

Brute Force Attacks

Thursday, June 15, 2006

Written by Matt Brunk

Two guys steal more than 10 million minutes of VoIP provider's services and then resell them at ridiculously low prices. The VoIP providers remain unnamed and I'd bet that these providers are hoping to remain more than anonymous.



Escaping the perils of hackers seems to be an exception and not the rule. In the **press release from the Department of Justice** "...according to records obtained from AT&T, more than 6 million scans were initiated by the Spokane hacker in search of vulnerable network ports. During the same period, AT&T records reveal only two other users with a greater number of scans on its entire global network."

The release describes how the enlisted hacker used "**Brute Force Attacks**" to scan and probe the providers for vulnerabilities. What I don't understand is how does anyone measure 6 million scans coming from three users and something not happen after scan 100 from the same guy? Who's protecting the providers? What are VoIP providers going to do differently to secure their networks for their customers?

ISPs including the VoIP providers need to wake up. Nearly every internet pipe is a dirty connection. **Clean Pipe vs. Dirty Pipe** is an ongoing oddity. Odd in that buying more bandwidth is always the first solution to merely pay for something that you didn't want or need but get because that's the way it's always been. Port scanning disrupts bandwidth and my customer firewall logs jive with feedback from their operations staff when internet access gets slow and choppy. Firing off emails to their ISP security center makes the customer feel better but the ISP including most, do nothing especially when the offending IP addresses logged are coming from customers using the same ISP.

For users unaware here's another example of VoIP gone wild. Not only do you need to worry about what comes into your network and what goes out of your company network but you must worry about who's network and services you do use. I guess in a few months we will read about some new whiz bang gizmo that will cure or minimize this issue too. I wonder who ends up paying for that.

But these are just personal irritants and a bigger question remains. I know it can be done, it will continue to be done and in spite of what any organization or law enforcement agency says or does - the vulnerabilities in VoIP just won't disappear anytime soon. Maybe the OSI model is overdue for a forklift review and upgrade. Maybe in the next model some of the old ways of communicating will be incorporated into that process- you know things like security, authentication, and sending a few electric shocks to remind hackers and guys like me that don't know security is in place to protect us from ourselves.

Comment on this article

Leave your comments (Show/Hide Form)

Other Visitors Comments

There are no comments currently....

Close Window