Internet Weaponry

Description: Steve and Leo trace the history and rapid growth of Internet Denial of Service (DoS) attack techniques, tools, and motivations over the past eight years. They discuss many different types of attacks while focusing upon the distributed bandwidth flooding attacks that are the most destructive and difficult to block.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-047.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-047-lq.mp3

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 47 for July 6, 2006: Internet Weaponry. Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

Steve Gibson and his magic moustache are back on Security Now!. Somebody suggested, you know, we have those little pictures of ourselves next to each posting on the This Week in Tech website. And I wink, and Alex's eyebrows go up and down. And somebody suggested we should get your moustache to go up and down.

Steve Gibson: Well, I'll tell you what's happening to it is it's turning more gray.

Leo: We could fix that. We can ungray that. We have the technology.

Steve: First I was thinking, that might be toothpaste. But no, it's definitely not toothpaste.

Leo: Or one of those milk moustaches. Well, I will – Nitrozac & Snaggy of the Joy of Tech, wonderful Joy of Tech comic strip, do these for us at JoyofTech.com. And I'm sure I can get Nitrozac to maybe put a little more black, do a little Grecian Formula in your...

Steve: I don't mind being unretouched. It's fine.

Leo: You're not as gray as the picture, actually. So we'll have to fix that.

Steve: Okay.

Leo: Yeah. So today we're going to talk about, I think, a fascinating subject. You call it "Internet Weaponry."

Steve: Well, yeah. I want to talk about botnets, as they're called, and the evolution of true Internet weaponry, which is unfortunately what exists today on the internet. And it is highly effective.

Leo: Much more effective than Kim Jong-il's missiles. Unlike them, they're aimed – this Internet weaponry is aimed at you and me and everybody who uses the Internet.

Steve: Well, it's aimed at anyone that the controllers of the weaponry choose to aim it at. It's extremely difficult, if not impossible, to hide. And it has unlimited range, until Kim Jong-il's missile that lasted for 35 seconds and then sputtered out.

Leo: So when you say "Internet weaponry," what are we talking about?

Steve: Well, this all began about eight years ago, sort of toward the end of '98 and in 1999, with sort of the general prevalence of the 'Net and machines on the 'Net. The very first recorded attacks were UNIX-based machines in a network where – because always the idea was that you needed to generate a lot of bandwidth. Now, attacks have increased, and we're talking Denial of Service attacks, using a lot of packets, Internet packets, basically to swamp either the receiving machine or the machine's connection to the Internet, the idea being that any given Internet connection has a certain speed. You know, a modem is 56K; DSL might be 384K; cable modems, you know, maybe you're able to receive, for example, a megabit. But whatever that rate is, that sets basically the total amount of traffic that is able to fit down that connection at any given time. So if more than that amount of traffic is being sent into sort of like the front of the connection, and the connection is only able to carry a certain amount, some percentage of packets will be dropped.

The router that's trying to saturate and force as much data down the connection, whatever its speed, the router's own buffers will overflow, and its strategy is simple. I just drop what I can't send. And as we've talked about in prior episodes, the Internet's protocols are robust in the face of dropped packets because it's understood that this is all very, you know, routers forward what they can in the best direction they know how to, but packets will get lost. And so the TCP protocol has a whole acknowledgment system and a retransmit logic. Protocols like UDP that don't have that built in, their applications, like DNS, know to resend a request if it hasn't received a response. So the notion of packets being dropped is something that the Internet can deal with.

The problem is, if somebody, for example, were flooding a DSL connection that can handle 384K, if they were flooding it with 384 megabits, that is, a thousand times more than it can handle, then there's very little chance, one in a thousand, for your good packets, that is, the valid packets you would like to receive down your DSL connection, there's very little chance for them to compete against this flood of attacking packets. And, you know, the attacking packets are nothing really but too many. There are just too many of them. And the router has no way of knowing, in a properly designed attack, which packets you want and which ones you don't. They all look the same to a router. So it just, you know, it just sends what it can onward and drops the flood, basically.

So it's not that the denial of service attack is all getting through to you and, like, overheating

your DSL modem or something. It's that you see a denial of service because the valid traffic can't compete, statistically, against this flood of attacking traffic which is trying to get through. So backing up a little bit...

Leo: Essentially it's a bottleneck, really.

Steve: Exactly. It is a bottleneck happening somewhere.

Leo: Yeah, okay.

Steve: And the other troubling thing about this is that modern denial of service attacks, so-called DDoS, the first "D" standing for "distributed," the idea is that thousands, and in fact today even tens of thousands, of machines scattered far and wide across the globe are being controlled centrally, and all instructed to launch their traffic, some attacking traffic, towards a certain point.

Leo: So that's the key. Because otherwise, if you just had one machine trying to do this, it wouldn't have enough bandwidth to really flood the opponent.

Steve: Well, that's a perfect example. For example, say that somebody on a cable modem was attacking – some one person on a cable modem was trying to directly attack some other person on a cable modem. Well, as we know, cable modems tend to be asynchronous – asymmetric, rather – bandwidth. You can download maybe a megabit, but you can only upload maybe 250K, or 256, so like one quarter of that. So the idea is, if one person were trying as hard as they could to attack another, well, their maximum upstream or outgoing bandwidth would be 256K, or 250K, for example, a quarter of a megabit, which is one quarter of what you're able to download. So you could accept that attack down your connection and still have three quarters of a megabit, that is, three quarters of your total bandwidth, available to you for valid traffic. So you might notice that, boy, you know, my cable modem or my DSL modem light used to be flickering, or normally flickers, now it's on steady. But you would still be able to use your Internet connection because it wouldn't be flooded, and your traffic would be able to get through.

