SECURITY NOW!

Transcript of Episode #8

DDoS Attacks

Description: Distributed Denial of Service (DDoS) attacks are occurring with ever-greater frequency every day. Although these damaging attacks are often used to extort high-profile gaming and gambling sites before major gambling events, attacks are also launched against individual users who do something to annoy "zombie fleet masters" while they are online. Some router and firewall vendors claim that their devices prevent DDoS attacks. Is that possible? What can be done to dodge the bullet of a DDoS attack launched against you while you're online?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-008.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-008-lq.mp3

Leo Laporte: This is Security Now!, Episode 8, for October 6, 2005: DDoS Attacks. Steve Gibson from GRC.com is on the line with Google Talk. Hello, Steve in Irvine, how are you today?

Steve Gibson: Hey, Leo, great to be back.

Leo: This is something you're an expert in per force, denial of service attacks, because you've been the victim.

Steve: Well, and how. It was a number of years ago. Some dialogue in our newsgroups upset some young hackers who had access to one of these fleets of zombies which are infecting end-user machines and just blew me and GRC.com completely off the Internet for a number of hours. And it was a real problem for me. That was my real first, you know, literally firsthand experience being on the receiving end of a distributed denial of service attack.

Leo: Let's first explain what a simple denial of service attack is.

Steve: Well, the idea is, any kind of packet traffic which can cause problems for the receiving end can create what's called a "denial of service," you know, the term meaning, of course, that whatever service you are trying to get is being denied you by someone, for whatever reason, who wants that to happen. So, for example, in the old days, websites used to have their web servers brought down by people doing something called a "SYN flood," S-Y-N. A SYN packet is the first packet of a TCP connection. When a user's browser, for example, wants to connect to a web server, it'll send a SYN packet. The web server allocates some resources to get ready for this connection, sends back what's called a SYN/ACK packet, and then a final ACK packet is returned to the server. What that does is that verifies the communication path between these two endpoints, the user's browser and the server, and sort of establishes the communication.

Well, if the browser or an end-user being malicious were to do nothing but send SYN packets just by themselves, the server would keep allocating all these resources, thinking that all these connections, like, wow, I've become really popular all of a sudden, as if all these users were wanting to connect to it. Well, what happened is that, before long, that server would run out of resources. It would sort of be like creating a memory leak. It would burn up all of the memory that it had allocated for accepting connections, and then regular users who were actually trying to connect would send their own SYN packet, which would end up getting dropped or ignored because the server thought that it was already too busy receiving real connections. So that was sort of the original denial of service attack against a web server.

Leo: So let me put it in baby talk. In baby talk, somebody basically sends so many requests to your - phony requests, but requests - to your website that you spend all your bandwidth trying to handle them and can't handle legitimate incoming traffic.

Steve: Well, actually, that's the second-generation denial of service attack. This first one actually consumed resources on the server...

Leo: Oh.

Steve: ...so that the server was no longer able to accept connections.

Leo: Oh, so the SYN is simply setting up a server connection, and that just uses up all the memory and the processor bandwidth on the server itself.

Steve: Exactly.

Leo: Oh.

Steve: It uses up memory and processor bandwidth, not the connection bandwidth.

Leo: Got it.

Steve: And so what was really interesting...

Leo: The upshot's the same, though, the server's too busy, doesn't have the resources to respond to normal traffic.

Steve: Exactly. However, it's not the bandwidth which has been consumed.

Leo: Got it.

Steve: It's the resources on the server.

Leo: Right.

Steve: And the reason that, well, we'll see why that's an important distinction in a second. Because, for example, just one guy sending SYN packets could have brought down and did bring down historically some major websites, just one computer sending SYN packets.

Leo: I remember this happening to Yahoo! some years ago.

Steve: And that's what that was.

Leo: Yeah.

Steve: Exactly.

Leo: Yeah.

Steve: Now, what happened was servers got smarter. Servers started being this denial of service attack aware so that they would, if their queue of pending connections got full, they'd start throwing away the oldest ones that hadn't come back and completed that three-way handshake. And so basically systems got resilient or able to protect themselves against this kind of attack.

Leo: How many different SYN requests would you need to bring down something like Yahoo!?

Steve: Only a few thousand.

Leo: So it's an easy thing for an individual to do from a single computer.

Steve: Yes. Well, now, once upon a time it was an easy thing. Now virtually all servers are hardened against that kind of attack.

Leo: So they just have a queue, and they just start dumping stuff at the bottom as new stuff comes in from the top.

