

# Re: Block Attacker showing wierd name – not just IP...

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2004-03/0225.html>

---

**From:** Jim Harrison [MSFT] (*jmharr\_at\_online.microsoft.com*)

**Date:** 03/08/04

Date: Mon, 8 Mar 2004 07:52:28 -0800

Sorry, Tony, but BlockAttacker only has value as an instructional mechanism to illustrate the use of environment variables created by alerts.

Anyone who employs it to "automatically block attacks" doesn't really understand the complexity implied in the term "attack" and is looking forward to future problems when the script blocks everything from Google because of a "late packet".

There is no way the script can properly evaluate the traffic because it doesn't exist by the time the script runs.

--

Jim Harrison [ISASE]

Read the help, books and articles!

This posting is provided "AS IS" with no warranties, and confers no rights.

"Tony Su" <anonymous@discussions.microsoft.com> wrote in message news:796501c4027c\$670e09b0\$a1012

I have seen this with only one ISA in the "array."

I wonder if the attack comes fast enough so that ISA is not able to respond fast enough it might appear like multiple blocks are created at once for the same IP address?

I personally believe the BlockAttacker script has value that goes beyond the normal IDS defenses...

- Although I don't know for sure, intuitively I feel that it likely takes more processing to evaluate an attack than to simply block all communications from that IP address  
- IDS is purely defensive. Although it will drop packets when a possible attack is perceived, it does nothing to discourage the attacker. I feel alot better if in response to a port scan <everything> is then denied to the attacker. In other words, rattle just one lock and now you're denied everything. I don't want the hacker trying different locks in turn looking for a weakness.

Tony Su

>-----Original Message-----

>It means you have the script running on more than one ISA in an array and both instances of the script are trying to create

>identical packet filters.

>This is yet another example of why using this script as a "think for me" mechanism is a bad idea.

>Think about it:

>1 - the script is fired from an "intrusion detected"

microsoft.public.isa: Re: Block Attacker showing wierd name – not just IP...

```
alert action
>2 - if the alert fired, ISA already blocked the traffic
>
>Since ISA is already blocking the traffic it
deems "invasive", adding a PF to block what was already
blocked only adds rule
>processing time to ISA default behavior.
>
>Solution:
>1 - ditch the script
>2 - delete the PF it created
>3 - start using a log analysis tool to see what's really
an "attack" and what isn't. Mark Burnett has a good
article on how you can
>do that here:
> http://www.securityfocus.com/infocus/1712
>--
> Jim Harrison [ISASE]
> Read the help, books and articles!
>
> This posting is provided "AS IS" with no warranties, and
confers no rights.
>
>
>"darthbaggins" <spam@nothanks.com> wrote in message
news:OqVa2dFAEHA.692@TK2MSFTNGP11.phx.gbl...
>What does it mean when, instead of just an IP address,
block attacker
>displays the IP address followed by hex codes in the
following pattern:
>{11A1A1A1-1111-1A11-11AA-1AA1AA1AA11A} ?
>
>I noted this all relative to a single IP but with about
20 or so different
>variations on the same code. The name is the only thing
that changes, the
>actual IP under the properties is still the same.
>
>Thanks in advance.
>
>
>
>
>.
```