And even if now, say, four attackers combined their bandwidth, and they were each a quarter megabit, well, now there'd be one megabit of attacking traffic competing with potentially one megabit of your valid traffic. And you'd probably – it would feel like a slowdown. It would feel like, okay, something's wrong somewhere. We don't know where or what, but boy, my connection is smoking. But I'm still sort of still connected to the Internet. So the idea is it's a matter of scale. It's a matter of how big the flood is that is competing with valid traffic.

Leo: I'd also like to just point out, because we've got a couple of emails about last week, that we're talking a particular denial of service attack, a flood denial of service. There are other denial of service attacks...

Steve: Yes.

Leo: ...where you take advantage of exploits or holes. And that wouldn't require the same amount of bandwidth. That would just – in fact, as somebody pointed out, you could do it

with an attack every five minutes because it would bring the machine down each time.

Steve: Well, I saw those postings over on the TWiT site, also. There was one, I mean, that posting brought up a very good point, which you've just made, which is that there are attacks which are not about floods. The classic one I just love. It was called the Ping of Death. And it was a fault in early versions of Microsoft Windows where, if you sent it a ping, if you sent the machine a single ping packet where you had spoofed the source IP to be the same as the destination IP, that is, you sent a packet that said this is a ping from you to you, the machine exploded.

Leo: Not literally.

Steve: Not literally, of course. But, I mean...

Leo: Windows didn't like it very much.

Steve: But it's so funny, well, because it tried to reply to itself.

Leo: Right.

Steve: And it didn't under- and it got in a total loop, and the stack got unhappy, and the processor performance went to 100 percent utilization, and basically the system just ground to a halt completely because, at a very low level in the operating system, it was continually trying to respond to its own ping, essentially.

Leo: Yeah, there are numerous attacks like that. But we're talking about the denial of service that comes from basically a flood.

Steve: Well, yes. And the problem with those other types of attack is they've all been resolved over time.

Leo: People fixed the holes. They fixed the flaws.

Steve: Exactly. For example, Microsoft realized what was happening, and they fixed the problem in their stack that would cause that to bring the system down when it received one bogus ping packet. And, I mean, and there are many other types of, I mean, very tricky, sophisticated, very clever attacks in the past. The original denial of service attacks against servers were not bandwidth attacks per se, they were TCP protocol attacks, the so-called SYN flood. What happened there was that, as we've talked about TCP connections before, the first packet to arrive at a server is a SYN packet, short for synchronize, which is the client saying and requesting a connection with the server. The server sets up some resources at its end to accept the connection, then sends back a SYN/ACK packet to acknowledge the receipt of the SYN and to send its own synchronization information to the client. And then the client responds with a final third packet, which is called the three-way TCP handshake.

Well, the fact that the server receiving the single SYN packet allocates a bunch of resources,

that is, memory allocations on its end in order to begin to set up and get ready for the connection, clever hackers figured out, hey, what if we just send a whole bunch of SYN packets to the server? It's going to end up expecting a whole bunch of connections which never arrive because we're not actually establishing a TCP connection. We're just saying we are. And so even with relatively low bandwidth, the early servers, which were not hardened against this kind of attack – as virtually all servers are now, I mean, Windows XP has this built in. It turns out that Linux and now UNIX are getting this technology, where they're much smarter about what resources they allocate upon the initiation of a TCP connection. So it's not any longer possible to bring servers down with a relatively small trickle of SYN packets. So really...

Leo: Not that some other exploit might not come along. I mean, there's plenty of bugs still to be found, no doubt.

Steve: Oh, absolutely. And so, you know, you're right, there...

Leo: That's one down, but there may be more.

Steve: There could be anything else.

Leo: Right.

Steve: But the evil elegance, if you will, of what happens with a true flood is that they're just, I mean, it's fundamentally overloading the Internet's way of operating.

Leo: And there's no way to defend because it's not a flaw in the Internet. It's taking advantage of the way the Internet is supposed to work.

Steve: Correct. In fact, an analogy that I like that I think I've used here when we were talking about this briefly before is a magnifying glass. If you put your hand out in the sunlight, it feels fine. It feels warm, you know, not a problem. Hands were designed for the sun.

Leo: Right.

Steve: And so putting it out there's not a problem. But if you hold a magnifying glass at the right distance over your hand, the same amount of radiation from the sun that was beforehand covering – well, beforehand – which was previously covering your entire hand, is now focused down to a single point. And now you've got a problem.

Leo: Yeah.

Steve: That hurts a lot. You've got, you know, burned flesh and blisters and other horrors, just from taking that normal amount of sunlight and focusing it on a point. Well, I love the analogy because it really fits with the Internet. There's, you know, 10,000 computers are not causing anyone any problem when they're all just surfing the web and browsing around and uploading and downloading files. But if those same 10,000 machines all do the same thing, that is, all focus their attention down to a single spot, that spot is in trouble. And of course the non-

malicious sort of corollary to this is the so-called "slashdot," where, you know, I don't know if it's even still so true, the...

