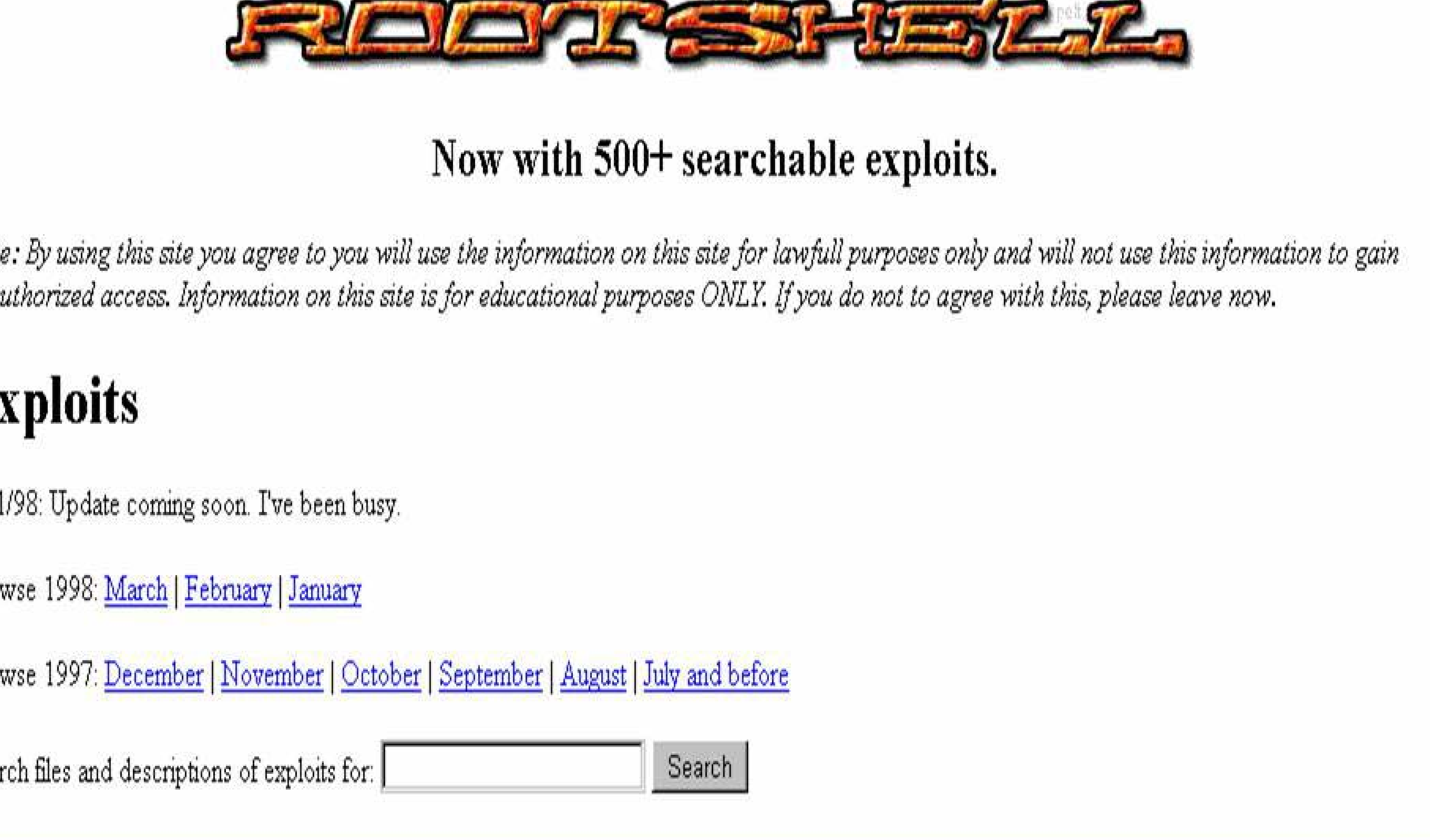
Morning Glories Go 'Boing'?

Microsoft Posts Web Server Fix

Flash Dips a Toe in Java, MP3

[illegible] Sa[illegible]

I Want My Inmate TV



Now with 500+ searchable exploits.

e: By using this site you agree to you will use the information on this site for lawfull purposes only and will not use this information to gain uthorized access. Information on this site is for educational purposes ONLY. If you do not to agree with this, please leave now.

xploits

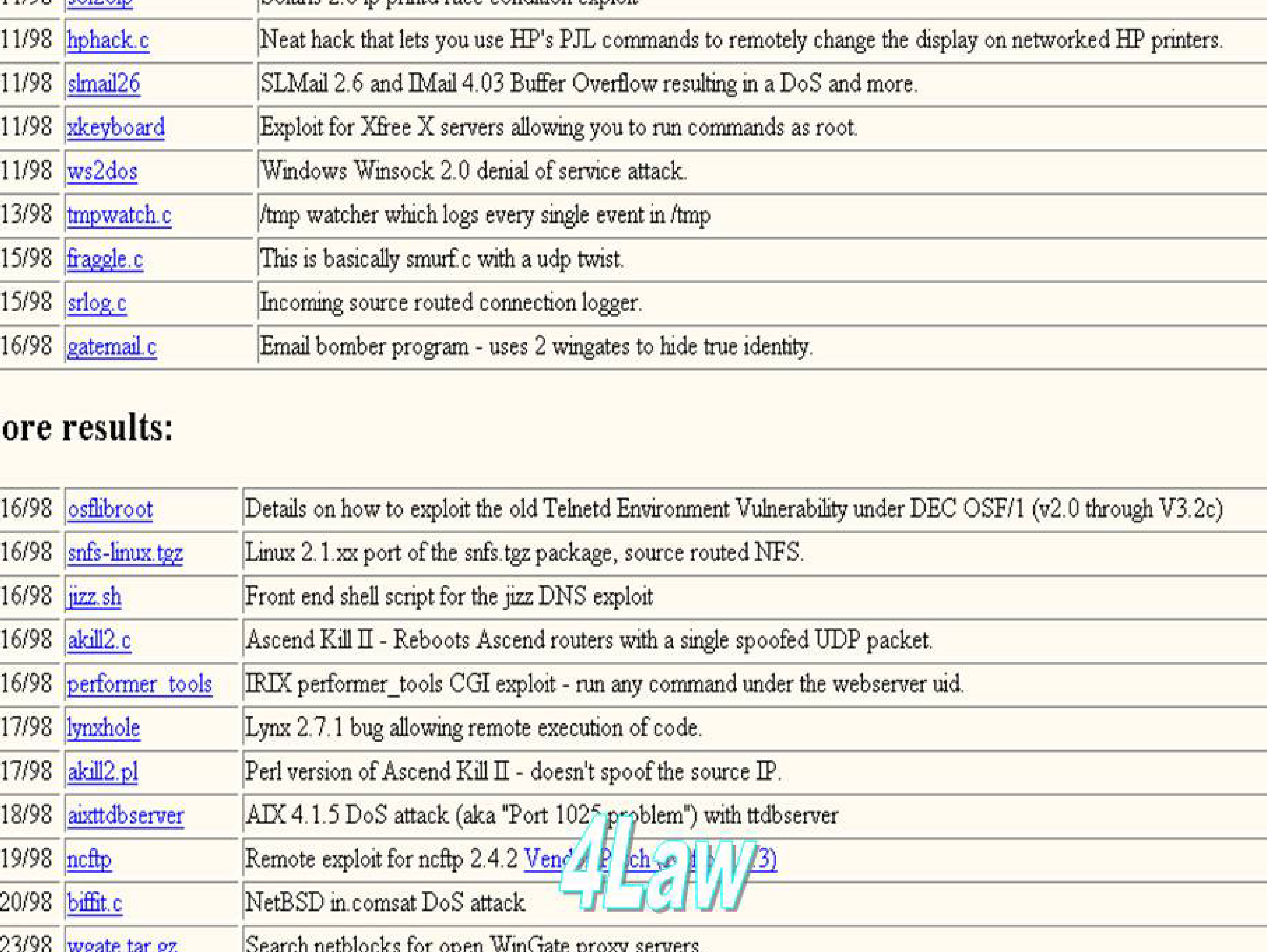
1/98: Update coming soon. I've been busy.

wse 1998: March | February | January

wse 1997: December | November | October | September | August | July and before

rch files and descriptions of exploits for:

