

Re: Unusual port scan?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-12/0100.html>

From: Patrick Kremer (patrick_at_nicsys.net)

Date: 12/29/03

To: <incidents@securityfocus.com>

Date: Sun, 28 Dec 2003 22:01:39 -0600

This is probably legitimate traffic. Check out the Akamai FAQ at http://www.akamai.com/en/html/misc/support_faq.html

Patrick Kremer
Chief Technical Officer
NIC Systems Group, Inc.
patrick@nicsys.net

----- Original Message -----

From: "J Bailes" <jonas2@knology.net>

To: <incidents@securityfocus.com>

Sent: Sunday, December 28, 2003 4:59 PM

Subject: 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

>

Re: Unusual port scan?

SecurityFocus Incidents: Re: Unusual port scan?

```
>
> 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/ripencc/pub-services/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
```

Re: Unusual port scan?

SecurityFocus Incidents: Re: Unusual port scan?

> *[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.*

>

> *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?*

>

>

>

-

>

--

>

>