Leo: Now it's called the "digg effect."

Steve: The digg effect.

Leo: But it's the same idea, yeah.

Steve: Exactly. It's where, you know, a whole – some highly popular site refers to some other site, and so suddenly that server is overwhelmed by valid users, too many valid users, who all want to bring up the same pages at the same time, and there just isn't enough power in the server or bandwidth in the connection or whatever. And so, you know, you're digged or slashdotted or something.

Leo: Right, right. So there's a legitimate attack. I mean, not attack, but it's legitimate traffic, so you can't say no.

Steve: True. Well, and so back from about '99 is where we began to first see this happening. There was a youngster, 15 years old, named Mafiaboy, in...

Leo: Ah, yes.

Steve: And remember the name well because it made a lot of press at the time. And this was really the first indication that the world had that, you know, things were not quite as good on the Internet as we thought. In February he attacked Yahoo! and brought Yahoo! down, and Dell. And you remember eBay going offline? Amazon.com was hit, as was CNN. And...

Leo: One kid did this.

Steve: One kid. And it was estimated he caused about $1.7 billion of damage...

Leo: Wow.

Steve: ...overall from bringing these serious ecommerce sites that really depend upon being on the 'Net in order to function.

Leo: Every minute down costs them money, big bucks.

Steve: Yes.

Leo: Did they catch him? Did they find out who he was?

Steve: Yep. He was in Montreal. He ended up pleading guilty to 55 counts of criminal charges and served eight months in a youth detention center.

Leo: Not enough.

Steve: And I don't know, but I would imagine, very much as was the case with Kevin Mitnick, that he's probably not allowed to touch a computer these days.

Leo: Either that or he's got a very good job with a security firm.

Steve: Yeah. Well, and so...

Leo: Or both.

Steve: So those, of course, were the – and so now we're talking six and a half years ago that, you know, these really high-profile attacks brought to everyone's attention, you know, that this could really happen. The other thing that happened was these attacks brought it to a much wider attention of other young people on the 'Net, you know, so-called "script kiddies" or, you know, young hackers who were often using IRC. IRC Chat was like a place where they hung out and talked and told stories and, you know, swapped software and URLs and things. And there's a funny – the way IRC works – IRC stands for Internet Relay Chat. The way it works is that you can often have a channel operator, an IRC channel operator, who's sort of like the ruler of the channel. And that person is able to kick off, just unilaterally kick off or ban anyone that they want to because, you know, they're in charge of the channel. Well, that caused fights among teenage...

Leo: Oh, yeah.

Steve: ...hackers...

Leo: Still does.

Steve: ...who were, you know, exactly, who were not appreciating being knocked off of their connection. So there were little squabbles that would form in IRC. Well, what ensued was the development of sort of the first personal denial of service attack tools, the so-called "bots," which these young programmers would develop, often writing them in Visual Basic or sometimes in C, there was source code floating around the 'Net that they could use to sort of get started. And so it was what they did after school was to build these – basically these bots whose purpose was to attack, typically, other people on IRC. Because if you are disconnected from IRC, you lost your privileges.

Or the way IRC works, it's a network of servers. That's why it's called Internet Relay Chat. The servers will relay messages from one server to the next. And turns out that, if a server is attacked, it will split the network. There aren't redundant connections among servers. So if one

server is attacked, it can fragment the so-called IRC channel, and you can end up with a server that doesn't have any leader on it. You then join that server, stop the attack. And the way the IRC protocol works, when the servers reconnect, they merge the users, and briefly you will have two operators, allowing one to kill the other.

Leo: Oh, man.

Steve: So what happened was, I mean, there really became this culture of blasting each other off the 'Net in order to sort of play king of the hill within these IRC domains, which became important social structures for young kids who were, you know, hanging out on IRC in the afternoons after school and in the evenings.

Well, one thing led to another, and then it became, okay, my bots are stronger than your bots. My, you know, my bots can – I can blast off anyone off the 'Net, and so on. Well, the problem is that, as we've seen before, what you need in order to have a strong attack is more bandwidth. More bandwidth means more machines. So the second order phenomenon that then began to happen was that this bot code was then stuck in viruses, actually installed through IRC using very powerful scripting languages. Naïve IRC users would ask for help, and somebody would give them instructions that would in fact download a Trojan, which is really what these programs are. These bots are Trojans. They would download these Trojans into their machine. So one way or another, the motivation was to spread one person's bots out on innocent victims' computers, as widely and with as high a concentration as possible. So that became the next game was seeing how many bots you could get in a so-called "botnet," or bot network.

And again, the sole purpose of these things at this time – and this is before these Trojans and bots became spam sending, that happened afterwards – the sole purpose was to generate a bandwidth flood aimed at a single point that would blast typically someone else in IRC off of IRC. And the other really interesting thing about this is that the bots themselves used the IRC system, and in fact today they still do, in order to receive instructions. The idea would be that the bots would be built with some domain name in them. And someone running a botnet would create a – would use a dynamic DNS system in order to – essentially in order to cause all of his bots, using whatever domain name he'd come up with, to connect to a server at a certain IP.