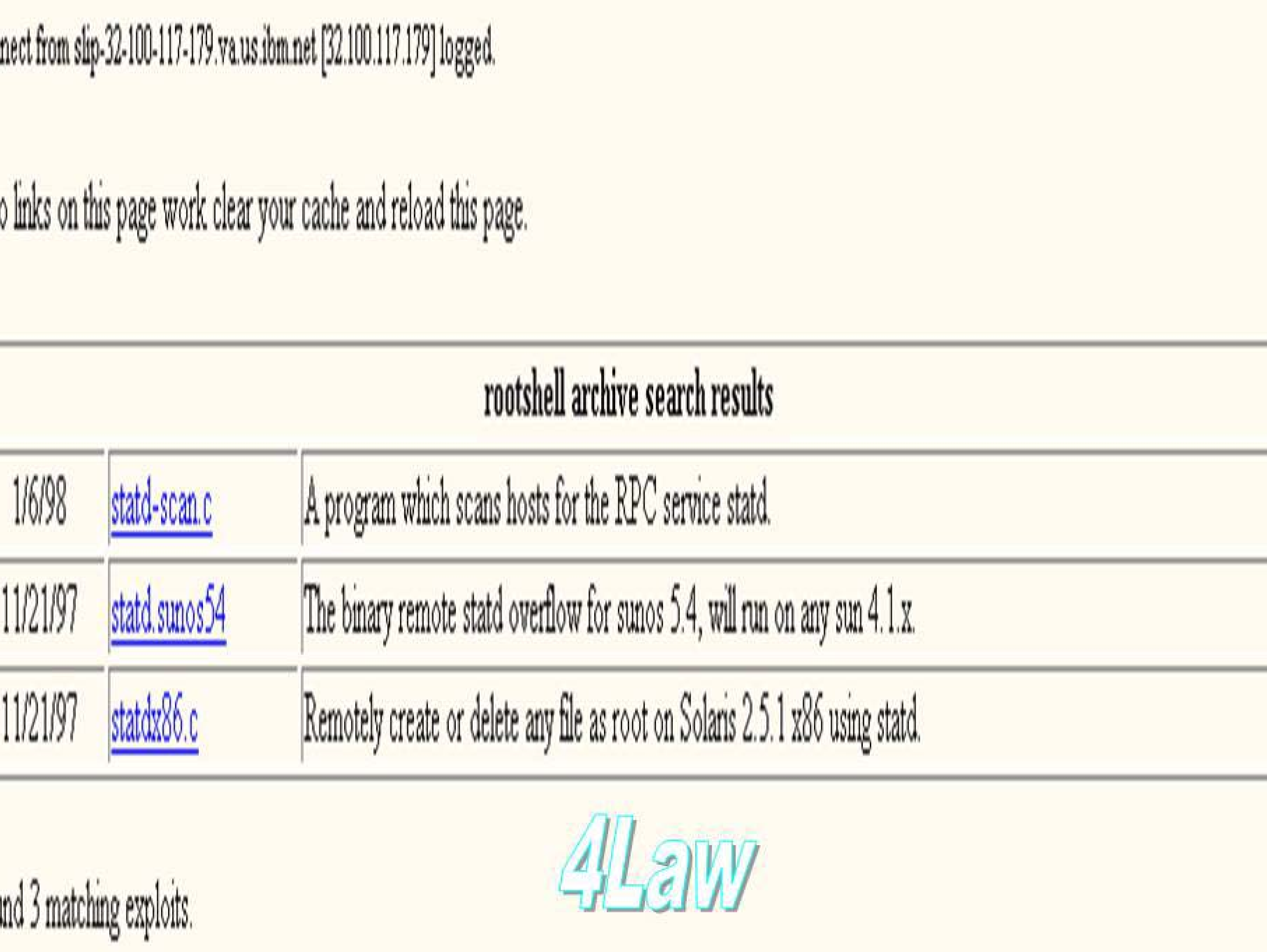
4Law



11/98	sol26lp	Solaris 2.6 lp printd race condition exploit
11/98	hphack.c	Neat hack that lets you use HP's PJL commands to remotely change the display on networked HP printers.
11/98	slmail26	SLMail 2.6 and IMail 4.03 Buffer Overflow resulting in a DoS and more.
11/98	xkeyboard	Exploit for Xfree X servers allowing you to run commands as root.
11/98	ws2dos	Windows Winsock 2.0 denial of service attack.
13/98	tmpwatch.c	/tmp watcher which logs every single event in /tmp
15/98	fraggle.c	This is basically smurf.c with a udp twist.
15/98	srlog.c	Incoming source routed connection logger.
16/98	gatemail.c	Email bomber program - uses 2 wingates to hide true identity.

ore results:

16/98	osflibroot	Details on how to exploit the old Telnetd Environment Vulnerability under DEC OSF/1 (v2.0 through V3.2c)
16/98	snfs-linux.tgz	Linux 2.1.xx port of the snfs.tgz package, source routed NFS.
16/98	jizz.sh	Front end shell script for the jizz DNS exploit
16/98	akill2.c	Ascend Kill II - Reboots Ascend routers with a single spoofed UDP packet.
16/98	performer_tools	IRIX performer_tools CGI exploit - run any command under the webserver uid.
17/98	lynxhole	Lynx 2.7.1 bug allowing remote execution of code.
17/98	akill2.pl	Perl version of Ascend Kill II - doesn't spoof the source IP.
18/98	aixttdbserver	AIX 4.1.5 DoS attack (aka "Port 1025 problem") with ttdbserver
19/98	ncftp	Remote exploit for ncftp 2.4.2 Vend[illegible] P[illegible]ch [illegible] 3)
20/98	biffit.c	NetBSD in.comsat DoS attack.
23/98	wgate.tar.gz	Search netblocks for open WinGate proxy servers.



nect from slip-32-100-117-179.va.us.ibm.net [32.100.117.179] logged.

o links on this page work clear your cache and reload this page.

rootshell archive search results

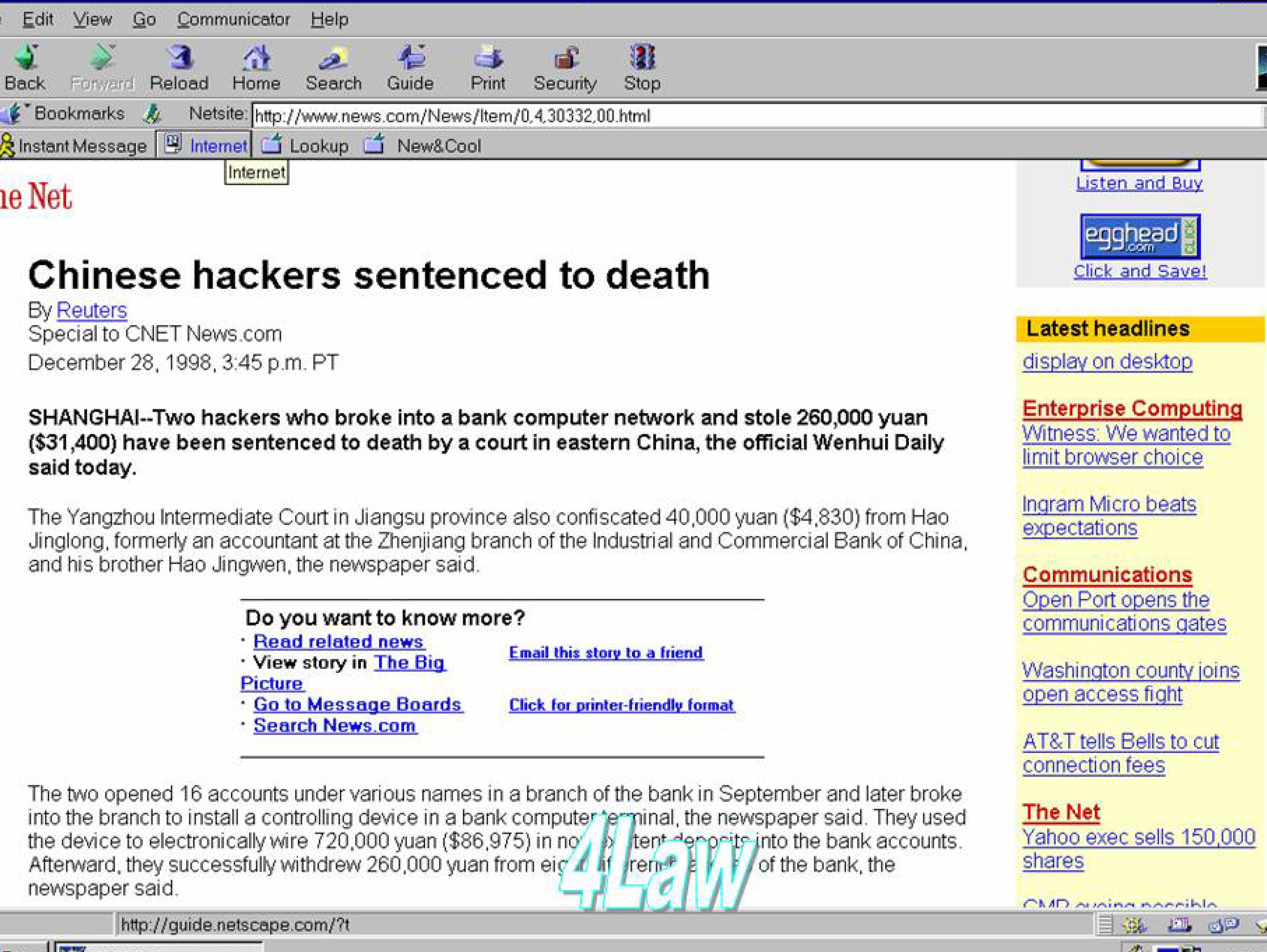
1/6/98	statd-scan.c	A program which scans hosts for the RPC service statd.
11/21/97	statd.sunos54	The binary remote statd overflow for sunos 5.4, will run on any sun 4.1.x.
11/21/97	statdx86.c	Remotely create or delete any file as root on Solaris 2.5.1 x86 using statd.

nd 3 matching exploits.

THREATS

Foreign Intelligence Services: Cuckoo's Egg

- Case involved intrusion into over 200 U.S. Government computers in 1986
- Four West German hackers used a stolen passcode to ride international data networks in order to gain access
- Hackers obtained sensitive but unclassified information which was sold to KGB
- Prosecution in Germany resulted in three convictions



ne Net

Chinese hackers sentenced to death

By Reuters
Special to CNET News.com
December 28, 1998, 3:45 p.m. PT

SHANGHAI--Two hackers who broke into a bank computer network and stole 260,000 yuan ($31,400) have been sentenced to death by a court in eastern China, the official Wenhui Daily said today.

The Yangzhou Intermediate Court in Jiangsu province also confiscated 40,000 yuan ($4,830) from Hao Jinglong, formerly an accountant at the Zhenjiang branch of the Industrial and Commercial Bank of China, and his brother Hao Jingwen, the newspaper said.

Do you want to know more?

- Read related news
- View story in The Big Picture
- Go to Message Boards
- Search News.com

Email this story to a friend

Click for printer-friendly format

The two opened 16 accounts under various names in a branch of the bank in September and later broke into the branch to install a controlling device in a bank computer terminal, the newspaper said. They used the device to electronically wire 720,000 yuan ($86,975) in nonexistent deposits into the bank accounts. Afterward, they successfully withdrew 260,000 yuan from eight different branches of the bank, the newspaper said.

