

Re: Probes on Port 135 and 445 continue

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-10/0312.html>

From: Moe Trin (*ibuprofin_at_painkiller.example.tld*)

Date: 10/17/04

Date: Sat, 16 Oct 2004 22:17:04 -0500

In article <MPG.1bda6c0588d983b98986e@news-server.columbus.rr.com>, Leythos wrote:

>In article <slrncn0vjt.k70.ibuprofin@atlantis.phx.az.us>,

>ibuprofin@painkiller.example.tld says...

>> *I'm curious how someone managed to educate them into such an enlightened position*

>*The Sorority has an AUP that I designed and passed through our legal department, it's the same type of AUP that we use for commercial / corporate accounts when they don't have one of their own.*

OK "imposed"...

>*Since there is no benefit to the Sorority to allowing external users to access services inside the house, such as P2P systems, there is no reason to permit it. The house has a slow DSL connection, in order to provide quality access to the largest number of users, all forms of "servers" are prohibited.*

This is more what I was asking about – what caused them to buy into it. A slow connection is a very good reason.

>*Since the network is monitored 24/7, it could be construed that the house would know of P2P activity and could be sued by the RIAA should one of the ladies start offering pirated material to the public.*

Monitored with their permission? Otherwise there are invasion of privacy issues. The RIAA has no right to monitor the connections, and could themselves be sued in the event that they did. A good landshark could make money out of that kind of stupidity.

>*The blocking of the ports, 135 through 139, 445, 1433, 1434 and 2500 was presented to the board, checked by a senior Bank IT manager against their firewall design (since a bank member is on their board), and approved without concern.*

I see no reason to have most ports below about 1030 open – that might also reduce Messenger spam. Depending, they may need 113 inbound, but I've not seen that one exploited yet. We normally forward related port 113 requests to a server running fakeidentd anyway.

*>As it is, the entire house generated about 8MB in logs per 24 hour
>period. For 40 users of the network, this is considered very small. Most
>all activity is AIM and Web related.*

What all are you recording to generate that much? That's like 100000 lines of text.

*>The monitoring also lets us detect a virus outbreak as soon as it
>happens*

Obviously would have been better to prevent the infection, but the concept is otherwise OK.

> which is how we got involved with them in the first place.

But this, I don't know how to parse. This sounds political, rather than technical.

Old guy