The tricky thing is since – as we saw before, IRC is Internet Relay Chat. The perpetrator, or the master of this fleet of zombies, doesn't himself need to connect to the same computer or the same server. He just connects to Internet Relay Chat and connects to the same channel, and all of his commands will be sent anonymously, relayed from one server to the next. Well, this is what's made it so very difficult to track the operators of these networks down because, I mean, it's very much like email, which is relayed from one email server to the next. However, in the course of email, of course, each server appends headers, as we've seen, in order to allow you to backtrack where your mail came from. Not so with the Internet Relay protocol. So it's extremely difficult to find out who's behind a fleet of bots.

Leo: If you were going to invent, really, a service, an Internet service that was designed for hacking, from everything you've told me so far, it'd have to be IRC. I mean...

Steve: Yes.

Leo: ...it's just the perfect test tube for all this stuff.

Steve: Yes. And it's really phenomenal when you look at it from that light. I mean, as you said, Leo, it is a perfect – it's a perfect medium for, first of all, for creating anger among people.

Leo: Right.

Steve: You know, who are then...

Leo: And, you know, and everybody knows everybody's Internet address.

Steve: Yup.

Leo: I mean, it's really remarkable.

Steve: Exactly. And in fact the protocol, the IRC protocol is documented in some RFCs, although no server really follows it completely. But then what's happened is very powerful clients – mIRC is one of the most popular IRC clients – very popular and very powerful clients have arisen, which you're able to do scripting to. You can customize it. You can do all kinds of things. And in fact there are benign bots within IRC that are used...

Leo: Oh, yeah.

Steve: ...for good purposes.

Leo: I have a Leo bot. We use bots frequently in various chatrooms I've been part of.

Steve: Right. I mean, it absolutely makes sense to have a presence there and maybe, like, have an autoresponder bot...

Leo: Exactly.

Steve: ...that will send back a message when it receives one. So what we have now, and what has evolved over time, are very large bot networks. And, I mean, truly, tens of thousand networks large. And I have had the privilege, sort of, I guess it's a privilege, to get involved in this years ago when GRC was originally attacked, the very first denial of service attacks which were launched in exactly this fashion. I ended up, you know, spending a lot of time reverse-engineering this, figuring out how it works. I remember surreptitiously joining, after reverse-engineering a bot that I received, surreptitiously joining the channel that this fleet of bots were in, and just watching them. When someone joins an IRC channel, they're basically announced as coming. And when they leave, they leave. Well, if you just sit here watching one of these private bot network channels...

Leo: It's chilling, isn't it.

Steve: ...you constantly, yes, you constantly have new machines announcing themselves, joining the network, and other machines leaving. And so what's happening is some...

Leo: And this is all automated. I mean, there's no human involved at all. This is...

Steve: Correct. Well, exactly. Somewhere, someone, some innocent person turned their computer on and connected it to the Internet. And behind their back, this Trojan that had been installed through some actions they took, whether it was surfing to a website, exploiting known security vulnerabilities, opening an email attachment, I mean, every conceivable way of getting software in, I mean, this was sort of the first spyware, or really malware, that was aimed really targeting people's machines. I mean, the whole commercial side, the Ad-Aware and adware stuff, the, you know, CoolWebSearch and all those things, those ended up sort of happening around the same time. But this was purely malicious in intent. And all the techniques that the young hackers could come up with for getting this stuff installed in people's machines is what was used. I mean, so that individual hackers would have tens of thousands of machines that their own customized version of this bot Trojan had infected. And so at any given time, some percentage of those total number of machines that were carrying that Trojan would be online and automatically logging themselves into this IRC chat channel. And what's chilling is they're reporting for duty.

Leo: Yeah, yeah.

Steve: I mean, they're logging in saying, okay, I'm ready to receive commands.

Leo: What is thy will, Master?

Steve: And so – exactly. And so somewhere, if this hacker chose to take pretty much anyone down that they wanted to, knocking them off the 'Net and holding them off for whatever period of time they chose, they log into a different server, use a password that only they and their bots know, because you're able to password protect these channels, and you're able to hide the channels, log into a hidden...

Leo: Which raises the issue, I mean, if you saw this channel, can't the FBI just find them and kill them?

Steve: Yes, I mean, and presumably that's going on all the time.

Leo: Right.

Steve: But all they have to do is, you know, edit their code, change the channel, and reinfect a bunch of machines. It is – actually, I remember years ago seeing some statistics about the rate at which a new bot would infiltrate people's machines, just through common user actions, I mean, you know, the kind of actions you don't want to have be common, but people not knowing better. And so somewhere this hacker connects to a different server, joins the hidden channel that his bots are a member of, and issues a command. The IRC system forwards that – basically it's a command, but it's a comment like any other posted into a chatroom, forwards that chat comment through the system, bouncing through any number of servers until it reaches the one where the bots are congregated, that they're all checked into. And they don't even have to all be congregated at the same server. There are also distributed bot networks that are smart enough to have a number of domains that they'll randomly choose so that they're not all congregating at the same server. I mean, this stuff has become, you know,

through a process of successive refinement from the hackers comparing notes and, hey, how are you doing this, oh, that's a good idea, I think I should try that, too. I mean, for them it's a game. And so what we have today is true destructive force, or as I called it, "Internet weaponry."

