

Re: Black Ice confesses faulty program!!!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-04/1621.html>

From: Chris L (chrisl317@comcast.net)

Date: 04/15/02

From: "Chris L" <chrisl317@comcast.net>

Date: Mon, 15 Apr 2002 13:38:09 GMT

What version of BID is this referring to?

--

Chris L

"TOYOTA MR2" <toyota_mr2@netvisao.pt> wrote in message news:1018861794.719441@newsfront1... >
FROM <http://grc.com/lt/bidresponse.htm>: "BlackICE does not currently prevent > outgoing connections or traffic except in cases where these connections are > caused by unsolicited incoming traffic, or are otherwise deemed > "dangerous/suspicious" traffic by the BlackICE program. When the user (you) > initiates an Internet connection, BlackICE assumes that you are aware of the > exchange of information, and approve of it. In most cases, this assumption > is correct (when you ask for information from a particular website for > example)." >> It's not supposed to assume anything, it's supposed to do its job!!! >> "Because the user initiates the connection with the GRC site, BlackICE will > not prevent information from being exchanged between your system and GRC, > any more than it would prevent information exchanges between your system and > any other website. (To do so would drastically interfere with your ability > to "surf" the Internet freely.) What happens is this: >> 1) You contact the GRC site and ask it to perform the "leaktest". > 2) The site asks you for certain information. This is the same information > that any other website asks for when you ask it for information (when you do > a search on Yahoo, when you download something from a friend's website, when > you ask for a price from a travel site, etc.). > 3) Your system sends the information it was asked for. (This information is > rather like confirming your "return address". It is needed to allow the > exchange to proceed smoothly.)" >> Install the program, leave the GRC.COM site alone, close ur browser and > perform the test!!! >> "We have been considering adding "User-Initiated Outbound Blocking" (which > is what leaktest is meant to check for) to BlackICE for some time. However, > no date has been set for this addition. Part of the problem is that we want > to be able to give our customers as much information about the outgoing > transmission as possible (to keep novice users from having to "guess" about > what to allow and what to block). This requires creating a user interface > that is somewhat more sophisticated than the simple interface that most > firewalls provide for this feature." >> Finally they confess they have a faulty and incomplete product that fails to > give u full protection!!! >> NOW... u can also read Gibson's reply... >> "Hi Dave, > Thanks for forwarding ISS/NetworkICE's latest response. It's a much more > thorough and clear reply than they have generated before. At one point I saw > "Trish M." quoted as asking: "Why does everyone believe everything Steve > Gibson says?" <<grin>> >> What they are essentially saying now – in your note from them – is that > BlackICE Defender responds only to outbound replies initiated from external > intrusion attempts. >> I have two problems with this: First, any good firewall will prevent > external intrusion. PERIOD. So why would there be a successful external > intrusion attempt that was able to reach some software running in your > computer in the first place? The truth is, if you don't allow a Trojan to > get into your machine then even a PC *without* a firewall is completely safe > against external attacks. It's not as if any computer can somehow be > "penetrated" by aiming a sharp pointy Internet packet at it unless you have > a firewall. That's just not the case. In my opinion, the threat from > "internal extrusion" of personal and

comp.security.firewalls: Re: Black Ice confesses faulty program!!!

private information (something inside > connecting outside) is actually much greater than from "external intrusion". > Sure, PCs on the Internet are being scanned all the time, but so what? > There's no way for them to get in – even without any firewall on a properly > configured machine. Being "Stealth" is cool, but *any* firewall does that > for you. > > Second, BlackICE is stating that they are not doing anything about "The > Spyware Problem" ... where some malicious software (malware) in your machine > decides to send stuff out or even to connect up to remote servers in order > to wait for orders. If you don't think "Spyware" is a problem for computer > users, take a look at what Google has on "Spyware" ... > > > > <http://www.google.com/search?q=Spyware> > ... and look at all of the types of Spyware now being handled by our > favorite anti-spyware program, LavaSoft's "Ad-Aware": Adware, Alexa 1.0–5.0, > Aureate v1.0,2.0 + 3.0, Comet Cursor v1.0 and v2.0, Cydoor, Doubleclick, > DSSAgent, EverAd, EzUla, Expedioware, Flyswat, Gator, Hotbar 1+2, OnFlow, > TimeSink v1.0,v2.0 and v5.0, Web3000, Webhancer, Transponder, Wnad and > more... (updated regularly) > > Finally, the ZoneLabs people who make the FREE ZoneAlarm firewall receive > about 5,000 pieces of eMail PER DAY from people using ZoneAlarm when that > bi-directional personal firewall detects something evil in their computer > trying to "phone home". By comparison, the BlackICE Defender folks probably > receive many fewer pieces of such eMail – if any at all – since, as > explained in Trish's note, BlackICE lets any such Spyware freely communicate > outbound without any supervision, detection, or blocking." > > This...in case u don't know is already 5 months old...November 8th 2001!!! > > > > > >

- *Next message:* [david56: "Re: What can be unsafe ?"](#)
- *Previous message:* [jnchew: "MSN over Firewall"](#)
- *In reply to:* [TOYOTA MR2: "Black Ice confesses faulty program!!!"](#)
- *Next in thread:* [Alexander Delarge: "Re: Black Ice confesses faulty program!!!"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)