The Telnet-pocalypse

Description: This week was so chockful of things to discuss that we had no time to discuss the fascinating technology and operation of Distributed Hash Tables. That discussion will be "tabled" for two weeks. This week, we look more closely into the somewhat troubling issues of SSL/TLS server security as revealed by SSLLabs.com, discuss the SWAT team arriving at Brian Krebs's home, examine the consequences of the revelation that 420 million routers are accepting trivial logins on their Telnet ports, and more!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-396.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-396-lq.mp3

SHOW TEASE: Time for Security Now!. Steve Gibson is here with a revelation that will chill you to the bone, if you truly understand it. We'll talk about Bitcoin and the Telnet-pocalypse. It's here now. Details next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 396, recorded March 20th, 2013: Telnet-pocalypse.

It's time for Security Now!, the show that protects you and your loved ones online, your privacy, your security and all that jazz. And, boy, there's never been a better time for the Explainer in Chief, Steve Gibson, than right now. Hello, Steve.

Steve Gibson: We've been busy lately, Leo. And...

Leo: Seems like the hackers are kind of, like, gaining on us.

Steve: Well, and we've got some news this week that is very worrisome. I haven't seen anyone else pick up on this aspect of it, but it's perfect for our listeners to understand.

Leo: Oh, great. Oh, boy.

Steve: And this involves something known as - what was a transient botnet known as

the Carna Botnet, which is the creation of one guy, one arguable sort of gray-area researcher. I mean, he acted responsibly; but, unfortunately, the disclosure of what he found really is worrisome. And we'll talk about that. We had planned also to carry the second half of the questions from last week's Q&A over to this week, but there's just no way we're going to have time. So those, I'm moving those five that we didn't get to last week to next week's Q&A because we have so much to discuss, news of the week, and I wanted to also talk about the operation and technology of distributed hash tables.

The topic came up when we were discussing, two weeks ago, the way Tor offers services. And the way people look up the locations of the services is in a distributed, secure, anonymous fashion which distributed hash tables allow. And in the research, sort of the background for this, I discovered, among other things, for example, that that's the way Amazon stores all of its data. It's not using SQL, so-called SQL complex relational databases because that's overkill for what Amazon needs. What they want is high availability, very fast, very robust, very scalable database technology. And all they need to do is look up data associated with short strings, or keys, and they're actually using distributed hash tables throughout all of Amazon's websites and offerings as the way, like, of the database technology they've deployed.

So it's not just for places where you want a decentralized database. Another perfect example is BitTorrent. BitTorrent uses distributed hash tables so that there's no place, like there used to be with Napster, where it could be subject to subpoena and shutdown. So that's our main topic today. And I thought we'd have time for more. But, boy, with all of the really amazing news that we have to cover, I think we'll have a very full and fun, interesting podcast.

Leo: Well, may I also wish you a Happy Vernal Equinox today.

Steve: And isn't this the first day of spring?

Leo: The first day of spring. And all over the world, this is from Boston Globe's Big Picture, these are pictures of spring all over the globe. This is the day when the day and night are equal. There are two of these a year. And there's Stonehenge, the sun rising between the lintels to mark the vernal equinox.

Steve: Cool.

Leo: So Happy Spring. It's raining here. We've got, I guess...

Steve: Is that what I'm hearing? I kind of hear something.

Leo: Can you hear a little tippy-tap on the roof? Yeah, we have a metal roof. Or something.

Steve: Yeah, that's neat.

Leo: I don't know what - it's not metal. It's some sort of composite.

Steve: I normally don't hear anything like static coming from your end, but I hear...

Leo: Yeah, it sounds like static. That's the rain, yeah. It's pretty, though.

Steve: Cool. Well, our big - one of the crazy events of the week occurred just after last week's podcast, which was last Wednesday the 13th. This occurred to a friend of the podcast, Brian Krebs, on the following day, on Thursday.

Leo: He was on a couple of weeks ago, in fact.