Latest headlines

display on desktop

Enterprise Computing
Witness: We wanted to limit browser choice

Ingram Micro beats expectations

Communications
Open Port opens the communications gates

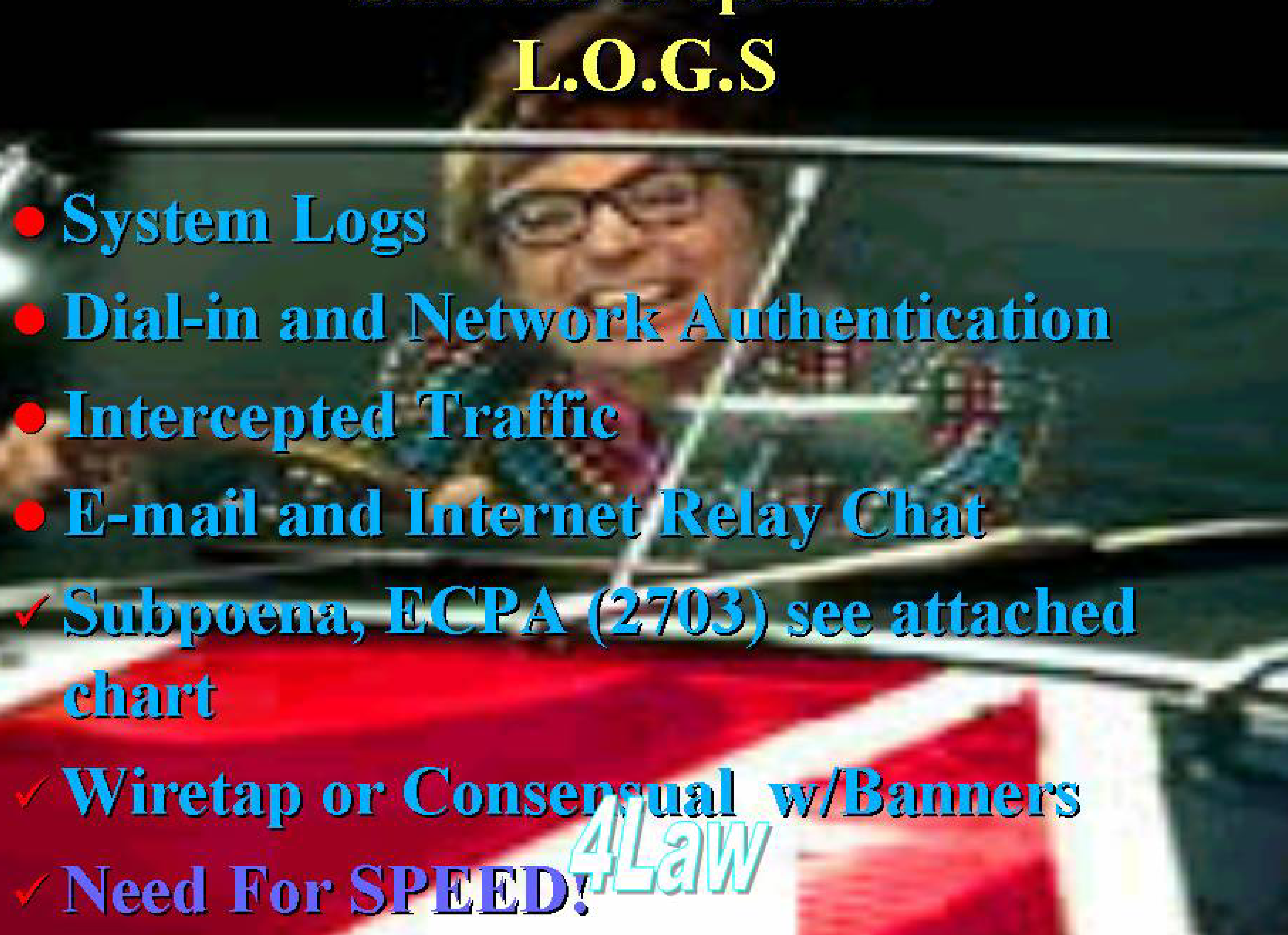
Washington county joins open access fight

AT&T tells Bells to cut connection fees

The Net
Yahoo exec sells 150,000 shares

CMP eyeing possible

Success is spelled:
L.O.G.S



● System Logs

● Dial-in and Network Authentication

● Intercepted Traffic

● E-mail and Internet Relay Chat

✓ Subpoena, ECPA (2703) see attached chart

✓ Wiretap or Consensual w/Banners

✓ Need For SPEED!

Hackers: Solar Sunrise

- Computer intrusions into military computer systems in 1998 during Iraq weapons inspection crisis
- Hackers exploited known vulnerabilities in Sun Solaris Operating Systems
- Some intrusions appeared to be coming from Middle East
- Raised concern that intrusions could be initial stages of information war by hostile nation

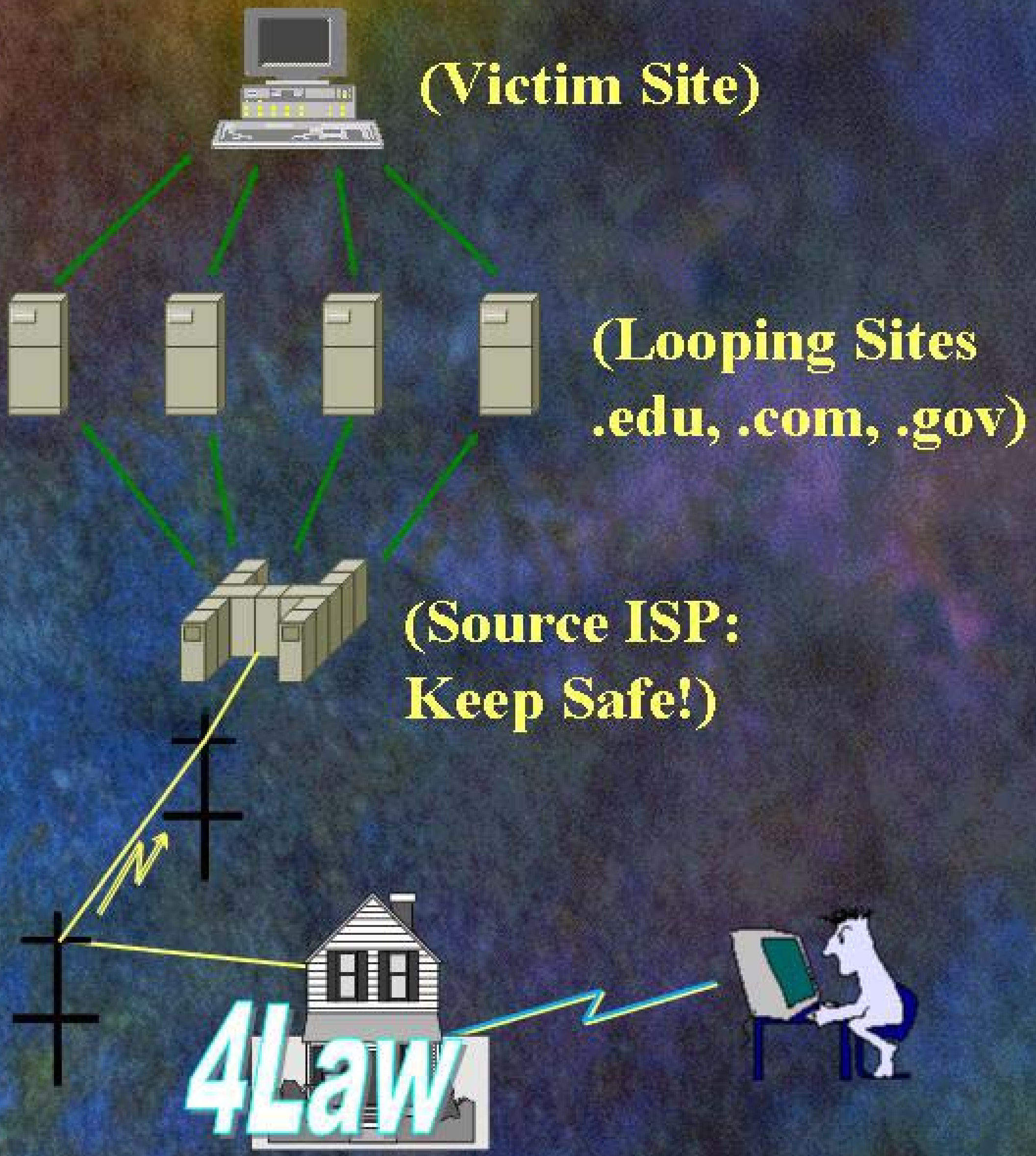
Hackers: Solar Sunrise

- 19 Court Orders in less than ten days
- Title III written, approved by DOJ and sworn to in one day!
- Consensual monitoring done by AFOSI
- Wiretap analysis done at FBI San Francisco by monitoring experts

United States Team Effort

- Federal Bureau of Investigation
- Air Force Office of Special Investigations
- National Aeronautics and Space Administration
- U.S. Department of Justice Computer Crimes Section
- Defense Information Systems Agency
- National Security Agency
- Central Intelligence Agency
- Department of Defense
- Service/Agency CERTs

Investigating the Crime



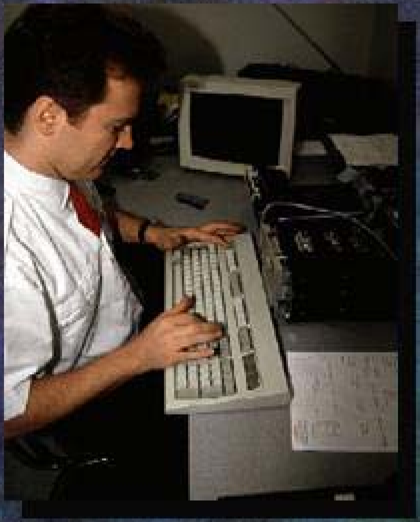
(Victim Site)

(Looping Sites .edu, .com, .gov)