Leo: Weapons of mass chatbotry.

Steve: Well, yes. And in fact, in July of 2002 you may remember that the RIA was also off the 'Net for many days off and on. In fact, it was very problematic for quite a while because the RIA had, you know, our wonderful recording industry association, had strongly endorsed some very, very strong anti-peer-to-peer filesharing legislation. And so in retaliation, one or more – we don't know, you know, to this day as far as I know it was never tracked down – one or more people who objected to that RIAA policy just said, okay, we'll show you who's boss of the Internet.

Leo: Who's really running the show, yeah.

Steve: And just blew the RIAA's website down and held it down for quite a while.

Leo: How big are these nets? How many do you have to have, how many co opted machines to be effective? And what are the defenses against these things? That's three big questions, I know, but...

Steve: Well, I know that Mark Thompson has told me – he has a friend with a major bandwidth provider network that has seen attacks of nine gigabits. So...

Leo: Jiminy Christmas.

Steve: Nine-gigabit attack. Now...

Leo: There's very few pipes that could survive something like that.

Steve: Oh, yeah. I mean, that's a serious, a serious debilitating attack. So say for the sake of calculating in our head that a typical bot on a cable modem – oh, and by the way, those are called "cable bots." Because you want to have...

Leo: You need bandwidth, yeah.

Steve: Cable bots are better than modem bots.

Leo: Right.

Steve: You know, modem bots are lame. No. First of all, they're not connected very often, so

they're not often participating in the fleet.

Leo: You need an always-on high-bandwidth connection.

Steve: That's really what you want.

Leo: Yeah.

Steve: So say that we had upstream bandwidth from an infected machine of, as I was saying before, like 250 kilobits, a quarter megabit, okay? So four of those would be a megabit. 4,000 of those would be a gigabit. Which means...

Leo: 36,000 machines.

Steve: Yes.

Leo: Even if you were more conservative and said half that, it would still be 18,000 machines.

Steve: There was one...

Leo: That's a huge net.

Steve: ...one botnet found of 100,000 machines.

Leo: Wow. Wow.

Steve: Controlled – a single controlling individual with 100,000 machines.

Leo: Now, are these always created by a virus? I mean, is that the only way to effectively create something like this?

Steve: No, it's anything you can do to get, you know, the bots are communicating Trojans. It's a Trojan which gets installed into a computer, arranged to automatically start whenever the machine is booted. And the first thing it does is try to phone home.

Leo: Okay, you join the net, the IRC channel, yeah.

Steve: Join the net, report for duty. And so the idea is that any techniques which can be used to get code running on someone's machine has been done.

Leo: So any security flaw, presumably these bots could then be instructed, well, okay, here's some code, execute it, try to find more recruits, try to increase the size of the net.

Steve: Yeah. A perfect example, for example, are the Internet worms that we saw, like Code Red and Nimda and so forth, that were very successful at propagating themselves. Now, their only interest was in their own propagation, although they also in several cases opened backdoors and left backdoors behind that then allowed their machines to be taken over remotely. But they weren't bringing along any other, like, remote-controlled bot technology, although of course the famous Code Red did have, and in fact many of them had, time-delay attacks where they would launch attacks on a given website. Remember there was whitehouse.gov was targeted, Microsoft's security update service was targeted. So they had their own malicious intent, but they were not remote-control Trojans that they were disseminating. So in general, you know, email, email attachments, you know, sort of shady websites that will use known vulnerabilities, or just somebody saying – in fact, this is one of the famous ones – here is a free utility that will speed up your Internet connection five times. There were...

Leo: And a lot of people would just jump at that.

Steve: Absolutely. It's like, whoa, my Internet connection really needs a five-times boost. So they'll download it and run it. And maybe it, like, it says, oh, your connection is already optimized. Thanks for coming by. Or, you know, or it might pretend to be doing that. What it's really done is install something malicious. So, you know, we've said before, and this is a perfect reason to say again, really only download things from well-known, high-reputation websites, you know, SnapFiles, CNET is going to be, you know, checking the files that they're offering and making sure, I mean, and they specifically say they've checked them for bots and viruses and Trojans, and these files are clean. But, you know, you really need to be cautious when you download something that seems like it may be too good to be true. It probably is.

Leo: Wow.

Steve: And so...

Leo: Okay, so that's the size that you need. That's how they get them.

Steve: Yep. Now, the final...

Leo: Now, how do you defend?

Steve: Well, the final step in this – and we'll talk about defense in a second – in the evolution of this has been doing this for profit. And that really changed the complexion of Internet attacks. Somebody realized, hey, if Mafiaboy was able to do $1.7 billion of damage to those companies, then wouldn't they have been willing to pay something beforehand not to have suffered that damage? Even 10 percent of that would be, you know, plenty of money, 170 million. So what people realized was, due to the evolution of the 'Net, and specifically a prime target have been online gambling websites, there are now companies whose, I mean, whose livelihood really depends upon being online, especially, for example, in the case of online gambling sites around the times of major sporting events, which the sites tend to specialize in –

horse races, boxing matches, whatever. And so what has happened and is now happening is there are extortion rings that seem relatively well organized which will contact a website's owner or owning company and say, hi there, we'd like to sell you our protection services.

