

RE: [fw-wiz] Vulnerability Response (was: BGP TCP RST Attacks)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-06/0020.html>

From: Paul D. Robertson (*paul_at_compuwar.net*)

Date: 06/01/04

To: "Marcus J. Ranum" <mjr@ranum.com>

Date: Tue, 1 Jun 2004 12:49:42 -0400 (EDT)

On Tue, 1 Jun 2004, Marcus J. Ranum wrote:

> *Ben Nagy wrote:*

> >> *As I said, I think time will tell. :)*

> >*I'm horribly torn here. I completely agree with you, but I just don't see*

> >*any evidence of change. Essentially what you are claiming, when you say that*

> >*"time will tell", is that little green men from the Planet Clue are going to*

> >*invade earth with their rectal clue applicators and drag most of the IT*

> >*industry in the world off to re-education camps.*

>

> *I didn't say that!!! I didn't even *THINK* that!!*

Yeah, but admit it, you're still wishing it would! ;)

> *I *hope* that in 10 years security practitioners will look back*

> *at the days of "the system-wide patching fad" and laugh.*

We wished 10 years ago that people would look at idiots writing code and laugh, I think your timeframe is way short...

> *We're a society of fads and "get rich quick" schemes. We'd*

> *rather pay 3X as much for special food that has 1/2 the calories*

> *of normal food – instead of eating 1/2 as much of the normal*

> *food (which actually has real flavor). We'd rather follow a fad*

> *diet that destroys our body with saturated fats than simply*

> *"eat lots. work hard. burn lots of energy." We're still in the*

> *era of get.rich.quick low-carb Internet security – perhaps it*

> *will be the aliens with their clue probes that get us out of it, but*

> *it's more likely we'll either stay there or wise up.*

The nice thing about carbohydrates is that your brain needs them– I see the low-carb diet as a self-fixing problem long-term.

> *But it's the first and best place to start. If you don't do something*

> *sensible at the perimeter – or you don't have a perimeter at all –*

Firewall-Wizards: RE: [fw-wiz] Vulnerability Response (was: BGP TCP RST Attacks)

- > *then all your systems are internet-facing. We've seen how well*
- > **THAT* works, too.*

It's a new trend again though!

- > *Why do we need to wok from where we are? Where we are is*
- > *not good!!! Working harder on it may not make it better. In fact*
- > *the preponderance of evidence is that it's getting WORSE.*

Ah, but that's a civil level of proof, and we're looking at a crime! ;)

- > *I see MS doing GOOD MARKETING in attempting to*
- > *unscrew that which is permanently screwed.*

To be fair, they are making some progress in the right direction, it's just that they started on Pluto and the goal line is on this planet.

Releasing an operating system with sixty-some thousand known bugs as "ready to use" should mean hard time.

- > *NO you haven't!!! You're like the guys who want to eat 3 gallons*
- > *of ice cream a day and still lose weight using some fad diet.*
- > *Those things many people call "firewalls" are just low-carb*
- > *feel-good half-hearted nods toward security. Their policies*
- > *have been set up by committees with marketing people on*
- > *them, and their security posture depends more on which business*
- > *unit brings in more money than on actually protecting the*
- > *network. I mean these darned things allow attachments*
- > *through; they allow ActiveX through, they allow IM through,*
- > *etc, etc, etc. That's not a firewall. That's a "slow router."*
- > *And these "firewalled" networks are full of users who come*
- > *and go with laptops that they just plug in wherever they*
- > *want whenever they want and are given an IP address and*
- > *off they go. Those "mobile users" are on common segments*
- > *with mission critical servers and the only "authentication" they*
- > *use is the fact that they're physically there. Did I just describe*
- > *the typical corporate network? Can you tell me what is*
- > *"firewalled" about *THAT*!?!?!? That's not firewalled. That's*
- > *low-carb-fat-free-firewalled.*

Amen, Brother Marcus!

- > > *The trouble is that malware still gets in. Poot. Them dang worms is*
- > > *like roaches, I tell ya. Looks 'ifn that there trusted network weren't quite*
- > > *so trusted after all...*
- >
- > *Peter Neumann likes to make sure people use the words "trusted"*
- > *and "trustworthy" properly. :) That was a trusted network but not*
- > *a trustworthy network. :) oops.*

Firewall-Wizards: RE: [fw-wiz] Vulnerability Response (was: BGP TCP RST Attacks)

I still say that 90% of the problem would disappear overnight if MS removed the execute bit from Outlook's attachments. That doesn't mean we wouldn't still have problems— but there'd be a lot less of them.

Paul

Paul D. Robertson "My statements in this message are personal opinions paul@compuwar.net which may have no basis whatsoever in fact."
probertson@trusecure.com Director of Risk Assessment TruSecure Corporation

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