

Re: What is the Pattern here ?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-08/0223.html>

From: !:?) (_at_*.com)

Date: 08/05/04

Date: Thu, 05 Aug 2004 18:26:54 GMT

Hi Moe,

Moe Trin wrote:

>>*If they are Honeypots they are broken.*

>

>

> *Not impossible*

These are all Dialup Connections that I had no connection with at the time.

>>*Why are they actively probing me ? I didn't probe them and many time I*

>>*Ignore them for hours before I check them out.*

>

>

> *How do you know they aren't being spoofed, and you are doing the "attack"*
> *of their real target for them.*

>

True and one of the reasons I asked in this NG if there was a pattern here that could show this or other possibilities.

I only do the one scan back and only when the same IP hits me over and over again.

They Scan the same Ports 3 times each (2745, 5000, 6129) every few minutes.

The Scans usually stop right away or soon after (to complete the Scan Pattern) and don't return with that IP.

They sometimes run NetBIOS at the end of a scan after I probe back but lately I've seen them using it at the end of their Scans that they never did before even when I don't probe back.

>

>>*I wonder if the Web Accellerators that are nothing more than Servers are*
>>*being abused by Spammers.*

>

>

> *Given that nearly all dialup hosts are run by people who shouldn't be using*
> *a computer – I'd certainly believe it. Last I looked at my spam email logs,*
> *a third of the spam was coming from r00ted windoze boxes on Comcast and*

comp.security.firewalls: Re: What is the Pattern here ?

- > ATT, and only a tiny fraction from professional spam servers in .cn, .it,
- > or .kr.
- >

Doesn't surprise me and I have ATT.

The ATT Web Accelerator is like a Web Server and I think could be abused to Host Zombie Web and DNS Servers for Spammers and Crackers.

- >
- >>I should have added that was true but MS leaving the door open
- >>by default deserves some of the blame too.
- >
- >
- > They are just doing what the sheep that buy it want. A *_very_ large*
- > *percentage of windoze users don't want to know anything, and even the*
- > *smallest security function that gets in the way of these fools clicking*
- > *on some icon (about half of which don't even know what the icon means),*
- > *annoys them. That's why microsoft has included the options of "remember*
- > *my password", and open (or install) everything by default without asking*
- > *me stupid questions. It's obviously an enormous security hole, but the*
- > *sheep don't know (or want to know) or care.*

Many Sheep didn't have a choice because all the new software was comparable only with Windows for the home user.

Those of us that wanted to sick with DOS were left high and dry for a long time.

But the worm turns.

Now Security and Stability have become more of an Issue today and that's come back to bite MS in the butt.

- >>No but I have a rule for each one to give me more info on my searches
- >>for that service.
- >>I use a Block All at the end of the Rules List and all the other Trojan
- >>Rules are just notes for general info.
- >
- >
- > Why bother? Block the stuff and ignore it.

I did but I changed ISP's and turn everything on to see what it's doing.
(Why I don't like the ATT Web Accelerator)

- >>I could delete the whole Trojan list and it wouldn't make any difference
- >>in security.
- >
- >
- > No, but it would waste a lot less of your time, CPU cycles, and diskpace.

Those Rules can be unchecked from the list or I can move the Block All TCP/UDP Rule at the end up above the Trojan List where it won't process them.

comp.security.firewalls: Re: What is the Pattern here ?

>>Sorry, I wrote PCTool and meant PCAnywhere (I don't use it much).
>>I don't run ANY tools from a Website and mostly use a Dos Batch File.
>
>
> Are you sure about that? You might want to run a sniffer while using
> those tools, and see where the packets are going. Remember, 53 is DNS,
> and 43 is whois. Neither service found on port 80 of some server.

I'm not sure why you list port 80 with 53 and 43 ?
(I did get a few hits on Port 80 but not sure if it was in the log I
Posted and think that only happened once after this.)

A WhoIs uses Whois.exe, Traceroute.exe, Ping.exe, ect... are files and
has rules for each in and outbound.