Leo: Oh, my goodness. This is the traditional protection scheme.

Steve: It's exactly what it is.

Leo: Oh, my goodness.

Steve: It is exactly that. And if you pay us $10,000, we will arrange not to have your site attacked during the upcoming, you know, blue chip horse race or who knows what.

Leo: The truth is, the only people they could protect against were themselves.

Steve: Well, yes, exactly. They...

Leo: They're really saying we won't attack you.

Steve: They can not give the order to their bot fleet. It's sort of like the way Washington saves us money. It's by not giving us the increases they were planning, and they call that a cut.

Leo: Yeah, don't charge what we thought we would.

Steve: Exactly. So very often, the first time one of these extortion threats is received, the owners blow it off and, well, this is old news now. No one blows it off today who's in the business. But they would say, ah, you know, I don't think it's going to be that bad, or I've got big servers, or I've got a big pipe, or I'm paying extra for super strong networking, whatever. And sure enough, the big day comes, and they are off the 'Net for 24 hours, just gone.

Leo: Wow.

Steve: They're black. No one can get to them. And they're losing their customers, who are pissed off that they can't get to the gambling site they were using. So those customers just go somewhere else. I mean, and so they realize there's a huge cost of not being on the 'Net because those customers that they have once lost are going to be very hard to reclaim. So, you know, the attack ends. An hour later the phone rings or email arrives saying, gee, we're really sorry. We were unable to prevent that. We see you were off the 'Net for the last day while the horses all crossed the finish line. So, gee, I hope that when that next boxing match comes up, and we contact you again to offer our protective services, you may think twice. And more often than not, they get paid. Now...

Leo: Do we have any idea how often this is happening? I mean, I imagine it's quite widespread.

Steve: Yes. The last time I spoke to a whole roomful of FBI guys – I meet with the, I can't remember what they call themselves.

Leo: Secret Service?

Steve: It's like a, well, it's...

Leo: It's a crime division, yeah, yeah.

Steve: The electronic crimes guy. But it's people from the Secret Service, the FBI and Border Patrol and all kinds of divisions have, you know, a side to them that is concerned with electronic crimes, the Electronic Crimes Task Force. And I was chatting with one of my FBI friends before this, and we were specifically talking about this kind of thing. And what often happens is that a few months will go by, and there'll be another request for more payment.

Leo: Right.

Steve: And so...

Leo: That's blackmail. They never stop. Once they've got a mark, they're going to keep going.

Steve: Yeah, I mean, and it is really a problem. Now, what's happened is, in response, these sites that really, really have to stay on the 'Net or they're in serious trouble, they've realized, okay, I guess I can't buy my bandwidth from, you know, the cheapest provider in town. So they've ended up hugely strengthening their connections. There are some commercial services now that deliberately have huge pipes and, like, proxying servers to accept the connections on behalf of one of their clients. So they're selling Internet protective services. These websites then, they're placed behind these denial of...

Leo: But these are legitimate vendors here. We're not...

Steve: Yes.

Leo: ...talking about, yeah, not the extortionists now.

Steve: Yes. And, I mean, and it's still the case that the largest attacks are able to cause problems. But mostly what's happened is the cost of doing business for these people who are having to now pay a serious true technology, you know, bandwidth provider to insulate them from these floods of packets, you know, their costs have gone up forever. So it's not like the Internet is a free ride for them because, you know, there is now true Internet weaponry loose on the Internet.

Leo: Amazing. So the defense is what? I mean, how do they do it?

Steve: Well, the problem is that we're talking about a distributed network, widely distributed, for example, 10,000 machines, or as we did the math for a nine-gigabit attack, 36,000 machines. You know, they're not all in one university, they're not all in one location because of the nature of the way they are spread, through websites, through email, through spam, through, hey, download this free Internet accelerator program. You know, everybody on the planet is going to be carrying these bots.

Leo: Right.

Steve: And so what happens is, as in my magnifying glass analogy, packet traffic is incoming from every ISP, every major Tier 1 provider, you know, through every network on the Internet. And at any given point the traffic doesn't look unusual. It's only as it begins to converge down towards its target that, you know, the wires begin blowing, and the network engineers say uh-oh, you know, something's wrong here because we're seeing all kinds of spikes, and servers and routers crashing on our network. So the problem is, you know, there isn't a way to practically backtrack this. And it's certainly the case also that bots could be given instructions ahead of time so they will launch their attack if not told not to. And you could even have smart bots that are able to figure out, like something posted on a web page somewhere, they could be getting their instructions from the content of a web page. I mean, so the problem is, it's a perfect example of the extreme sophistication and power and flexibility of the Internet is being turned against it, and citizens on the Internet.

Leo: And so because it's so widespread, you can't filter it.

Steve: Right.

Leo: You can only throw bandwidth at it, basically.

Steve: Right. Now, there have been attacks which were filterable. For example, there was a famous attack, in fact, that we didn't talk about yet, was in late October of 2002, remember when the DNS system was attacked.

Leo: Oh, boy.

Steve: That was a – it was a one-hour-long massive ping attack. It was just an ICMP flood. It was so strong, though, it was directed at all 13 of the main DNS servers, the so-called "root servers," which maintain the master directories of domain names. Nine of the 13 DNS servers were brought down. Only four of the servers managed to stay on the 'Net.