Steve: Yup.

Leo: Our show.

Steve: He was subjected to both a virtual and a real-world attack of sorts. We're all familiar with the term DDoSed, and his site came under attack from a purchased denial of service attack by a distributed botnet which offers its DDoSing services for hire. But in the physical world he was SWATed, which is the name - SWAT, of course, is the acronym for Special Weapons and Tactics. A hacker, whose identity Brian believes he knows, spoofed an emergency 911 call from Brian's phone. I think his cell phone, but I don't remember for sure.

Leo: Yeah, it said cell phone. And by the way, that's very easy to do. That's not a sophisticated hack.

Steve: Right. And so Brian was, like, I think he was removing some masking tape from his door jamb where he'd been painting or something. I don't remember quite the details.

Leo: He was expecting houseguests. He was going to have a dinner party, and he was tidying up. And, yeah, there was something on his door jamb. He bends down to pick it up, looks up, and lo and behold, there are guns trained on him. Holy cow. Scary.

Steve: A bunch of police cars all positioned out in front. Guns leveled at him. They told him to turn around and walk slowly backwards towards them. And he was handcuffed and then walked away from the house, up the street. Meanwhile, of course, he was trying to explain to people that there was nothing amiss whatsoever in his home, and that this was a false alarm which he had even had the foresight, I think it was about six months before, he wrote a letter to his local police department warning him that this sort of thing might be happening. Well, the standard beat cops just blew all that off, but

finally someone who had the mannerisms and dress of a supervisor came up and said to Brian, "Are you the guy who wrote us the letter about six months ago?"

Leo: Yeah, that was me.

Steve: "And told us this might happen?"

Leo: Yeah.

Steve: And Brian said yeah, that's me. And so the...

Leo: It's really an easy thing, and it's happened on the West Coast with movie stars. And Part 1 is it's not hard to figure out where somebody lives because that's all public record. And unfortunately, in the old days you had to go to the courthouse in that local area, the county courthouse, to get that information. But there are a number of websites that have sent people around physically to do that and have put it online. So it's not so hard to find out those home sales records. And then, unfortunately, anybody can spoof these 911 calls. They told the SWAT team, he said, "This is Brian Krebs. My wife has been shot by Russian gangsters." And so of course they're going to respond the way they did. I don't think they mistreated him in any way. But it's still terrifying.

Steve: No. No, and in fact, the moment the supervisor realized that this was extremely likely, both from Brian's mannerisms, the fact that he wasn't distraught and upset, and the fact that he was the guy that had written a letter six months before, the supervisor spoke something into his radio, and all the guns came down.

Leo: But you understand they have - there's no - that's - this is the difficulty.

Steve: How could they not take it, yes, how can they not take it seriously.

Leo: And believe me, the next time Russian gangsters break into Brian Krebs's house, he'll want them to do this. And that's the problem is I don't know what the easy answer is to this. We assume in society a certain amount of civilized behavior. And this very uncivilized behavior, really childish behavior, mostly it is children or people with childish mentalities who do this, we're not really set up to handle it in any way. They did call his - they called his phone, his home phone, and he just - he heard it ring, but he didn't respond.

Steve: Oh, that's right. Right, right, right. They called a couple times. I think they called his cell phone because he made a comment that he'd left it upstairs.

Leo: Had he answered, maybe that would have defused the whole thing.

Steve: Yes, because he would have said, oh, no, that's fine. Remember, and I'm the guy who wrote the letter six months ago telling you this might happen.

Leo: Right, right.

Steve: But you're right, there was no answer several times, so that, they thought, okay, well, our first...

Leo: I think they'd still send a couple of units over because maybe the Russian gangster would say, yeah, this is Brian Krebs. Everything okay here. No problem. Is okay. So it's terrifying.

