

RE: Unusual port scan?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-12/0096.html>

From: Hamish webhosting.net.nz (*koremeltdown_at_hotmail.com*)

Date: 12/29/03

To: jonas2@knology.net, incidents@securityfocus.com

Date: Mon, 29 Dec 2003 05:41:14 +0000

Hi there,

are you able to tell us via your logs what sort of timing there was between each port being hit?

Also, does the log dump shown here show all of the instances of this port being hit by this intruder?

I am thinking this might be some sort of DOS or attempted DOS attack on your PC and/or network.

Kindest of regards,

Hamish Stanaway

Absolute Web Hosting

Owner/Operator

Auckland

New Zealand

<http://www.webhosting.net.nz>

<http://www.buywebhosting.co.nz>

>From: J Bailes To: incidents@securityfocus.com Subject: Unusual port scan?
>Date: 28 Dec 2003 22:59:12 -0000 MIME-Version: 1.0 Received: from
>outgoing2.securityfocus.com ([205.206.231.26]) by mc7-f7.hotmail.com with
>Microsoft SMTPSVC(5.0.2195.6713); Sun, 28 Dec 2003 19:54:54 -0800 Received:
>from lists.securityfocus.com (lists.securityfocus.com [205.206.231.19]) by
>outgoing2.securityfocus.com (Postfix) with QMQPid 1EB898F384; Sun, 28 Dec
>2003 14:36:29 -0700 (MST) Received: (qmail 22429 invoked from network); 28
>Dec 2003 23:17:15 -0000 X-Message-Info: JGTYoYF78jGdg+ZvfInuZhGvmkzMUPfx
>Mailing-List: contact incidents-help@securityfocus.com; run by ezmlm
>Precedence: bulk List-Id: List-Post: List-Help: List-Unsubscribe:
>List-Subscribe: Delivered-To: mailing list incidents@securityfocus.com
>Delivered-To: moderator for incidents@securityfocus.com Message-ID:
><20031228225912.15403.qmail@sf-www1-symnsj.securityfocus.com> X-Mailer:
>MIME-tools 5.411 (Entity 5.404) Return-Path:
>incidents-return-7058-koremeltdown@hotmail.com@securityfocus.com
>X-OriginalArrivalTime: 29 Dec 2003 03:54:54.0444 (UTC)
>FILETIME=[84A63AC0:01C3CDBF]
>
>

RE: Unusual port scan?

SecurityFocus Incidents: RE: Unusual port scan?

>

>My router logs on my personal/home machine just started receiving with
>these scans:

>

>12/28/2003 13:05:44.133 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:04:50.236 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:04:42.705 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:04:16.067 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:04:11.991 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:58.982 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:56.639 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:50.440 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:48.958 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:46.164 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:45.112 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:44.031 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:43.199 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:42.428 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:42.238 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800
>12/28/2003 13:03:42.168 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1802
>12/28/2003 13:03:41.757 – 81.52.250.105 : 80 >>> xx.xxx.xxx.xxx : 1800

>

>

>The scans supposedly came from:

>

>[Query: 81.52.250.105, Server: whois.ripe.net] % This is the RIPE Whois
>server. % The objects are in RPSL format. %% Rights restricted by
>copyright. % See <http://www.ripe.net/ripenc/db/copyright.html>
>inetnum: 81.52.248.0 – 81.52.250.127 netname: AKAMAI-FT-US descr: Akamai
>Technologies – US machines connected to FT AS5511 country: US admin-c:
>NARA1-RIPE tech-c: NARA1-RIPE tech-c: NF1714-RIPE status: ASSIGNED PA
>mnt-by: FT-BRX changed: gestionip.ft@francetelecom.com 20030321 source:
>RIPE route: 81.52.240.0/20 descr: France Telecom descr: Opentransit origin:
>AS5511 mnt-by: FT-BRX changed: gestionip.ft@francetelecom.com 20030214
>source: RIPE role: Network Architecture Role Account address: Akamai
>Technologies address: 500 Technology Square address: Cambridge, MA 02139
>phone: +1-617-250-4768 e-mail: ip-admin@akamai.com admin-c: NF1714-RIPE
>admin-c: JP1944-RIPE tech-c: NF1714-RIPE tech-c: JP1944-RIPE nic-hdl:
>NARA1-RIPE notify: ip-admin@akamai.com changed: ip-admin@akamai.com
>20021025 source: RIPE person: Noam Freedman address: Akamai Technologies
>address: 500 Technology Sq address: Cambridge, MA 02139 phone: +1 617 250
>4768 e-mail: noam@akamai.com nic-hdl: NF1714-RIPE notify: noam@akamai.com
>changed: noam@akamai.com 20021025 source: RIPE [End of Data]

>

>

>The scan seems to be looking for: ansys-lm – ANSYS-License manager for port
>1800 concomp1 – ConComp1 for port 1802

>

>According to this: <http://aaron.boim.com/unix/sshTunnel.html>, it may be
>scan for an open proxy used for SSH? I dunno.

>

RE: Unusual port scan?

SecurityFocus Incidents: RE: Unusual port scan?

>I'm not familiar with these services (nor am I running them). I did not
>have any browser windows open at the time of the scan. So, out of nowhere,
>why would an Akamai box scan me for these services? Is anybody else
>getting this kind of traffic?
>
>
>-----
>-----
>

Check your PC for viruses with the FREE McAfee online computer scan.
<http://clinic.mcafee.com/clinic/ibuy/campaign.asp?cid=3963>