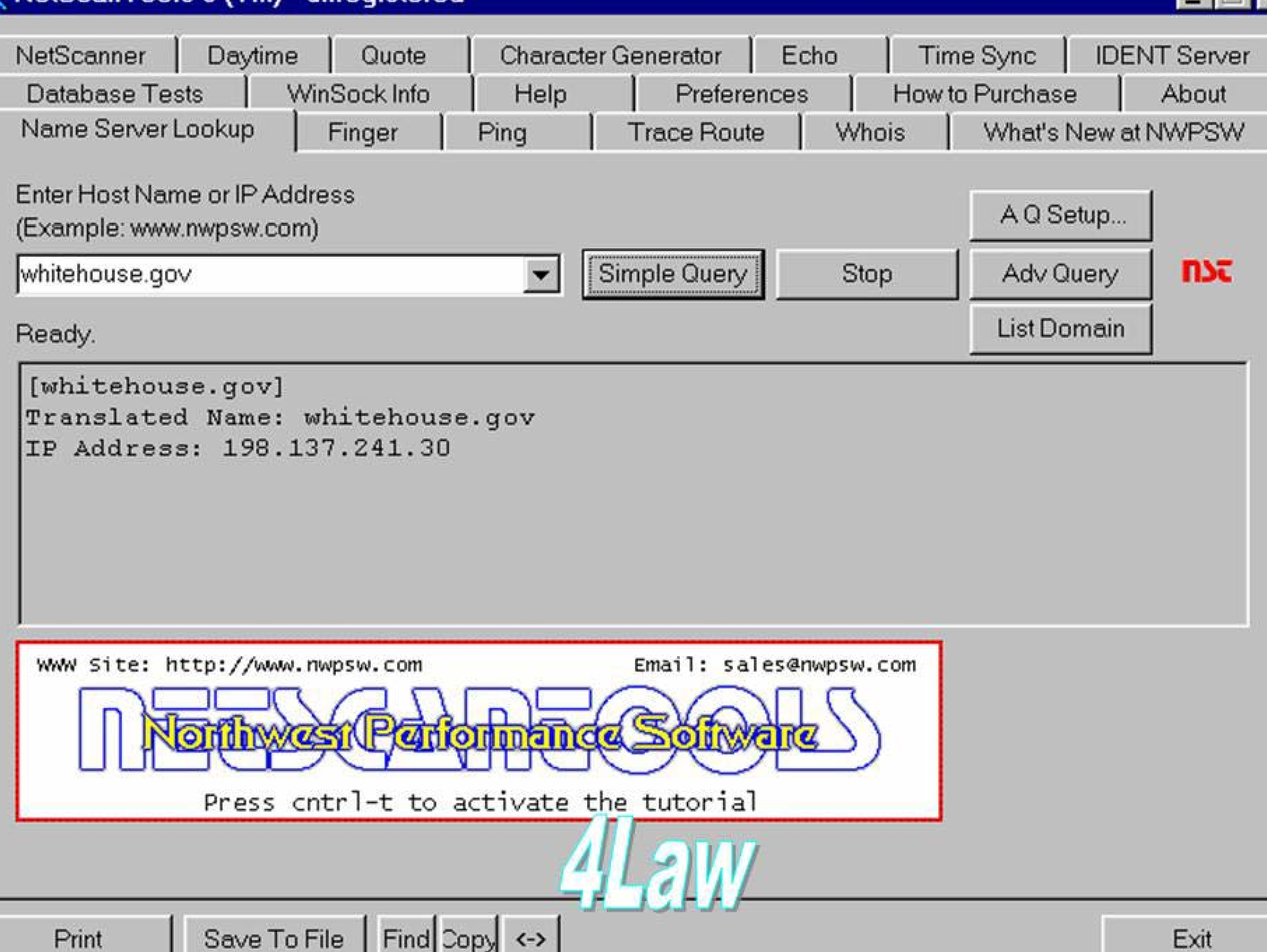
(Source ISP: Keep Safe!)

Pattern and Characteristics of Attack

- Hacker gained entrance to site with tools from a university site (often DNS Server)
- Obtained root access using "statd" vulnerability
- Installed sniffer program to collect user passwords
- Created backdoor to get back into system
- Patched vulnerability by downloading patch from UNC
- Exited system without exploring



4Law



Enter Host Name or IP Address
(Example: www.nwpsw.com)

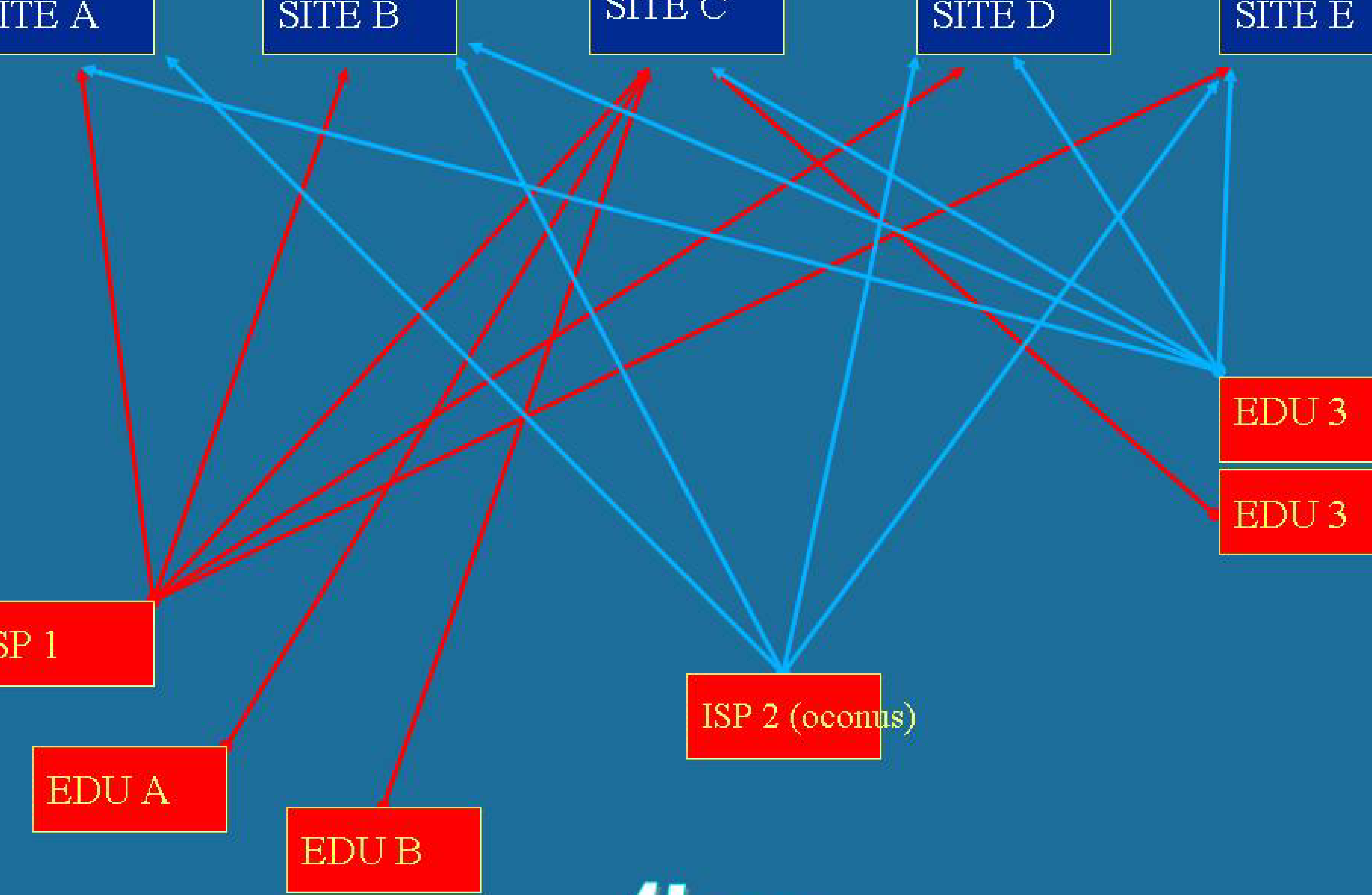
whitehouse.gov

Ready.

```
[whitehouse.gov]
Translated Name: whitehouse.gov
IP Address: 198.137.241.30
```

WWW Site: http://www.nwpsw.com Email: sales@nwpsw.com

Press cntrl-t to activate the tutorial



ITE A

SITE B

SITE C

SITE D

SITE E

EDU 3

EDU 3

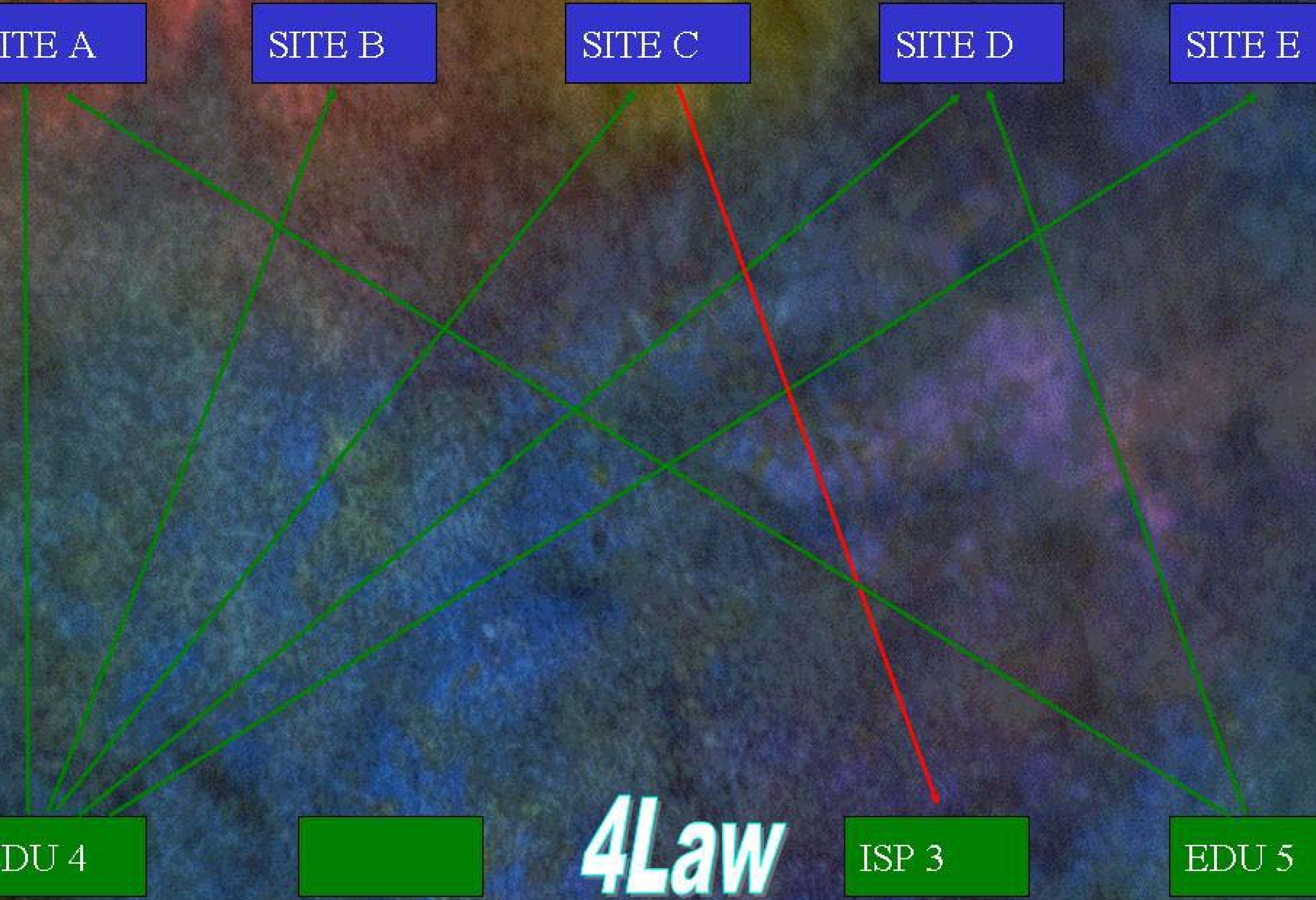
SP 1

ISP 2 (oconus)