Steve: Anyway, Brian posted about that last week. He also has posted since some further investigation results. So anyone who wants more on this, Brian's site, again, is KrebsOnSecurity.com. And the most recent blogs, postings, the second most recent is about this, where he describes the events that transpired last Thursday. And then his most recent posting, just recently, was the result of him pursuing back through his various avenues who he thought it was that was responsible, and the conclusions that he came to. So, and there is more that we haven't talked about. So it's worth a - anyone who's interested, wow.

Leo: He's done a lot of research, and actually pretty convincingly has tracked down the kid. He's, I think, 20, lives in Milford, Connecticut, well-known kid, same kid who hacked Mat Honan. I've actually had conversations with him on Twitter. And it's - but there's nothing much you can do about this.

Steve: No.

Leo: It's just so scary, so scary. The scary thing is if something goes wrong. If, for instance, you don't expect the SWATing, and you have a weapon, and you think somebody's breaking into your house, and you pull the weapon, you're dead. It's kind of hard to take that back.

Steve: Yup. And if you're someone with a very different temperament than Brian, where he was completely relaxed, he understood escalating is not what you do at a time like this. But somebody else who reacts differently, I mean, tensions are high on the side of the police.

Leo: And as Krebs points out, this also is a great expense and misdirects emergency personnel that might be needed in another situation, a real emergency.

Steve: Yeah.

Leo: So all in all it's really, boy, I just don't know what you do. I mean, one thing we've got to fix is the spoofability of phone numbers. It's trivial right now.

Steve: Yeah. So I mentioned a site, SSLLabs.com, a couple weeks ago. SSLLabs.com has a service, free, that allows you to put the domain of any server, any public web server, into the site, and it will test that site's SSL and TLS security technology. I mentioned it relative to GRC, my site, because we used to get a D or a D-minus, I don't remember, when I was running Windows 2000. Because I was supporting older ciphers and because Windows 2000 was so old, I couldn't offer any newer, stronger ones. It was one of the real benefits for GRC, especially, of moving up to Windows 2008 R2, which I'm going to discuss a little bit more next week because it's one of the questions we didn't get to last week, which we will get to next week, was about that, from some guy who administers - administrates? - a lot of Server 2000 installations.

But this prompted a bunch of our listeners, I probably have no idea how many, to put sites that they are interested in into SSLLabs.com. I know that many put GRC in because I saw in my logs all of the inbound tests from SSL Labs coming to GRC as people ran the tests themselves. One listener was very worried because he put the address of his bank, which is TD Canada Trust, and this was easywebsoc.td.com, into SSL Labs and received a grade for his bank's SSL security of F. It got an F. You can get an E, by the way, which is somewhere between D and F. This got his bank an F. So he wrote saying, "Oh, my god, should I worry?"

So I wanted to create a little bit of context for this, a little more context. I went back to SSLLabs.com. And Leo, if you go there - and you could use the link that's in my show notes, if you wanted to, and that brings up the test for this TD Canada Trust bank. It summarizes all of its findings in four categories: the quality and strength of your certificate, that is, the certificate that that secure server is offering; the nature of the protocols that it supports...

Leo: Oh, geez. That's a pretty big red F.

Steve: It leaves, yeah, you can understand why people might be a little concerned if their bank is getting an F.

Leo: Oh, boy.

Steve: The key exchange strength and the cipher suite strength. So this TD Canada Trust got 100 on their certificate. So it's a big green bar that goes all the way. They got a zero on protocol support, and that earned them an instant F.

Leo: They're using SSL 2.0.

Steve: Yes. And it's not that they don't offer more, but they offer it.

Leo: They need to turn this off.

Steve: Correct. And so that's what did it to them. That SSL v2.0 earned them an instant F. There's no way to get a better...

Leo: So they're vulnerable to BEAST, is the problem.

Steve: Well, actually, no. That's a different problem. SSL 2.0 is just no longer recommendable. And remember that, from our discussions about the way the handshake goes, the client, which is in this case a user, their platform, their Windows, their Android, their iOS, their Mac, whatever, Linux/UNIX, their platform sends to the server a list of ciphers and cipher suites that they understand. So it's like, here's a menu, a bunch of things that we understand. So it's up to the server then to choose what it wants.

