

RE: [fw-wiz] Source of T/TCP traffic

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-09/0040.html>

From: Dave Killion (*Dkillion_at_netscreen.com*)

Date: 09/09/03

To: "'Knut Bjornstad'" <kbjo@interpost.no>, firewall-wizards@honor.icsalabs.com
Date: Tue, 9 Sep 2003 09:18:30 -0700

From what I've seen, and I could be dead-wrong, is that IIS and IE form a T/TCP bond when connecting. IE will actually try T/TCP first, and fall back to normal TCP after failing. This is how IIS-served webpages load so quickly on IE. You can tell when you're loading a non-IIS served page with IE because there's a bit of a pause while T/TCP fails.

So three cheers to Microsoft for putting this half-dead protocol on life support. ;)

Dave Killion
Senior Security Engineer
Security Group, NetScreen Technologies, Inc.

-----Original Message-----

From: Knut Bjornstad [mailto:kbjo@interpost.no]
Sent: Tuesday, September 09, 2003 4:23 AM
To: firewall-wizards@honor.icsalabs.com
Subject: [fw-wiz] Source of T/TCP traffic

Our IDS are seeing a lot of peculiar T/TCP traffic – the alerts on this is no problem in itself – I can easily disable them. But when I try to analyze the traffic, it seems like ordinary web traffic from various MS IE sources. Now T/TCP is – according to my impression – a halfdead attempt at speeding up TCP, and nothing I would associate with this kind of everyday events. My theory is that this is caused by some firewall or similar product that modidfies outgoing traffic by adding the necessary TCP option to the packets.

First question: Do anyone in this forum know of a product that does something like that (I suspect something from Checkpoint, but I am not sure about that)?

Second question: Given that T/TCP has problematic security, can ordinary firewalls handle the protocol by setting up relevant rules?

--

--Knut Bjornstad -- ErgoIntegration AS ---Oslo, Norway-----
--kbjo@interpost.no -- t:47 23 14 53 36 -- mob: 901 15 917 --

RE: [fw-wiz] Source of T/TCP traffic

Firewall-Wizards: RE: [fw-wiz] Source of T/TCP traffic

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

- application/x-pkcs7-signature attachment: [smime.p7s](#)