EDU A

EDU B

4Law



ITE A

SITE B

SITE C

SITE D

SITE E

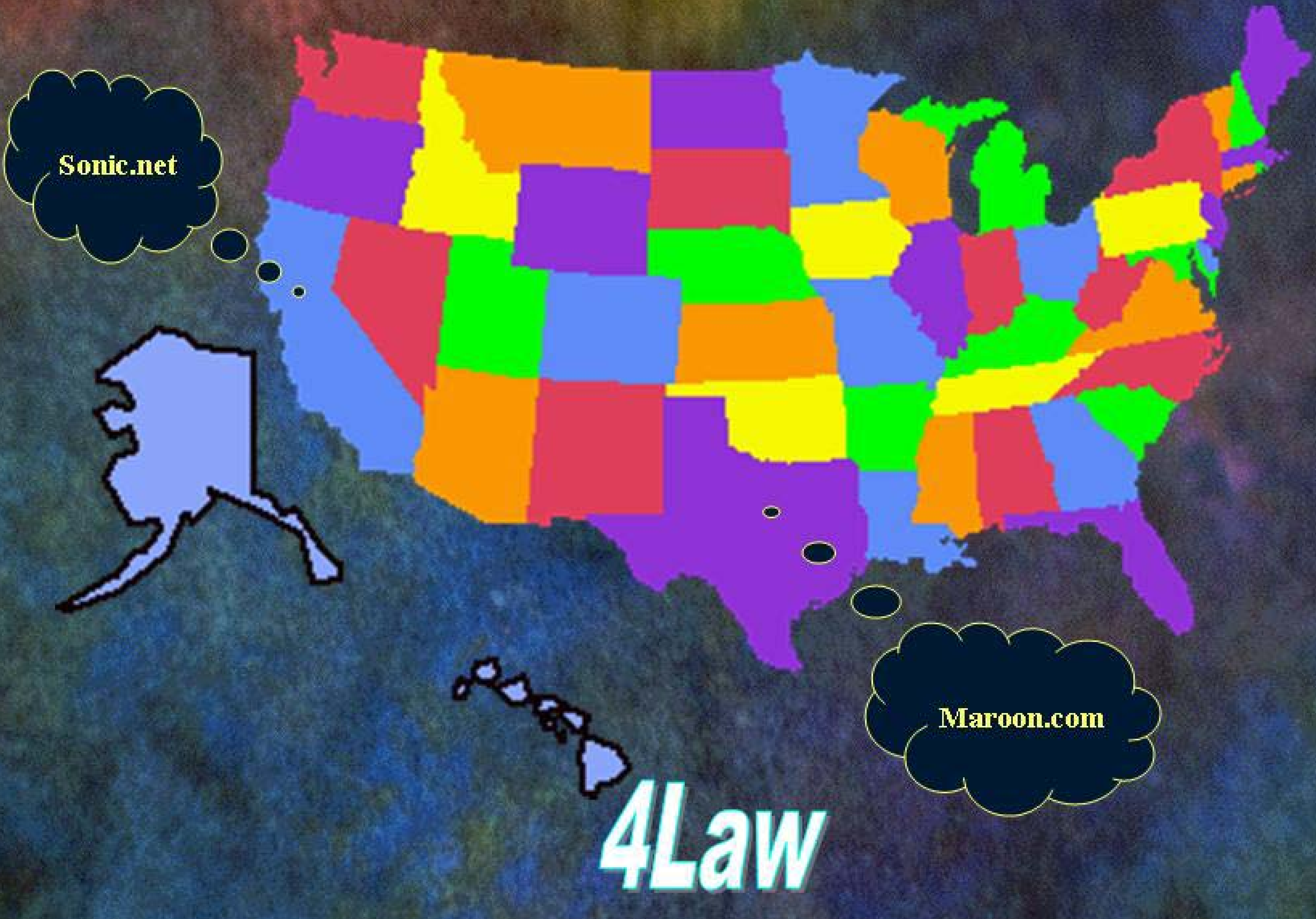
DU 4

ISP 3

EDU 5

4Law

US Source ISPs



Identifying the Subjects

- Interview of System Administrator at SONIC.NET
  - Already knew of two hackers
  - Identified account names as MAK and STIMPY
- Network Trap and Trace identifies user accounts accessing victim sites
- Successful telephone traces of calls to residence of STIMPY
- Pen register on residence confirms access to SONIC.NET originating from STIMPY's residence
- Title III intercept and content review provides sites visited and IRC chat with ANALYZER
- Physical surveillance at MAK's residence identifies occupants of house at time of connection

Identifying the Subjects

- Search warrants executed at residences of MAK and STIMPY
  - Online at time of warrant execution
  - Unaware of press leak
- MAK and STIMPY arrested and interviewed
  - Both admitted relationship with ANALYZER
  - Arrests widely publicized
- Consensual monitoring at MAROON.COM reveals connections and hacking activity originating in Israel
- Trap and trace inconclusive but establishes access via Internet from Israel

Events of the Week

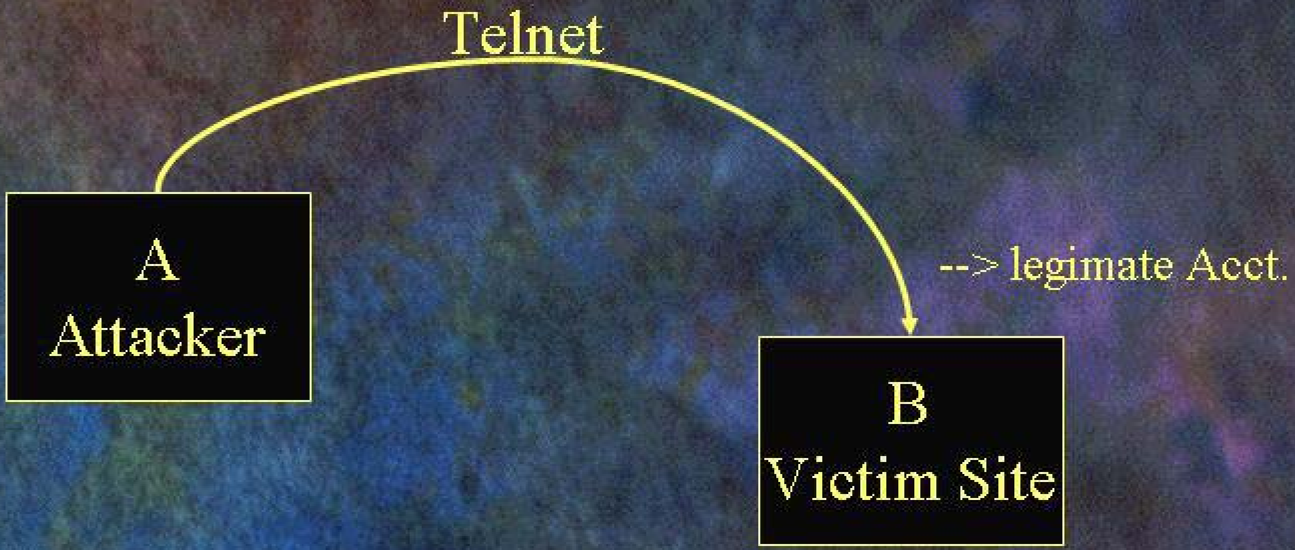
21 Feb - 26 Feb 98

- Analysis of sonic.net captured data
  - Title III & Sys Admin Provided Data
    - 8 Days of Logs
      - 1. FBI 2. Massaged TCP Dumps (letter given to OEO)
    - Stimpy (T-III) & Mak (Sys Admin) Accounts
      - Stimpy (aka too-short) - up to 25 Feb
      - Mak (aka Makeveli) - up to 21 Feb
    - Telnets, FTPs, Probes, & IRC Sessions

Connection Analysis

- Date/Time
- Source IP
- Destination IP
- Source Port
- Destination Port
- Analytical Comments
- CONTENT REVIEW

Anatomy of the Hack



Telnet

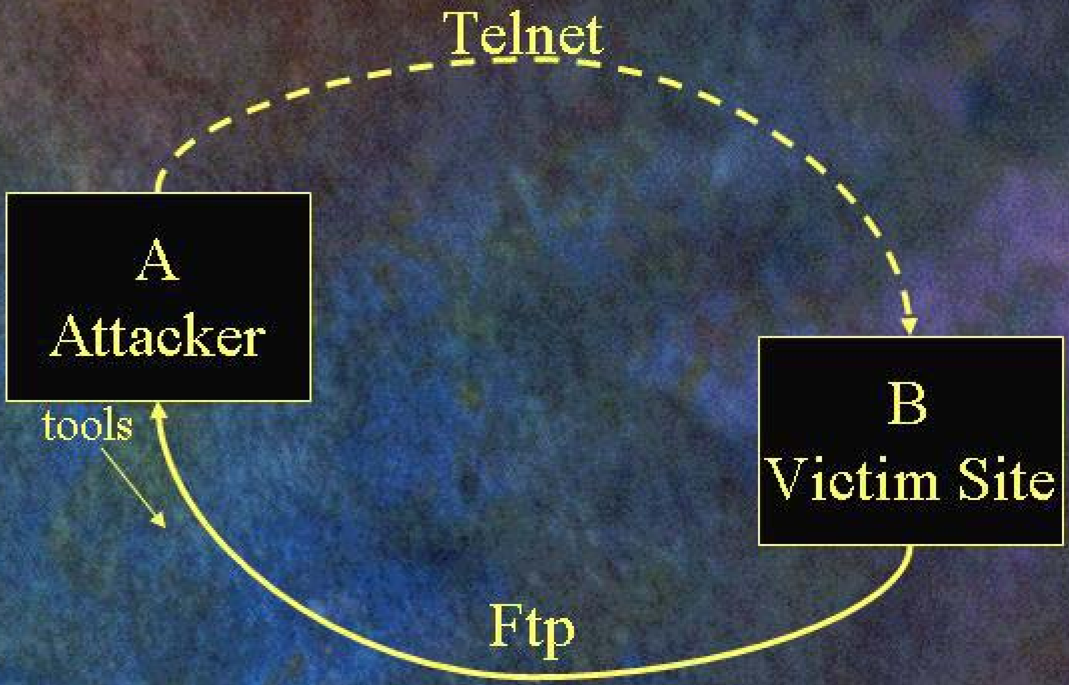
A
Attacker

--> legimate Acct.