And so the server looks at its list and compares the list of things it knows about, the different ways to securely interact in detail, and finds, like, arguably the best one, whatever that means, and we'll talk about that in a second because that's where BEAST comes in, finds the best one that it chooses from among what the client has said it understands.

Now, what this means is that, if you had a man in the middle, the man in the middle could intercept the client's initial outgoing connection and hold onto it for a second, then turn around and only offer SSL v2.0 to the server. Now, my server will say, sorry, if all you've got is SSL 2.0, we can't talk. And so a contemporary, well-configured web server today...

Leo: Like my Bank of America, A+.

Steve: Oh, yay.

Leo: Yay.

Steve: Good, yes.

Leo: I had to check it after that.

Steve: A well-configured server will not agree to accept a v2.0 SSL connection. It just says, sorry, if that's all you've got, we can't talk. Unfortunately, TD Canada Trust does accept it. So it's this man-in-the-middle vulnerability, the idea that somebody in the middle could downgrade the security the client is actually offering to a level that is so insecure that then there are other exploits which can be used against it. So that's what earned it an F.

Leo: Chase, by the way, Chase.com, C.

Steve: Yeah?

Leo: Key exchange was red; cipher strength was yellow.

Steve: Yeah. So the other things that are happening is that, in protocol...

Leo: This is fun. I like running this.

Steve: Isn't this neat? It is.

Leo: I know. This is awesome.

Steve: It's wonderful, yeah. So remember that the problem with BEAST, the B-E-A-S-T, the browser whatever it was that it stands for, but it's our guys that were on the beach, they realized that any cipher block chaining protocol, where the residual from the end of one block is fed into the beginning of the next, and that is true up to TLS 1.1. So both SSL 2.0, which is already bad for different reasons, but also SSL v3.0 and TLS v1.0, which is essentially the same as SSL v3.0, they all have their cipher block chaining protocols chaining across the blocks that are being sent, that is, across packets of blocks. And it's that interpacket chain that creates a vulnerability which can be exploited by this BEAST attack.

So what's happened again is that, when a client offers a bunch of protocols, the traditional wisdom was, oh, cipher block chaining and fancy ciphers like AES-256, for example, those are going to be better than RC4 because RC4 is just a pseudorandom stream generator. It doesn't use chaining. And so normally servers put their CBC-based fancy new ciphers first. And so that's the other thing that SSL Labs tests is essentially it gives the server different sort of - it teases them with different sets of protocols to see which ones the server chooses. And unfortunately, again, this TD Canada Trust has its CBC ciphers taking priority over the older RC4-based cipher, and once again it loses points because that means it's vulnerable to the BEAST attack because it will happily use this interlocking packet weakened cipher protocol rather than not.

And lastly, under the cipher strength category, it only got a 60 out of 100 because it's still supporting the weakest cipher key lengths ever. It's got a whole bunch of 40-bit key lengths and some 56-bit key lengths. And those are just no longer strong enough. You just can't, you know, we were talking the other day about the 64-bit key, which I can't remember who, it was a service that was saying, oh, well, because of export restrictions we're just using a 64-bit key and not anything higher.

Leo: Evernote.

Steve: That's right, Evernote. But here, this is 40 and 56-bits. So there's just no reason

to offer these weaker ciphers. And the server identifies itself as IBM_HTTP_Server and is deployed by AkamaiTechnologies.com.

Leo: Oh, it's Akamai.

Steve: So this is a major cloud deployment IBM server that is just sort of default configured. And this is what you get if you just install the software and don't do any tweaking.

Leo: Ah, that's it. Of course. Yeah.

Steve: Yes. Yeah, it just gives you everything. Here's everything.

Leo: But you've got to think a bank has some pretty high-qualified, heavy-duty experts, security guys.

