

Re: freebsd-security Digest, Vol 61, Issue 3

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0014.html>

From: Crist J. Clark (*cristjc_at_comcast.net*)

Date: 06/07/04

Date: Mon, 7 Jun 2004 13:39:43 -0700
To: Neo-Vortex <root@Neo-Vortex.Ath.Cx>

On Mon, Jun 07, 2004 at 04:10:46PM +1000, Neo-Vortex wrote:

> On Mon, 7 Jun 2004, Michael Vlasov wrote:
>
>> On Sat, 29 May 2004 12:00:52 -0700 (PDT),
>> <freebsd-security-request@freebsd.org> wrote:
>>
>> Hello !
>>
>> Today i see in snort logs :
>>
>> [**] [1:528:4] BAD-TRAFFIC loopback traffic [**]
>> [Classification: Potentially Bad Traffic] [Priority: 2]
>> 06/07-09:44:39.044590 127.0.0.1:80 -> 10.6.148.173:1566
>> TCP TTL:128 TOS:0x0 ID:577 IpLen:20 DgmLen:40
>> ***A*R** Seq: 0x0 Ack: 0x75830001 Win: 0x0 TcpLen: 20
>> [Xref => <http://rr.sans.org/firewall/egress.php>]
>>
>> [**] [1:528:4] BAD-TRAFFIC loopback traffic [**]
>> [Classification: Potentially Bad Traffic] [Priority: 2]
>> 06/07-09:44:39.075824 127.0.0.1:80 -> 10.6.249.83:1299
>> TCP TTL:128 TOS:0x0 ID:578 IpLen:20 DgmLen:40
>> ***A*R** Seq: 0x0 Ack: 0x568A0001 Win: 0x0 TcpLen: 20
>> [Xref => <http://rr.sans.org/firewall/egress.php>]
>>
>> [**] [1:528:4] BAD-TRAFFIC loopback traffic [**]
>> [Classification: Potentially Bad Traffic] [Priority: 2]
>> 06/07-09:44:39.107072 127.0.0.1:80 -> 10.6.96.121:1032
>> TCP TTL:128 TOS:0x0 ID:579 IpLen:20 DgmLen:40
>> ***A*R** Seq: 0x0 Ack: 0x37920001 Win: 0x0 TcpLen: 20
>> [Xref => <http://rr.sans.org/firewall/egress.php>]
>>
>> Why ? ;-)
>
> Ok, that means that someone (or thing) is spoofing packets to your box
> (i know, and so does snort, that its spoofed because the source ip is
> 127.0.0.1 and its coming in on an interface apart from lo0) this is
> sometimes used as a DoS attack (its one of those fun addresses to use as

- > *source addresses for them), although, by the looks of it (because theres*
- > *multiple dst-ports being used), someone is using a program like nmap to*
- > *portscan your host using a spoofed ip*

The original post is not really on topic for this list. It is a general security incident question whereas the topic here should be more FreeBSD specific.

That said, that traffic looks like Blaster backscatter. Early on in Blaster, there was some ill-conceived advice to map windowsupdate.com to 127.0.0.1 to prevent the DDoS. So what happens is that an infected host picks a random address "near" its own, in this case, it looks like the infected host is in 10.6.0.0/16, looks up the hostname to attack and gets 127.0.0.1. It sends a SYN to 127.0.0.1, which is itself, but odds are it has no HTTP server running, nothing listening on 80/tcp so it replies with a RST to the source... the spoofed source... with the source of the RST being the destination of the SYN, 127.0.0.1. These RSTs are what you are seeing above.

So, if this traffic is coming from some internal 10.16.0.0/16 network, it's time to go looking for a Blaster infection. If it is originating from the outside, not a lot you can do, but there is nothing harmful about it unless there is enough of this noise to eat significant resources.

--

Crist J. Clark		cjclark@alum.mit.edu
		cjclark@jhu.edu
http://people.freebsd.org/~cjc/		cjc@freebsd.org

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"