Steve: Exactly.

Leo: Yeah.

Steve: So what then happened was we went from a DoS attack to a DDoS attack, to a distributed denial of service attack. And this is where this notion of zombie fleets come in, the idea being that malware has infected a large population of computers, maybe a hundred, maybe a thousand. There are some fleets that are apparently tens of thousands of end-user computers that are slaved to a single or a small group of zombie masters. In this scenario, this large group of computers are all told to attack a single end-user, whether it's a website or an individual. And so what happens is this distributed set of machines all start sending traffic. It doesn't even have to be, in this case, a SYN packet.

And, in fact, I was not attacked with a SYN flood. I was attacked just with good old pings, just enough ping packets, the so-called ICMP. What that did was it flooded my bandwidth so that my connection to the Internet was congested. And that's the scenario that you were talking about where, if enough of these, like, you know, several hundred machines were all pinging my web server at the same time, then normal bandwidth trying to access my website was no longer able to get there.

Leo: So they choked - the difference is they choked the pipe, not the server.

Steve: That's exactly right.

Leo: The ping of death.

Steve: So anywhere that you had a choke point in the bandwidth - and it might have even been, like, a router upstream of me. Because the idea is that packets are flooding in from all over the Internet, and they're sort of converging. You could think of it sort of as a convergence down to a single point. And, in fact, an analogy that I've used is, if you put your hand out in the sunlight, you know, it feels fine. It's warm, you know, hands were meant to handle sunlight. That's no problem. But if you take a magnifying glass and hold it over your hand, focusing essentially that same amount of sunlight down to a single point, suddenly you start seeing a little smoke and some charred flesh because that same amount of sunlight is now focused down to a single point. Similarly, Internet traffic. If it's focused to a single point, all being directed at a single target, that target's just gone. It's off the Internet.

Leo: So how do we fight a distributed denial of service attack? Can we just ignore pings?

Steve: Well, what happens is that - well, in fact, that was one of my first defenses was I asked Verio, I said, you know, it's nice to be able to ping me and to run a traceroute to see if GRC's around. But, gee, I'm being attacked. I'm being flooded with all this ICMP traffic. Let's block that. And so Verio, my supplier at the time, blocked that and prevented the attack from getting to my server. The problem is that now - and this is really a problem today - these tools have become increasingly sophisticated, so that attacks then started using this TCP traffic, the so-called SYN packets. Well, I can't and couldn't block those because those were the packets that valid users, you know, valid users didn't need to ping me or to do a traceroute. They needed to connect their browsers to my web server, and to do that they needed to use this TCP SYN packet. So I was unable to filter those or to have my ISP block those to keep those from getting to my computer, or nobody would be able to.

Leo: You could block them, but you were off the 'Net, yeah.

Steve: Exactly. We were off the 'Net again.

Leo: So how many different servers are we talking about in a distributed denial of service attack?

Steve: Well, I've seen small - small zombie or bot armies are several hundred, maybe four or five hundred. And they even get up to the several thousands.

Leo: Could you set some sort of automation that, when it saw a certain number of SYN packets from a single IP address, that it said, we're going to block that IP address for five minutes or ten minutes?

Steve: Ah, well, now, that's another good point, is the other thing that these packets are doing is that they're spoofing their source IP. When a legitimate packet comes to a server or to an end-user, it identifies who sent it, that is, by IP address, and what its destination is. The destination IP gets it to you. The source IP is the IP to which you send the return traffic. So the packet has to have both. In these denial of service attacks, the source IP is being randomized on purpose so that you really don't know if it's legitimate or not.

Leo: You couldn't block anything.

Steve: So you may never see two packets from the same source IP.

Leo: This can be done on zombie computers, thanks to the raw socket support that was built into Windows XP.

Steve: That's exactly right.

Leo: I mean, raw sockets exists on UNIX and Linux and so forth. But because Windows XP is so prevalent, and a zombie attack has got to take over a bunch of unsophisticated computers, they make a natural platform for that. Is it better now that Microsoft's taken out raw sockets?

Steve: Well, it's better, except that we still have the ICMP attack. And one of the things that I've received a bunch of questions about is what does an end-user do when they're attacked? It's one thing for, like, major websites to be attacked. But, for example, end-users will be involved in an online chat or an online conference, or maybe they're, like, doing online gaming. Whenever a bunch of people are hooked to a game server, their IP has to be known. That is, the IP address of everyone on this game server needs to be known because that's how the game server is able to exchange traffic with you. So what can happen is that, one way or another, or for whatever reason, somebody upsets somebody else on the Internet. You know, they get pissed off because they're blasting them or...