Steve: Well, I think what they've done is they've subbed this out. They've said, okay, we know about charging people. We don't know about security. And Akamai says, oh, I bet you they've got gold seals and all kinds of junk all over their website, talking about how wonderful their security is. But it's not. It's just, unfortunately, not - obviously, here, they've got an F at the moment. So, I mean, this is not going to hurt TD Canada Trust in terms of, like, their reputation because only people who listen to this podcast know about the details of the way they're connected. But if a bad guy was really, really intent on exploiting their customers, it's much more possible to do so with a connection of this low grade than not. So anyway, that's what that's all about.

Leo: And who knows who to blame. I mean, I wouldn't rush to blame Akamai. It may be that when you set up your server at Akamai, you have checkboxes, and whoever was doing TD Ameritrade said, yeah, we should make it as flexible as possible, let's make sure we support everything, and checked all the boxes. Who knows how this happened? I wouldn't blame anybody. A surprisingly large number of banks are pretty good, though. Wells Fargo, straight A's.

Steve: Nice.

Leo: Yeah. Chase kind of - some middle-of-the-road stuff. BofA, A's. So it just, you know, this is probably a worthwhile thing for people to run: SSLLabs.com. They have a site test right there.

Steve: Yeah. And, if you find out that your bank is rated low...

Leo: Complain.

Steve: By all means, send a note. Yeah, complain, send a note to some web admin somewhere and say, hey, check this out. Are you sleeping well at night?

Leo: Yeah.

Steve: Just a note that Windows 7 Service Pack 1 has finally moved from "install it if you want" to "we're going to give it to you without you asking for it" mode. That happened also with Patch Tuesday last week, but I didn't see it in time to mention it.

Also at the same time, and this is relevant for anybody doing new installations of either Windows 7 or Server 2008, Microsoft also released a - and this is appearing under Windows Update under "Optional" - a complete, comprehensive rollup of all post-Service Pack 1 security patches since Service Pack 1. And having just installed a bunch of Server 2K8s and also a bunch of Windows 7 boxes, I mean, this is a great benefit to have this. The alternative is, you know, you install Windows 7; then you install SP1, which has been available for quite a while; but then you do, okay, give me all the other security patches. And there's, like, 64 of them. And they install one by one. Each one takes a snapshot of all of the system's configuration at the time it was installed and archives everything that it's replacing.

So the point is you end up with this massive blob of, like, history which has been stored on your system. It just annoys me to see, like, because Microsoft allows you to uninstall any of these things. You can roll them back, if you need to. And so because you're installing individual update events, it's archiving all the things it's changing every single time. Many of them are completely redundant. So I'm really excited and pleased. I wish this had come out two months ago. But still, it's better to have it now than not. So it's under "Optional Updates," and anybody - there's really no need to do it if your system has already been kept up to date because it'll - you'll probably run it, and it'll say, well, there's nothing for me to do.

But anybody installing and setting up a new Windows 7 system or new Server 2008 R2, which is essentially the server version of the same Windows 7 operating system, definitely wants to know about this. So you would install Windows 7; presumably then Service Pack 1, it's probably a prerequisite; and then immediately install this rollup, and you're saved from, like, this individual annoying incremental update across the board.

Leo: Love those rollups.

Steve: Yes. They are. And no one was really expecting this because Microsoft has moved on, famously or infamously, to Windows 8. And I just, oh, my goodness. How are you feeling about that, by the way?

Leo: Well, A, I think it's safe to say there will not be a Service Pack 2 for Windows 7.

Steve: No, that was the point I was making was that nobody expected...

Leo: Even one.

Steve: Nobody expected even, well, we had SP1 a long time ago.

Leo: Oh, we had one, the rollup, that's right. We talked about this in Windows Weekly. They're not calling it a service pack, but it is, it's a rollup, yeah.

Steve: Right, yeah.

Leo: You know, Windows 8, I have such mixed feelings. Under the hood, I think it's widely agreed it is better in a great many respects. Certainly file copy works better, a lot of the things work better. It's faster. Security, well, we'll see.