B
Victim Site

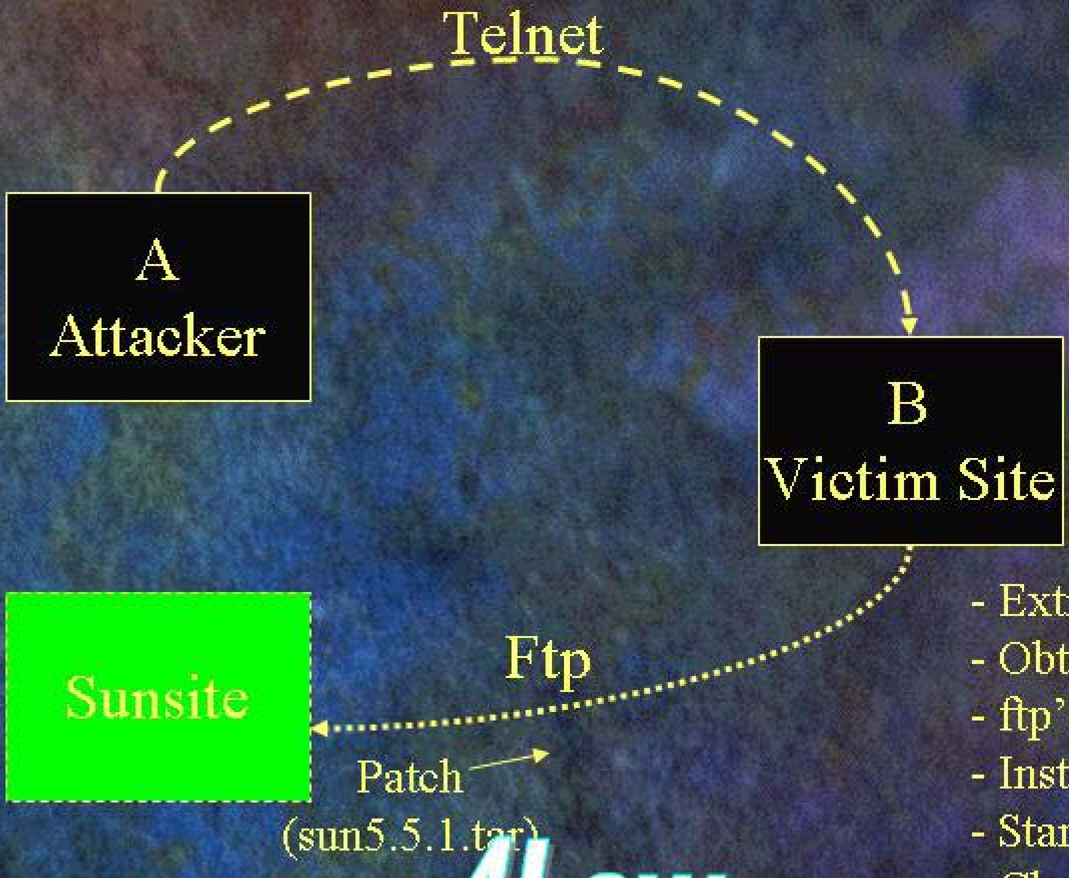
4Law

Anatomy of the Hack



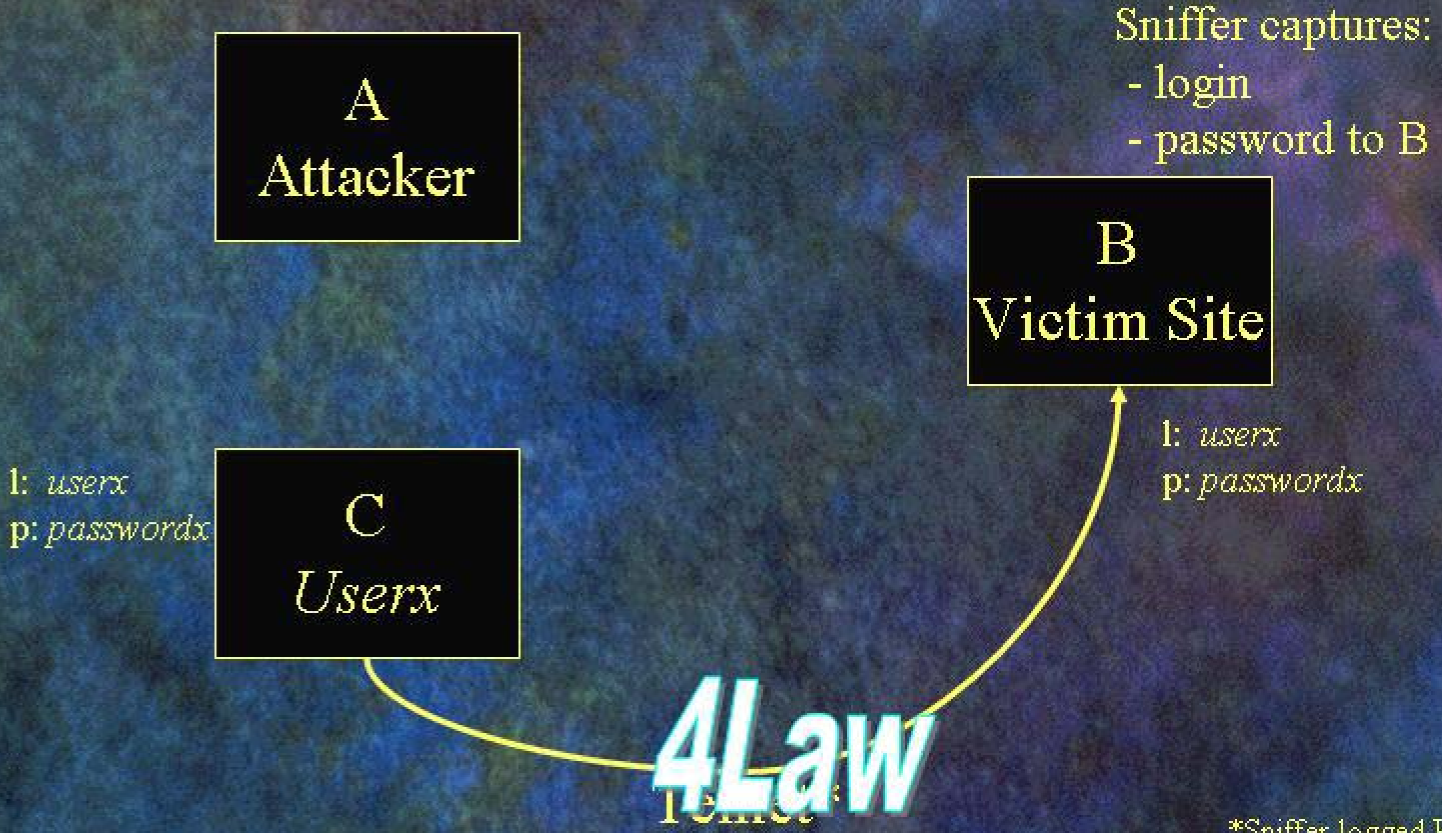
4Law

Anatomy of the Hack



- Extracts (tar -x) tools
- Obtains root (tclsh)
- ftp's patch
- Installs Patch
- Starts sniffer (ttymon)
- Cleans up (ll)
- Exits telnet session
- Revisit site