Leo: Happens all the time.

Steve: ...they say something that upsets somebody else. And before they know it, they're now under attack. And it actually does happen all the time. End-users who have one way or another upset somebody else on the Internet find themselves, an end-user, a single person, the victim of a denial of service attack. Basically they're just blasted off the Internet.

Leo: Many people have asked me about this. It happens a lot with instant messenger clients, where they'll get flooded with a lot of requests to message. Or, yeah, a game server, you could get pinged to death. There are all sorts of ways to do this. Is there a way to protect yourself?

Steve: Well, there really isn't. You don't have the ability to filter. You know, you can't call AOL and say, hey, AOL, I want you to block this stuff from my connection.

Leo: Well, you can turn off pings in the router, though; right?

Steve: Well, yes. The problem is, by the time it comes to the router, it's already clogged your connection.

Leo: Because your connection is upstream from you, yeah.

Steve: This connection clogging is the real problem. And, in fact, it's one of my complaints with router manufacturers and some residential firewall manufacturers who say on the box that this will protect users from denial of service attacks. That's the other question that I get a lot is people saying, hey, should I buy this router that'll protect me from a denial of service attack? It won't. It can't.

Leo: Well, it technically is protecting your router from the denial of service attack, and what's inside the network. But it doesn't protect you upstream, so it doesn't matter.

Steve: Well, exactly.

Leo: I mean, it's not a lie, it's just that it's ineffective.

Steve: What the router can do is the router can see that there's a whole bunch of traffic that is being aimed at one of the computers behind the router. The only thing it can do is to block that traffic.

Leo: Right, right.

Steve: So it's not like...

Leo: But the traffic's still coming down your pipe, it's just getting blocked...

Steve: Well, exactly. So it's not like the computer can still be accessed. The computer is not being attacked. But it's also off the Internet.

Leo: It has no Internet access.

Steve: I mean, it's got no connectivity because the router had to shut off any traffic going to that computer. The only way it can protect it is to disconnect it.

Leo: Well, is the only solution not to piss off people in games, or what? I mean...

Steve: That really is the truth, Leo. That's the only thing you can do. Now, the other approach is to somehow, if possible, change your IP. It's trivial for a dialup user to change their IP because every time you connect to the Internet through a modem, you're going to be assigned a new IP. It's much less easy if you're a DSL or a broadband user. Most...

Leo: This is interesting. It means you probably shouldn't have a static IP address unless you've got a web server or some other reason to do it.

Steve: Well, yes. And, in fact, if you disconnect your router from your cable modem, or even more significantly, maybe unplug your cable modem - say that you're an end-user. You've upset somebody on the Internet for whatever reason in an IM chat or on online gaming or something. And now you're suddenly - your light's on constantly, you've lost your connection to the Internet. If you disconnect completely, that is, not just your computer from the router, but you want to actually unplug the router, probably power down the cable modem, and wait a while...

Leo: Don't do it right away because they'll just give you the same IP address back; right?

Steve: Yes, that's exactly what happens. The router identifies itself by its MAC address. Now, that's one other thing you can do is many routers now allow you to either user the router's own MAC address or to specify a MAC address. That's done because some cable providers lock your subscription to the MAC address of your computer. So the router needs to be able to clone the MAC address. If your provider is not requiring that you not change your MAC address, you can change it. And that will trick your ISP into allocating a different IP address for you when you reconnect to the Internet. And the point is, these attacks are not aimed at you, like at your equipment, in any particular way. They're always aimed at your IP. So if you can arrange to change your IP address, either by disconnecting completely for a few hours, when you reconnect you'll probably get a new IP. Or if you can trick your router into pretending to be a different router by changing its MAC address, then again, your ISP will give you a new IP, basically a clean IP.

Leo: They're not going to want to do this, of course, because it's not helping them. They're just going to give that IP, the bad IP to somebody else, and the problem will just be spread around, so...

Steve: Well, in fact, that's something that happens also. Sometimes users will hook up to their broadband provider, get a new IP, and that IP is under attack from the person who had it before, they were under attack. Now you get a new IP. Or, for example, sometimes I know that it may be that the user before was very active with file sharing. This was happening a lot in the Napster and the Kazaa days, where you would get a new IP, and suddenly you were getting all this inbound traffic from other peer-to-peer users who thought you had the file that they wanted, trying to get the file from you because whoever it was who had the IP before, you know, that's what they were doing, and now you've got their IP.