Steve: Some guy on TV is saying that his mother finds it very intuitive, but I just, you know, I'm not getting...

Leo: Oh, I don't find it - I think the real problem, as I see it, is it's really two different operating systems. They say, well, that's just - we've replaced the Start Menu with a Start Screen. No, really, you've replaced - it's more than just a start screen. It is Metro, and there are Metro apps, and there are desktop apps. And it's a little confusing. There's two versions of Internet Explorer with different capabilities, and you're not always sure which is running. So it's just, it's things like that. I think they'll probably iron these wrinkles out, but - I'm not dis-recommending it. I just...

Steve: They stumbled on something called Vista, and then they came out with Windows 7. So maybe there will be a 9, and they will fix, in doing 9, they will fix what they learned about 8. In which case I'm pretty much staying with my every-other-OS rule.

Leo: Seven's awfully good. I thought 7 was the best version.

Steve: Oh, Leo, I will be so happy with it. I've been using it a lot more. I'm very familiar with it. I set up a new 7 machine here because its OS is a clone, essentially, of the Server 2008 R2 that I'm running GRC servers, the newly set-up servers on. And the more I look at it, the better I get to know it, the more impressed I am. I'm very, very, very impressed with Windows 7.

Leo: Yeah, yeah.

Steve: Still on XP because it does what I need. But I've got a 7 box next to me.

Leo: I think it's conceivable that you could make Windows 8 run better just by eliminating Metro. And there are ways, third-party ways to do that. I don't know.

Steve: To revert it to something that looks like...

Leo: Yeah. Get rid of that Metro stuff.

Steve: So something really confused people this week. Some researchers looked at an update that Cisco made to their IOS. Now, this is not "iOS" the way we always talk about it, meaning Apple's OS. This is capital I, capital O, capital S, that well predates Apple having anything called iOS. I've got IOS running in my Cisco router here and at the datacenter. Cisco is, of course, a major router and switch manufacturer from the old days. IOS is their Internet operating system that they've always had on their devices. They have traditionally had a very strong password encryption, one-way, hash-based. It's got all the buzzwords. It's PBKDF, password-based key driven - what? - key derivation function. It runs a thousand iterations of MD5, of the MD5 hash, with salt. So it's salted, it's got a good hash, and it runs it a thousand times. Everybody was happy.

Then, curiously, some researchers looked at what they had done when they, with some ballyhoo, said, hey, we're coming up with a new password scheme. It does one iteration of SHA-256 with no salt. And people are like, huh? What? Because, I mean, with current state-of-the-art GPU-accelerated hashing, SHA-256 was designed for speed. It loves to be run in parallel on GPU hardware, not to mention custom silicon just built for that. And nobody could understand what was going on. So these researchers brought this to Cisco's attention; also, apparently, through some responsible disclosure, made this public. And Cisco has a response, a so-called "Cisco Security Response," and I'll quote a little bit from it.

They said: "The design called for using Password-Based Key Derivation Function version 2 (PBKDF2), as described in RFC 2898 section 5.1, with the following input values: hash algorithm, SHA-256; password, the user-provided plaintext; salt, 80 bits generated by calling a cryptographically secure random number generator; and iteration count, 1,000." And they said: "Due to an implementation issue" - now, this is the PR speak. At no point do they explain anything about it. They say: "Due to an implementation issue, the Type 4 password algorithm does not use PBKDF2 and does not use a salt, but instead performs a single iteration of SHA-256 over the user-provided plaintext password. This approach causes a Type 4 password" - which is the new one - "to be less resilient to brute-force attacks than a Type 5 password of equivalent complexity." So they're saying yeah, we know. And there it is.

Leo: Yeah. We know.

