

Re: Req: info on IP range popup ad software supposedly called "Extreme Marketing"

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-12/0582.html>

From: Joe Schmoe (nomail@forme.com)

Date: 12/31/02

From: "Joe Schmoe" <nomail@forme.com>

Date: Mon, 30 Dec 2002 22:58:26 -0500

On Tue, 31 Dec 2002 02:00:23 +0000, Todd Knarr wrote:

- > *In comp.security.misc <pan.2002.12.31.01.05.40.224115@forme.com> Joe Schmoe <nomail@forme.com> wrote:*
- >> *Why would it be inbound? I'm talking about generating a valid IP that*
- >> *exists within your own subnet that will pass an outbound filter. The*
- >> *machine generating the packet AND the spoofed IP are both on the same*
- >> *subnet controlled by the same router.*
- >
- > *It'd depend on the filtering. I'd probably implement rules that would*
- > *prevent both scenarios. Examples:*

Todd,

Before I start in I would just like to say this is good stuff. I know this thread is getting way off track, but I haven't enjoyed an exchange like this for a while. Having said that.....

- > *1. Dial-up. The controller in the modem racks knows which IP address was*
- > *assigned to each dial-in line. Ingress filtering is applied to each*
- > *line prohibiting any packets sourced from an IP address not*
- > *associated with that line.*

Ok, this one you may have me on..... But if you can figure out which IPs are associated with which ports, there is a program called winject which forges packets for windows dialup connections. Not sure if this would do the trick...

- > *2. Ethernet. I'd pick a switch that could filter on MAC and IP*
- > *addresses,*
- > *and configure it to drop all packets on a port not from an address*
- > *that should be hooked up to that port. Depending on hubs and*
- > *unmanaged switches there may be a range of addresses usable on a*
- > *given managed port, but it should be small. For maximum paranoia,*
- > *associate MAC addresses with ports and filter on that. That makes it*

comp.security.misc: Re: Req: info on IP range popup ad software supposedly called "Extreme Marketing"

- > *impossible to impersonate another NIC at a cost in troubleshooting*
- > *when people change NICs or equipment.*

I'm pasting a part of a message I wrote elsewhere in this thread dealing with this exact scenario, it also illustrates why home users running unprotected windows systems are especially sweet targets;

Begin pasted quote-----

But as someone else in this thread pointed out, your MAC address is also included in your packet headers... Furthermore, mediaone could have MAC binding enabled in the router so it will not allow packets to pass in which the ip address and MAC address contained in the packets headers do not match it's table of assigned MAC/IP pairs.

Still not a problem... I simply scan my subnet for boxes with port 139 open, then I can peruse my scan logs and pick a target. Once I decide on a target I just do a nbtstat -A <ip address>....

Now, not only do I have your IP, but I also have your MAC address. I can now forge perfectly acceptable packets that will pass through the router unmolested and cannot be traced back to me, they will all point back to you or whatever target I selected.

end pasted quote-----

- > *3. Cable modems. The CMTS knows the IP address assigned to a given cable*
- > *modem, and it's a bitch to forge the CM serial number. Configure the*
- > *CMTS to kill any modem sourcing packets from anything other than the*
- > *addresses properly assigned to it.*

Yeah, it depends on the cable co. where I live now this is how they do it. But in my old town, they bound it to the PC's NIC instead, I'm sure they still do it this way as it's been less than a year since I moved.

Joe.