Leo: And they were brought down by pings, by floods.

Steve: Yes. Just an ICMP. Now, what's interesting is that DNS doesn't need ICMP. It's nice to be able to ping a DNS server to see if it's up and if it's responding. But technically you don't need...

Leo: Not required.

Steve: Right. So what could be done is filters could be put in routers far enough upstream, that is, away from the DNS server, so that the concentration hasn't yet had a chance to become so extreme that that filter can't handle the traffic. And the filters could be set, drop incoming ICMP traffic to this IP address. And so what would happen is the distributed attack would be – well, that particular distributed attack would be stopped far enough upstream, when it was still dispersed enough that individual filters could stop their portion of the attack that was trying to move through them as it concentrated.

The problem is, DNS does use UDP. And so the reason we haven't really bothered filtering ICMP is, first of all, it would be a problem if DNS servers didn't respond to pings. You'd like them to do that. I mean, that would, you know, break who knows what else that is, like, checking on DNS server response times and Lord only knows. But you could always attack the same protocol that the service or server uses. In the case of DNS, it's the UDP protocol. And famously, in the case of any website, it's TCP aimed at port 80. So if an attack, for example, were using UDP – well, say it was like a DNS attack on port 53, but aiming at a web server. If the web server didn't need to serve DNS, it could just have that blocked upstream, and the attacks could not get through to it. But all web servers inherently have to be able to accept TCP packets, typically on port 80. So if the attack is profiled so that it looks exactly like what your customers are doing, like your valid traffic, there really, truly is no way to filter it.

Leo: So you're essentially saying there's no defense.

Steve: There really is no defense. The only thing that can be done is that – and this is what some of the commercial anti-denial-of-service service providers have done, is they could have servers connected to very large pipes, which accept the connection on behalf of the actual website's servers and respond to every single incoming attacking packet, assuming that it's valid. And now the problem is you have something called "denial of service back scatter." Since the source IPs of the incoming packets are spoofed, they're normally just random numbers, and it's a SYN packet, the server will respond with a SYN/ACK packet back to the apparent source IP. Well, if it's a random source IP, this just sprays these SYN/ACKs all over the Internet.

And in fact, some really brilliant people down at the San Diego Supercomputer Center, they owned a large block of never-used IP space. They set up a monitoring system to watch the incoming SYN/ACK traffic that just happened to statistically land within their big IP space. And they were able to track – this is so cool – they were able to track and monitor denial of service attacks occurring all over the Internet from the back scatter generated by servers that were under attack, trying to respond with SYN/ACKs to bogusly addressed packets. So some percentage of the total traffic from a random IP would happen to have the IP in this net that, you know, network and also net as in a fishing net, that the supercomputer center was watching. So they could tell when attacks were occurring, how strong the attacks were; and since the server would be sending the SYN/ACK from its own IP, they knew who was being attacked on the Internet at any time.

Leo: And the conclusion was...

Steve: It's bad.

Leo: Well, I mean, there is one solution, which is to really – and I certainly think we do this as best we can, I certainly do, and I know you do – tell everyone you know about it so that they don't fall prey to these bot nets, that they don't get their computers zombied.

Steve: Yeah.

Leo: Otherwise you're out of luck.

Steve: Yeah. Well, of course, I famously made a lot of noise when Microsoft was getting ready to put Windows XP out for the first time because there was something they were adding to XP known as "raw sockets," which for unfortunately complex reasons was a really bad idea, and allowed attacks to be much worse than they would otherwise be. It's not that they weren't happening before, that UNIX didn't always have raw sockets, that, you know, there weren't other ways to generate floods of bandwidth. All that was true. But XP was the dominant platform. I knew that people would be unfortunately installing bots and Trojans into XP. And, you know, there's no better place that a denial of service bot wants to be than in a machine with raw socket capability because it makes it so much easier for it to launch an extra strong debilitating attack. Anyway, as we know, Microsoft didn't understand what I was trying to say. And it wasn't until...

Leo: It got attacked.

Steve: ...yeah, the MSBlast worm used XP's raw sockets against Microsoft...

Leo: Right.

Steve: ...that they finally thought, ouch.

Leo: We'd better do something.

Steve: We've got to take this out of XP. And of course, in Service Pack 2, that fixed so many other security problems with XP, Microsoft also removed raw sockets. And things are better today.

Leo: Yeah. So, folks, tell every – I mean, anybody who listens to this podcast isn't really likely to be a member of a bot net. But tell your parents, your friends, your less sophisticated acquaintances, don't open email attachments. You know, do all the security things we talk about day in, day out, you know, update your system regularly, make sure you apply all the critical updates. You know, don't open attachments, don't – have a good antivirus. Be careful. And then I guess if they have been botted, in many cases an antivirus scan will detect it. But of course if they've used a rootkit they may be completely invisible.

Steve: Yeah. I, you know, I guess bottom line is, I mean, you know, people sometimes believe that I'm an alarmist, that I'm, you know, raising concerns that are above the level that the threat requires.

Leo: Right.

Steve: And, you know, my position is, hey, I'm just explaining what is. I'm just saying this stuff is happening. It does exist. Malicious programs are on the 'Net that can be downloaded that will do what this says. So...