Steve: So an implementation issue. Now, I am not, our listeners know, I am not a conspiracy guy. But I don't get this. I mean, I don't get how Cisco would apparently deliberately and knowingly weaken, dramatically weaken the login strength of their router technology. I can't explain it. They did. And they got caught, essentially. They didn't document it. It wasn't public. In fact, they documented it as strong. And when the researchers looked, they said, uh, no. This is - what you said you did is not what you did. So they had to know. They're saying an implementation issue. This is not even conceivably a bug. You can't think of a bug, I mean, maybe if it had done 10 instead of a thousand iterations, oh, well, we initialized our counter wrong. Well, no, there's no counter. And there's no salt. So I'm just, okay.

Leo: And IOS is used in all the - in the commercial Cisco routers; right? What is...

Steve: Oh, my, yes. Oh, I mean, like, yeah, yeah. It is the big iron router of the Internet. Now, since then there's competition. There are other people also in the game. Cisco still has a huge presence out on the Internet. And every so often weaknesses are found in the current version of IOS, and so people upgrade. And so, as they upgrade to newer versions of IOS, they would be, over time, inheriting this dramatically weakened password hash on routers that form essentially the backbone of the Internet. So I don't know why.

Leo: [Laughing and singing] I don't know why, but they do.

Steve: So, interesting publication came out on the 18th, so two days ago, Monday, from the U.S. Department of Treasury, the Financial Crimes Enforcement Network. And if you just Google "FIN-2013-G001," it's the first link that comes up, FIN-2013-G001. What you get is a PDF about Bitcoin.

Leo: From the Financial Crimes Enforcement Network.

Steve: Yes. And the subject is, dated March 18th, Monday, Application of the - they call it "FinCEN," Financial Crimes Enforcement Network. So Application of Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. So, you know, they're...

Leo: They're calling for a crackdown?

Steve: No. The good news is we're okay. And that's why this is amazing. There's been grumblings in Congress. Various random representatives and senators have said [grumbling], you know, we need to outlaw this crazy thing. So they define a user of - well, so in sort of a summary at the top it says "A user of virtual currency is NOT" - in bold italics - "what they call an MSB." And they later define MSB as meaning Money Services Business, which is subject to regulation. So they say, "A user of virtual currency is NOT an MSB under FinCEN's regulations, and therefore is not subject to MSB registration, reporting, and recordkeeping regulations."

Leo: But somebody like Mt. Gox, which is an exchange, would be.

Steve: Yes. Yes. So they're saying, "FinCEN's regulations define currency, also referred to as 'real' currency, as 'the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance.' In contrast to real currency, 'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses 'convertible' virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.'"

And I'm skipping way down because I highlighted the things I wanted to share where they're explaining. They say: "This guidance refers to the participants in generic virtual currency arrangements, using the terms 'user,' 'exchanger,' and 'administrator.' A user is

a person that obtains virtual currency to purchase goods or services. An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."

And then under "Users of Virtual Currency," they said: "A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is NOT" - again, bold italics - "an MSB under FinCEN's regulations." So that's more good news. "Such activity," they say, "in and of itself, does not fit within the definition of 'money transmission services'" - so that's the key phrase that they look for - "and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs."

And then lastly, under "E-Currencies and E-Precious Metals" - I didn't know what an e-precious metal was. I guess there's a market, an electronic market for that. But they said: "The first type of activity involves electronic trading in e-currencies or e-precious metals." And they say: "In 2008, FinCEN issued guidance stating that, as long as a broker or dealer in real currency or other commodities accepts and transmits funds solely for the purpose of effecting a bona fide purchase or sale of the real currency or other commodities for or with a customer, such person is not acting as a money transmitter under the regulations."

And actually there's one last thing I forgot. Under "De-Centralized Virtual Currencies" - so, I mean, they're leaving no doubt here. They said: "A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort. A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter."