Anatomy of the Hack



Sniffer captures:
- login
- password to B

A
Attacker

B
Victim Site

l: *userx*
p: *passwordx*

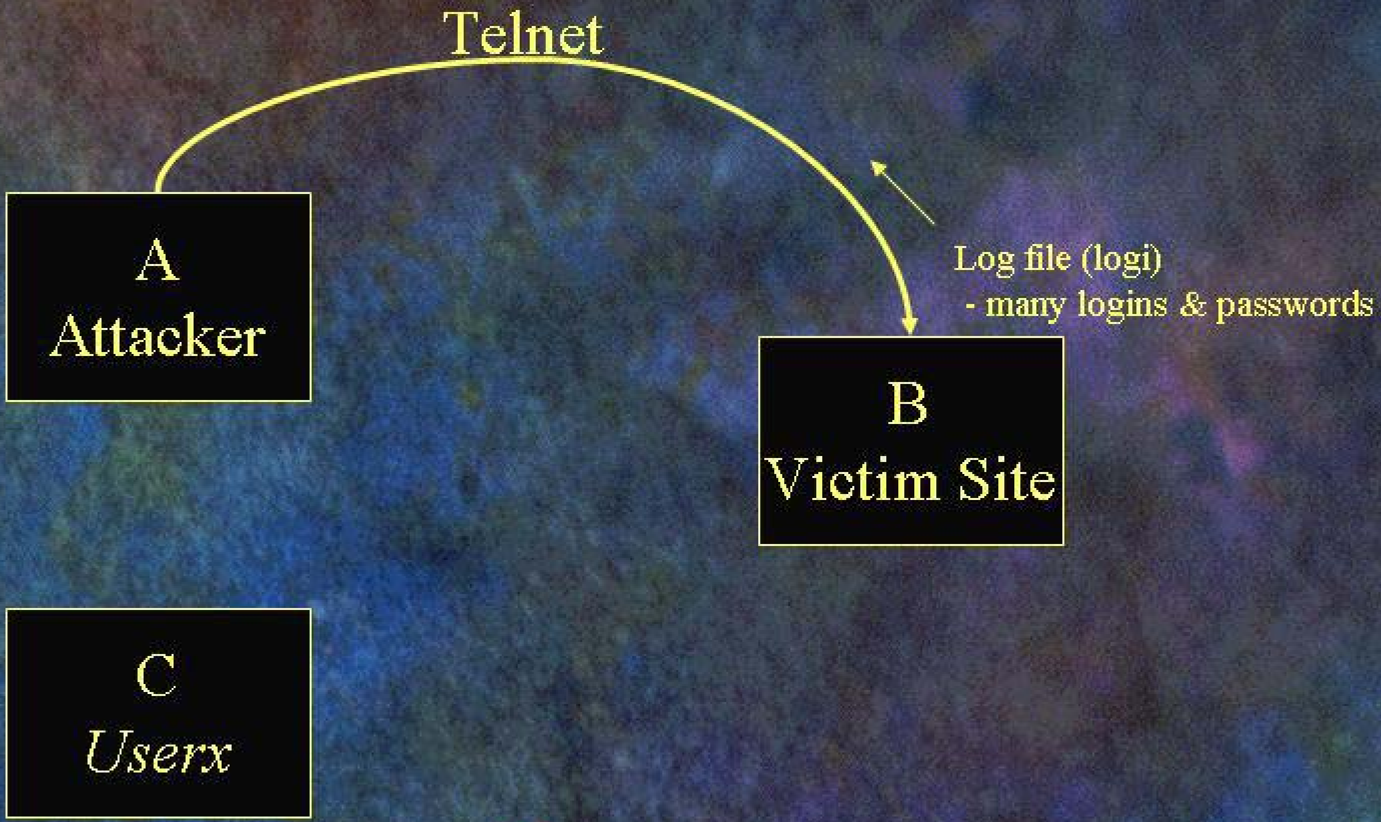
C
Userx

l: *userx*
p: *passwordx*

Telnet*

*Sniffer logged POP, telnet, ftp

Anatomy of the Hack



Telnet

A
Attacker

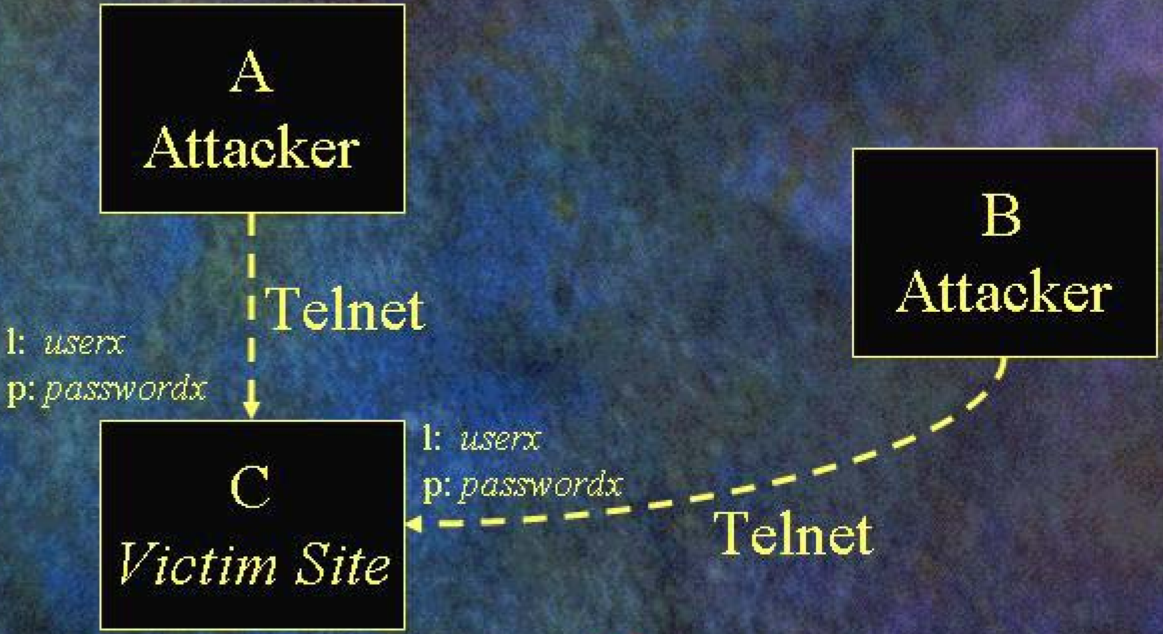
Log file (logi)
- many logins & passwords

B
Victim Site

C
Userx

4Law

Anatomy of the Hack



A
Attacker

Telnet

l: *userx*
p: *passwordx*

B
Attacker

l: *userx*
p: *passwordx*

Telnet

C
Victim Site

4Law

Internet Relay Chat (IRC)

21 Feb - 26 Feb 98

- Stimpy account used by both brothers
  - IRC tipped the hand
    - Older brother surfed net (mostly music sites)
    - Stimpy involved in chats & hacks
- Stimpy/Mak Partnership
- Mak's Web Page
  - www.G0D.org
    - tools, hacking files, members of #enforcers
      - Analyzer, Guy Jentaoris, etc.

Internet Relay Chat (IRC)

21 Feb - 26 Feb 98

- Mak/Analyzer Relationship
  - Analyzer (aka Hellno)
    - 129.116*.*
    - Hertzelia-*.*.access.net.il

. is the last 2 octets in Analyzer's dynamic ip address.

  - Mentor/Student
  - 3 llnl.gov sites & 1 .net site given to Mak by Analyzer (l: danny68)
  - Coached him in attacking pearlharbor.navy.mil
    - blocked site
  - Mak used l: rewt p: kapish in accessing sites

Internet Relay Chat (IRC)

21 Feb - 26 Feb 98

- Other Relationships
  - Other School Friends
  - Analyzer/Jentaoris Relationship (.il’s)
  - Analyzer/CallDan Relationship
- Altered DNS Information & Host Names
  - e.g. the.only.good.islam.is.a.dead.islam.net
- Characterized Players

End of the Party

21 Feb - 26 Feb 98

- 25 Feb 98
    - Story released to Media by DoD
        - FBI initiated search of MAK & STIMPY residences
            - Computer equipment and peripherals seize
- 26 Feb 98
    - Washington Team Members take 0600 flight
        - no booze/all snooze

Lessons Learned/Knowledge Gained

21 Feb - 26 Feb 98

- Communicate, Communicate, Communicate!
- Value of IRC Analysis
- Hacking Group Analysis
- Post Analysis Needed
  - Revisit HDs, check out other channels, other players, etc.
  - Quicker turn-around of Post Analysis
- Sharing of Information between Agencies

Interview with AntiOnline

- ❶ MAK interview discloses questions asked, items seized and investigation focus
- ❷ Interview of ANALYZER after arrest of MAK and STIMPY Claimed to have hacked 400 DOD sites
- ✓ Does live hacking demonstration of .gov site to gain credibility
- ✓ Provides list of dozens of logins and passwords for .mil sites

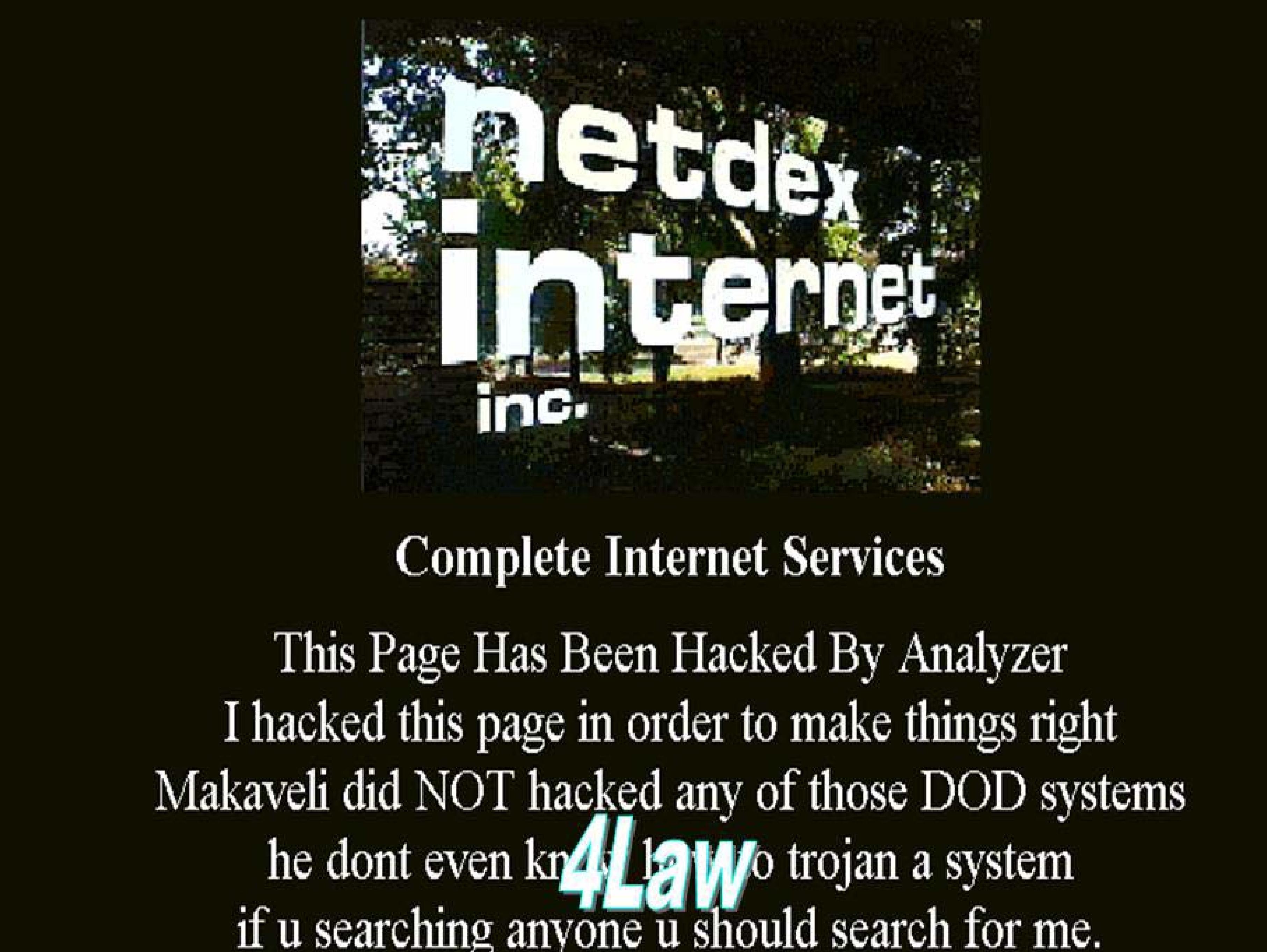
4Law

Interview with AntiOnline

March 4, 1998

Analyzer - u see makaveli was my student if u wish to call it that way
Analyzer - he didn't know how to Trojan systems or any shit like that
Analyzer - he only used my shell list
Analyzer - my short shell list
Analyzer - cos beside that shit i have about 400 systems of DOD
JP - may i ask, what country you are from?
Analyzer - no
JP - ok, that's understandable
JP - so makaveli was just your student?
JP - why did you decide to take on a student?
Analyzer - well all my years as a hacker i had bad experience with students and such but since i was going to retire i was going to teach someone some of my knowledge and guide him

