

Possible CodeRed Connection Attempts

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-07/0129.html>

From: dave.goldsmith@intelsat.com

Date: 07/20/01

Message-ID: <490B4C213EC8D211851F00105A29CA5A1100A9B0@admex1.adm.intelsat.int>
From: dave.goldsmith@intelsat.com
To: incidents@securityfocus.com, focus-ids@securityfocus.com
Subject: Possible CodeRed Connection Attempts
Date: Fri, 20 Jul 2001 08:42:13 -0400

We have a sniffer located on the network segment behind our Internet router and in front of the firewall. The stats below show attempts from Internet hosts to connect to port 80 on random IP addresses on our class B network. I have not included any connections to the machines that are running web servers that are reachable from the Internet.

Because the firewall blocks port 80 connections, except for the designated web servers, all I have are the initial SYN packets so I don't know for sure that all of these packets are being generated by the CodeRed worm. However, I believe that the vast majority of them are.

The stats are broken down by hour and then included a summary for the day. I have included all of July 18th as a baseline for what appears to be "normal" hacking/probing activity. Starting around 9am on July 19, the numbers start to skyrocket. The times are EST.

Dave Goldsmith

Day Hour Total Unique
Connections Sources

```
=====
07/18 00 143 20
07/18 01 148 15
07/18 02 89 15
07/18 03 96 18
07/18 04 144 22
07/18 05 127 16
07/18 06 98 15
07/18 07 111 16
07/18 08 116 15
07/18 09 149 22
07/18 10 143 18
```

SecurityFocus Bugtraq: Possible CodeRed Connection Attempts

07/18 11 175 24
07/18 12 134 22
07/18 13 146 20
07/18 14 118 21
07/18 15 95 17
07/18 16 133 22
07/18 17 104 17
07/18 18 78 17
07/18 19 76 15
07/18 20 67 15
07/18 21 85 15
07/18 22 62 12
07/18 23 105 14

Day Total 2742 194

07/19 00 120 17
07/19 01 81 12
07/19 02 62 11
07/19 03 97 20
07/19 04 85 18
07/19 05 128 20
07/19 06 140 20
07/19 07 212 34
07/19 08 645 137
07/19 09 5717 1281
07/19 10 36879 8186
07/19 11 150913 34361
07/19 12 362011 79789
07/19 13 519846 111148
07/19 14 556220 117946
07/19 15 547087 115193
07/19 16 540009 115983
07/19 17 519810 111290
07/19 18 499565 107106
07/19 19 390019 89331
07/19 20 14541 3493
07/19 21 9733 2233
07/19 22 9093 1882
07/19 23 8539 1672

Day Total 4171552 274041

-
- **Previous message:** [Eric Chien: "RE: Full analysis of the .ida "Code Red" worm."](#)
 - **Next in thread:** [Ken Eichman: "Re: Possible CodeRed Connection Attempts"](#)
 - **Reply:** [Ken Eichman: "Re: Possible CodeRed Connection Attempts"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)