

Re: Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-05/1377.html>

From: Duane Arnold (*notme_at_notme.com*)

Date: 05/21/03

Date: Tue, 20 May 2003 23:02:11 GMT

> *The Lurker is right. Black Ice sucks ! Zone Alarm, Norton, etc all are a*
> *better choice.*
>
>

I want to know what you know!

> *I personally hated BI's application control. Baselineing every .exe*
> *file is ridiculous when perhaps only a few dozen applications actually*
> *access the net.*

Then you have missed the point, because it's not the exe that wants access to the Internet. It's a dll, ocx, vbx etc, etc. that is using an exe like the Iexplorer.exe, msimn.exe, or svchost.exe to get out to the Internet. That is those programs job to access the Internet, and subcomponent programs use the exe(s) or any exe whose job is to access the Internet on their behalf. Those subcomponent programs are the potential Trojans that can make the phone call home. Those subcomponent programs are the ones that can overly an existing dll, ocx, vbx, etc. or get deployed deep in the O/S directory so that it is not recognized as being a suspicious program.

In that respect, BI is doing exactly what it needs to be doing taking an inventory of every program element on the machine. And my machines are clean of Trojans when I do the baseline and everything is fine at the point of the baseline. Now if IOStrom.dll hits my machine and wants to use Iexplorer.exe to make the phone call home, BI is going to stop IOStrom.dll telling me that it wants to use Iexplorer.exe to access the Internet. A clear *RED* flag that something is not right.

BI's Application control combined with it's IDS has the ability to see and exe, dll, ocx etc. coming in the network traffic, or being executed from a Website and stop the execution. I have been in touch with ISS about how BI is using IDS with Application control to stop execution of malware coming in the network traffic. I was told that it was not using the Application Control Database to do this.

BI has a weakness in that a dll or something similar with the exact name of

a file the is being overwritten that has been approved for execution and communications can beat it. But if the file is being written to a directory that does not have that file in it, BI is going to stop it. On the other hand, I lay that at the foot of the O/S, that allows this to happen. But NT based O/S can stop this if properly configured. The overlay testing I did was with calcu.exe which came from another directory with the same file version and date and time stamp, but I think BI would stop it if it had a different version and time stamp of the one being overlaid. I'll have to check with IIS on this.

IMHO, BI is doing **EXACTLY** what it needs do be doing to protect the machine. It can stand a little improvement with outbound protection by application linked to an IP. If BI gets that **watch out**!

You know you can tell BI not to **baseline** exe(s).

Dr. **D** :)

****** AGAIN I WANT TO KNOW WHAT YOU KNOW! ******

>

> *And this makes the baselining of every .exe sensible?*

If I did a baseline and Duane.exe hit the machine that was going to deploy IOstorm.dll and register the dll in c:\windows when it executed, I want that execution of duane.exe to be stopped before it happens. I want the **clue** that Duane.exe hit the machine and I did nothing on my end that would account for Duane.exe being on the machine trying to execute. But of course that only way BI and I are going to know about this issue is because of every exe on the computer has been accounted for and is in an approved state for execution, because I did the baseline and Duane.exe was not part of that baseline.

That is also one of the ways BI is stopping the Leaktest.exe. Another clear **RED** flag that something is not right!

Dr. **D** :)

****** AGAIN I WANT TO KNOW WHAT YOU KNOW! ******

The process of protecting the machine with the baseline concept is a two fold thing with not only stopping execution of a program from running, but also to stop the program executing from phoning home.

1) The worm Duane.exe or (container program) can deploy a backdoor program like IOstorm.dll that can make the phone call home. Do you want Duane.exe to execute? Do you want to be notified that Duane.exe is about to execute?

2) The worm can disable the AV and the firewall if Duane.exe is allowed to execute. If it was not on the machine at the time of the baseline and tries to execute, do you want to be notified that it was trying to execute? Do

you want it do execute?

3) Duane.exe doesn't even need IEexplorer.exe to make the phone home call . It can make the phone home call itself. Duane.exe can use the O/S itself and make the phone home call. Do you want Duane.exe to execute? Do you want Duane.exe to make the phone home call?

>

> *Leaktest.exe, as many have already pointed out, is a sham.*

Leaktest is not a sham. It is a valid test of an application such as BlackIce's or any other Personal Firewall's ability to stop the phone home attempt. Whether that phone home attempt is being done by a dll through an exe like msmin.exe or a standalone exe such as Leaktest, which is using the O/S to make the phone home call or the subcomponent program using the O/S itself to make the phone call and not need an (exe) period.

> *You're talking in circles. I don't think you understand your own*

> *examples.*

>

What part of this don't you understand? Go back and read the post I made to *donut* about just what is happening with the Leaktest.

***** AGAIN I WANT TO KNOW WHAT YOU KNOW! *****

> *I've got 2 rules configured for my browser... inbound and outbound. This*

> *could be done with one rule, but this method allows for fine tuning.*

I doesn't look like Kerio may be the solution I am looking for, because of the rules that must be set for Application control. Like I said in a previous post, the people I am dealing with are going to run from any complicated anything and they don't want to be bothered with rulesets. That's the beauty of BI, because you can tell it to turn off Application and Commutation control letting something like Kerio have that control and BI's IDS and firewall component are still going to do their thing.

Then you can turn on the Application and Communication control and BI will protect very well in that area too. But what I like most is that BI can go very low-tech for people that don't want to be bothered with a bunch of rulesets, or BI can go complicated for someone at my level. Either way, BI gives the protection.

Oh well, it looks like I am still on my quest to find something to complement BI.

Thanks for your insight into Kerio.

Dr. *D* :)

comp.security.firewalls: Re: Firewall

I want to know what you know about BlackIce ... keep it, because I already know you don't know nothing about BlackIce.

Dr. *D* :)

--

The protection of the machine is a process and not a given!