>>I allow it for my ISP only at the moment but am still undecided about
>>that as I can block that with no effect.
>>I've read pro's and con's on it and haven't made up my mind about it.
>
>
> NSA recommends denying echo, redirect, and netmask, and allowing the rest.
> <http://www.nsa.gov/snac/index.html>. I disagree, suggesting that you allow
> 0, 3, 4 and 11 INBOUND, 3, 4, and 8 OUTBOUND, while denying all else. Some
> may consider type 4 (Source Quench) as undesirable (possible DOS). YMMV

At the moment I only allow Echo Request (out), Reply (in) and Time
Exceeded (in).
Type 3 I don't think I need and is abused by some ISP's if I remember right.

>>The Port 443 I block.
>
>
> [compton ~]\$ grep -w 443 rfc/port-numbers
> https 443/tcp http protocol over TLS/SSL
> https 443/udp http protocol over TLS/SSL
> [compton ~]\$
>
> Inbound, I'd agree, as you are not running a Secure web site, but
> outbound? Why?

I added that and a few others to be sure I wasn't sending out and was
calling those Dialups to probe me.

>>I always use a Block all except when adding a new App that requires a
>>lot of rules.
>
>
> That's the difference in philosophy between a so-called personal firewall
> and a real firewall box. We don't worry about applications needing
> specific access, because we only look at the service and protocol involved.
> We also don't install rouge applications.

Re: What is the Pattern here ?

comp.security.firewalls: Re: What is the Pattern here ?

I don't have a newtork here and a Router isn't really a firewall but does a good job filling the holes.

>>>Are you saying 'Block All' doesn't mean Block *_ALL_* ??? What happens if
>>>someone sends you a protocol Type 2 (IGMP) or Type 92 (MTP) packet? Does
>>>your firewall toss up it's hands and go into the corner to cry?
>>
>>No the Block All (UDP/TCP) works.
>
>
> [compton ~]\$ egrep '(icmp/tcp/udp)' /etc/protocols
> icmp 1 ICMP # internet control message protocol
> tcp 6 TCP # transmission control protocol
> udp 17 UDP # user datagram protocol
> [compton ~]\$
>
> That's great, but protocol 6 is not protocol 17, is not protocol 2 or any
> of the other 135 protocols that can be carried in an IP frame. See
> <http://www.iana.org/assignments/protocol-numbers>

Sorry I first read IGMP as ICMP.
My Firewall blocks all IGMP.

>>Without the Block All and the Rules Assistant on sometimes a UDP drops
>>through the list and no action is logged.
>
>
> As long as it's dropped, and no one on the inside of the firewall is not
> complaining about broken services, then that's fine.

True and also if I were on a network.
I didn't like not seeing it Logged as Blocked or Permitted though.
If I didn't have a Log All Rule at the end of the list to see what went
by I would never have known that was happening.
AtGuard told you about this and suggested a Block All and or a Log Rule
at the end of the list.
But NIS hid that info in their help files and then you had to read
between the lines about adding a Block All Rule since it said some UDP's
drop through.

>>>Why do you care? The firewall blocked it. Anything else you may do is
>>>just wasting CPU cycles, and not providing a useful service to you.
>>
>>Why not have a info box to list what uses that service both good and bad ?
>
>
> If you have nothing better to do than to look at each and every packet you
> see – that's fine. People like me don't have time for that.

If you have them turned on all the time yes but when you want as much
information on a Port's Services and Abuses.

Re: What is the Pattern here ?

comp.security.firewalls: Re: What is the Pattern here ?

>

>

>>*Just like some Files when you click Properties and you get the info Tab.*

>

>

> *You forget that not all of us are running windoze. This system doesn't have
> a single icon, menu bar, or similar in sight. Or do you think those commands
> I've been showing are from some exotic section of windoze that you haven't
> seen before?*

Never liked windows because security and stability was a joke where they
are just now starting to address those problems.

DOS wasn't as pretty as Windows but it was a lot more stable.

Right after installing Win9x you have 80 plus errors in 90 plus
categories in the registry.

Installing programs on an unstable OS with that many errors won't show
problems right away but...

The more Programs you install the greater the load and Stability becomes
a problem.

Well looks like your the one I should ask this question to.

What OS is best to replace Windows for the home User that may or may not
be connected to a network.

I see Lindows gaining but with so many from Redhat and others which one
is best for home use ?

>

> *Old guy*

Another Old Guy !:)

Kevin