Leo: It may be too late. Once, you know, if there really is a massive problem, then it's too late. Better to raise the alarm now.

Steve: Well, to me it doesn't seem like this is escalating any further. I mean, law enforcement has been successful in tracking down a lot of these people. The one glitch in the extortion racket is that somehow money needs to go from the company that's been extorted back to the extorters. And so it's – and Western Union has been used often in order to sort of try to create some sort of not-easy-to-follow trail. But the problem is, with more and more governments cooperating now, what is now becoming a widely recognized problem, you know, when it used to be five years ago, you would talk to somebody and say I need help, you know, tracking down an Internet attack. They'd go, huh? A what? Now it's like, oh, yeah, sorry to hear that, you know, you've got a client who's got a problem. I mean, you know, now it's understood.

Leo: They know about it, yeah.

Steve: So, yeah, so there's a lot more cooperation. And so certainly it's difficult for these extortionists to get paid, though apparently there are still ways because, as far as I know, it's still going on.

Leo: Well, and I'm actually, as bad as that is, more concerned about the vulnerability you described in the DNS system. And while nothing bad, really bad, has happened yet, they've obviously made some noises indicating they could do it.

Steve: Well, it's absolutely the case that, if DNS were – if all the servers were held down long enough – see, that's the thing. This one-hour attack frightened people in the networking community because it was very clear then that DNS could be held offline. The problem, though, is that DNS servers are also distributed, and they cache all their addresses locally. So typical, you know, Amazon.com, my own GRC.com, eBay, whatever, those addresses are widespread. And only when they expire in a local server's DNS cache is it necessary for that server to go and update itself. Typically that's a day. So you'd have to hold all the DNS servers down and off the 'Net for a day in order for the DNS history, for the DNS caches, widely distributed among the millions of DNS servers that are, like, owned by ISPs, and in some cases individuals, for their caches to drain and for them not to be able to then get themselves refreshed. So, I mean...

Leo: It's hard to do.

Steve: On the other hand, it would bring down the 'Net. The entire 'Net would basically come down. I mean, IP addresses would still work, but who knows anyone's IP address? We all use DNS.

Leo: That's why, going back to the hosts file, you might want to start making a hosts file of your own of all the sites that you really, really like, just in case. And of course I hope you'll include TWiT.tv in that list so you can still get our podcasts should the worst happen. That's just a – it's amazing, really amazing.

Steve: Yep.

Leo: Well, it's one reason why our sponsor Astaro is doing so well. People are very aware of security nowadays. And naturally, when your company's looking for security, the place to go is Astaro.com, Astaro Corporation, makers of the Astaro Security Gateway. If your small or medium business network needs superior protection from everything, I mean, spam, viruses, of course hackers, as well as complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall, all in an easy-to-use, high-performance appliance like I have – I'm so glad to have it, makes me feel better – contact Astaro, Astaro.com, or 877-4AS-TARO to schedule a free trial of an Astaro Security Gateway appliance in your business. Of course they do offer the free version for consumer download at their website. And, boy, if you're managing a larger network with a bunch of gateways, you want to look at the Astaro Command Center. What a slick way to keep track of what's happening on your network. And let's pray and hope that you never see all those lights go red with a big denial...

Steve: Oh, yeah.

Leo: ...of service attack. Ooh, that would be a scary, scary thing. You know, I think it's an interesting job now to be a system administrator.

Steve: It's not boring. There is so much going on. You've got, you know, as we've talked before, you've got worms scanning around, trying to propagate themselves. You've got, you know, attacks of one sort or another. You've got incoming unsolicited spam. I mean, there's a lot going on on the network.

Leo: Lot of beasties out there.

Steve: Yeah.

Leo: GRC.com is the place to go for more information about many things. Of course this is where you can get show notes and the 16KB versions of this show. Transcriptions, too, thanks to Elaine. GRC.com/security now. It's also a good place to go to get the ultimate disk recovery and maintenance utility, the wonderful SpinRite, Steve's bread and butter during the day.

Steve: Yup.

Leo: Also, for information or testimonials from customers, and there's some great ones, SpinRite.info.

Steve: We got one – I was thinking of you the other day, Leo. Someone wrote they had a hard drive die, and they sent it to a data recovery company who gave them a quote of, I think it was $1199.

Leo: Yeah. Very typical, actually.

Steve: With no guarantee of success.

Leo: Right.

Steve: Just that was the quote. And the guy said, uh, send it back. So he bought a copy of SpinRite, and three hours later his drive was back online, working perfectly.

Leo: Ah, yes.

Steve: And fixed it. So...

Leo: What a nice story. There's lots of those at SpinRite.info. Yeah, you know, more and more I'm telling people, if it's a physical error, you know, if the disk is gouged, SpinRite won't fix that, and you might have to spend 1100 bucks. But anything short of that, SpinRite's the first thing to try, really is a great tool.

I guess we're done for the day on our Internet Weaponry segment. What a fascinating topic, though.

Steve: Yeah. 48 next week is a Q&A episode, so we'll answer questions and catch up with email and then move on from there.

Leo: All right, Steve.

Steve: Approaching one year of Security Now!

Leo: Yay. So a happy Fourth of July week to you. I hope you took a little time off for fireworks. I bet you didn't.

Steve: Nope.