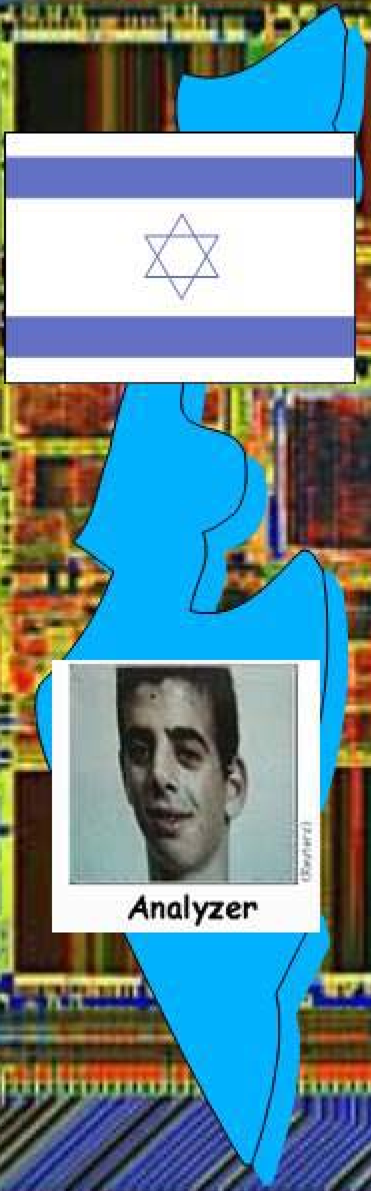
4Law



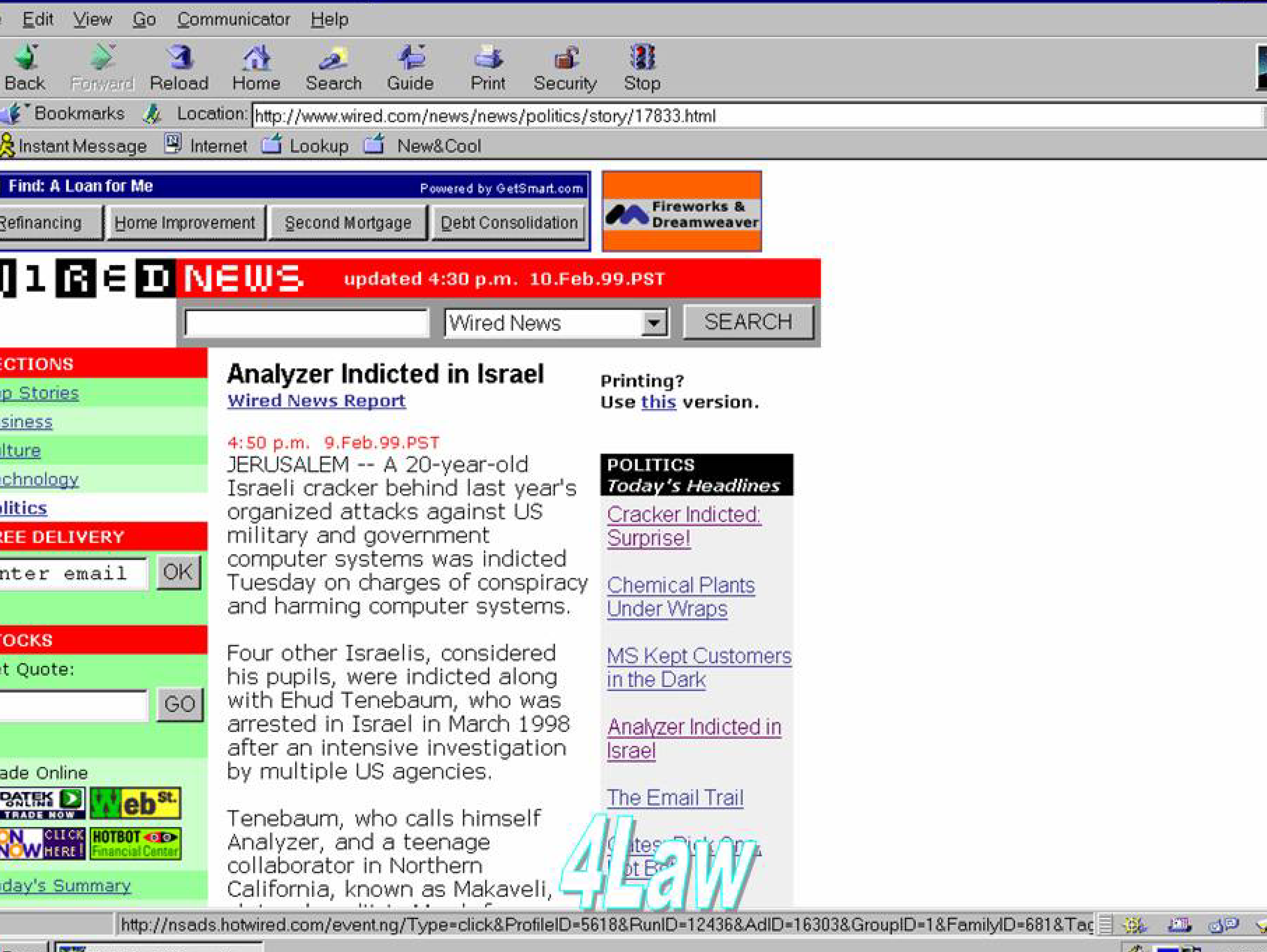
Complete Internet Services

This Page Has Been Hacked By Analyzer
I hacked this page in order to make things right
Makaveli did NOT hacked any of those DOD systems
he dont even know how to trojan a system
if u searching anyone u should search for me.

Solar Sunrise: The Analyzer


Analyzer

(Reuters)


Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.wired.com/news/news/politics/story/17833.html
Instant Message Internet Lookup New&Cool
Find: A Loan for Me Powered by GetSmart.com
Refinancing Home Improvement Second Mortgage Debt Consolidation
Fireworks & Dreamweaver
IRED NEWS updated 4:30 p.m. 10.Feb.99.PST
Wired News SEARCH
ECTIONS
p Stories
siness
lture
chnology
litics
REE DELIVERY
nter email OK
OCKS
t Quote:
GO
ade Online
DATEK ONLINE TRADE NOW
Web St.
ON NOW CLICK HERE!
HOTBOT Financial Center
day's Summary
4Law
http://nsads.hotwired.com/event.ng/Type=click&ProfileID=5618&RunID=12436&AdID=16303&GroupID=1&FamilyID=681&Tag

Analyzer Indicted in Israel

Wired News Report

4:50 p.m. 9.Feb.99.PST

JERUSALEM -- A 20-year-old Israeli cracker behind last year's organized attacks against US military and government computer systems was indicted Tuesday on charges of conspiracy and harming computer systems.

Four other Israelis, considered his pupils, were indicted along with Ehud Tenebaum, who was arrested in Israel in March 1998 after an intensive investigation by multiple US agencies.

Tenebaum, who calls himself Analyzer, and a teenage collaborator in Northern California, known as Makaveli,

Printing?
Use this version.

POLITICS
Today's Headlines

Cracker Indicted: Surprise!

Chemical Plants Under Wraps

MS Kept Customers in the Dark

Analyzer Indicted in Israel

The Email Trail

Gates Didn't ... Not B...

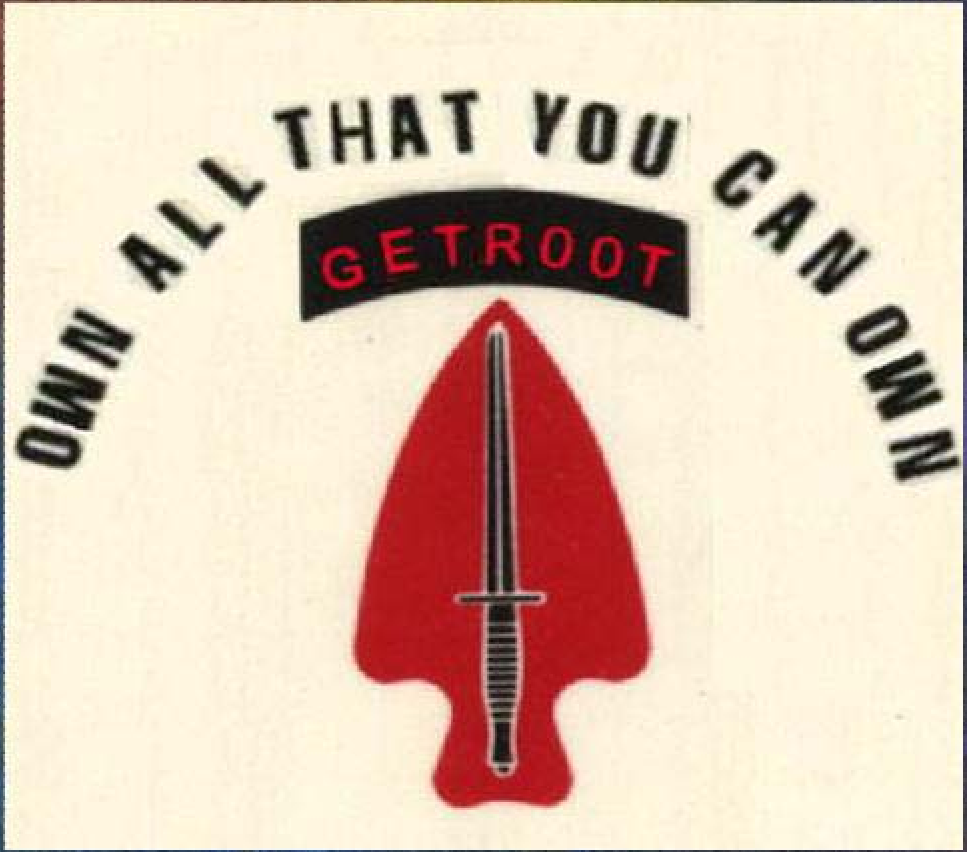
Status?

- Provided alerts
- Investigators traveled to Israel
- 2 Juveniles Pled Guilty
- Analyzer in Israel
  - Out of the Military
  - ✓ Charged 2-9-99 with 4 others
  - ✓ New Computer Crime Statute

- Calldan Levi Coffman (NASA IG)
- Sean Trifero (Boston
  - 5 years
- NCIS & WFO - N.Florida
- Total 10 indicted
- Analysis Continuing

...

he Truth is Out Ther



4Law

National Infrastructure Protection Center
Federal Bureau of Investigation
Room 11719
935 Pennsylvania Avenue, NW
Washington, DC 20535

nipc@fbi.gov
(202) 324-3000

SSA Scott K. Larson
202-324-036[illegible] [illegible]on@fbi.gov