Leo: This sounds like something we have to solve in the long run, that there's a structural flaw here.

Steve: It is a mess.

Leo: There's no solution, though.

Steve: The problem is, this has all sort of evolved over time.

Leo: Right.

Steve: These are very new problems compared to the technology of the Internet, which has now, of course, a vast infrastructure keeping it from changing.

Leo: So the bottom line is, try not to annoy anybody on the Internet. Don't attract attention. If you can change your IP address, it's probably a good idea to change it periodically. Maybe look for an Internet service provider that gives you that capability. And if they have a large enough pool of addresses, you should be able to report a problem with an address, and they could put it on the shelf for a while, and pull it out of circulation.

Steve: I would say that, in general, for people who are really security conscious, if they can disconnect their cable modem and their router, power down the router, just from time to time, maybe if you know you're not going to be using your computer, like, all day Sunday, just turn the power off on your cable modem and your router, let them sit for a day. Chances are, when you turn them on at the end of the day or the next day, they'll come up with a new IP. And it's just sort of a good idea to change it from time to time. It's really not the case that your IP can ever be super stealthful and secret because, for example, most people will find that their email address contains their IP as a consequence of the way that the information has gone from their email client to their ISP. So it's not, you know, something that it's really possible to keep super secret. But changing it from time to time really does make sense.

Leo: Let me just raise this, and it may be a dead end, but I use a service, it's essentially a proxy server. It's a security service called iPhantom. And it anonymizes my IP address to their IP address. Any attacks, any time I'm online, if I'm on BitTorrent or whatever, I appear to be coming from that IP address. Would that be an effective solution?

Steve: That would be an effective solution. Basically you're using them as what's called a "proxy" in order to route all of your traffic through them. Then their IP is the only one that's going to be visible. If you disconnect from them, then later reconnect, chances are you'll be coming out of a different pool of their IP. And I would imagine that someone like that has all kinds of defenses that they've already got in place upstream that are much more than your provider provides to you.

Leo: Right. I mean, that's their business. That's one of the things they really ought to do.

Steve: Right.

Leo: Well, it sounds like the other message that probably consumers should get is, if you see on the box "protects against," you know, "ping attacks, protects against DoS attacks," that's not true.

Steve: No. That's exactly right. And I'm glad that we've made this very clear because it's an annoyance that these vendors are claiming, I mean, they know that people are concerned about being attacked on the Internet, about these denial of service attacks, so they're putting it on the box. But if traffic is flooding your connection, there's nothing the box at the receiving end of the flood can do to get out of the way.

Leo: It's too late.

Steve: The only thing you as an end-user can do is dodge that bullet by one way or another arranging to change your IP address. And, you know, you may want to change your online gaming name or whatever it was that caused you to draw this fire because, of course, if you just reappear in the same environment with the same name, even if your IP has changed - and this has happened a lot - people will attack you at your new IP.

Leo: And in addition, if you're using - if you're being attacked over instant messenger, for example, being flooded with IM requests, nothing you can do about that either, really, because you have to let those in; right?

Steve: Well, exactly. And the IM system will automatically pick up on your new IP if you maintain the same username in the IM system. If you change your IP and then reconnect into the IM system, your new IP automatically gets passed in so that you're able to receive that information.

Leo: So you can't run - you can run, but you can't hide.

Steve: That's exactly right.

Leo: Steve, it's fascinating. The ins and outs of denial of service attacks, both the original DoS attacks and the newer, scarier DDoS attacks. And one more reason why people should also update their operating systems, run anti-viruses, and try to keep their system from being one of the zombies that's being used to attack others.

Steve: Oh, absolutely.

Leo: Yeah, I mean, that's another way we can practice some hygiene on the Internet.

Steve: Being good citizens on the Internet.

Leo: Steve Gibson is at GRC.com. Information about all of our Security Now! shows, including small 16-bit downloads for those of you on a dialup or with smaller storage devices, and transcripts for those of you who like to read while you listen, are available at GRC.com/securitynow.htm. Our thanks to AOL Radio at aolmusic.com for providing the bandwidth for Security Now! so that we can offer this absolutely free. And every Thursday we'll be back with yet another Security Now!. Steve Gibson, thanks for joining me.

Steve: Always a pleasure, Leo. Thanks.