So for we end-users of Bitcoin, there is no longer any gray area at all. The United States Department of Treasury Financial Crimes Enforcement Network says we're doing nothing wrong. I saw this, and I also thought - I highlighted it, and I'm going to send the PDF off to Mark Thompson because, as I mentioned a couple weeks ago, he's experimenting with taking bitcoin in exchange for physical goods. And for anyone who's interested in or has bitcoins or wants to mine bitcoins and wonders about the legalities of what they end up doing with them, this makes it clear. We're okay.

Leo: The only thing that bothers me a little bit about Bitcoin is I'm just used to the notion that money is tied to some sort of creation or physical, you know, doing something. And Bitcoin's really just tied to how many CPUs and GPUs you want to put in series.

Steve: Well, okay. Of course we famously went off the gold standard when money was...

Leo: Right, so it's not tied to gold, either, is it, yeah.

Steve: And U.S. currency is tied to nothing. I mean, it is - it's created out of thin air.

Leo: Well, initially. But there's something going on. For me to get money from an advertiser, for instance, we do something.

Steve: Well, just agreement, Leo. That's all it is.

Leo: Well, the actual value of it is by agreement. But it has a natural life because we agree what something is worth by consensus. I don't know. It's just there's something, it feels like there's something missing in Bitcoin that, well, all you have to do is run a giant server farm, and you can have as much money as you want. That doesn't seem quite right to me.

Steve: Yeah, it's - well, okay. I mean, that puts money into circulation, bitcoinage into circulation. What is so elegant - and again, we really nailed this in our Bitcoin podcast [SN-287]. So anybody who hasn't yet heard the Bitcoin podcast, let me commend everyone to go back and listen to it because you'll get this. What is so elegant is, independent of how much effort people put into mining, we already know today, yesterday, and tomorrow the rate at which new bitcoins come into the realm.

Leo: Right. So really those Bitcoin computers are just like the printers at the Treasury. They're just creating the currency which we will then determine the value of by trading, just as we do with dollars.

Steve: And think of it this way. The more printers there are, the slower they run.

Leo: Right. So that's naturally gated; right. And there will be a maximum amount of coinage reached in a few years, and that'll be that.

Steve: In 20, what is it, 2040 or - I think at 2040 it hits, like, it stops. It's already slowing down, and it's following a curve. And so the rate at which new bitcoins are being minted is following a trajectory that is absolutely set. Nothing can change it. And we will then end up with a crypto - I mean, the Internet, the world will have a cryptographically strong, tradable, virtual currency. And people will be buying and selling it using it, just like any other currency.

Leo: Currently a bitcoin's worth $63.98 on Mt. Gox.

Steve: Woohoo, and I've got 50 of them. So...

Leo: Yeah. But it's really an interest- I think it's starting to gather critical mass. That's why it's of interest is it's no longer just kind of an academic exercise. It seems to actually be gaining. You can buy pizza with it. God knows you can buy drugs with it.

Steve: My computer made $3,000. It paid for itself and a few other machines.

Leo: Right, right.

Steve: Just, like, overnight. I woke up one morning, and I happened to check, and there was 50 bitcoins. Like, hey. I like this. Now, that was a long time ago. And it is a statistical thing. So the chances today of that happening again are ridiculously vanishingly small.

Leo: That's the other thing that bothers me. But all currencies are essentially, unless they're tied to something like gold, something of actual value, they're all Ponzi schemes. They're all pyramid schemes. You just have to get in early.

Steve: Well, and the problem - the argument for releasing the dollar, the U.S. dollar from the gold standard, of course, was that our economy was inherently creating new wealth. We were actually creating new value. We needed money to be brought into the economy at the same rate that actual new value was being created. And so rather than, like, ridiculously inflating the cost of gold, we disconnected it so that it's like we could - money could track the actual creation of wealth, so it was pretty much at parity.

Leo: So you don't need to be a bitcoin miner. At some point bitcoins will be exchanged for goods and services in a free fashion. And then it's a true currency. The miners are merely putting the currency into production in a way that's frankly more rational than the Federal Reserve Bank printing something.

Steve: Yes. You could argue that it is less prone to, well, it is absolutely tamper resistant. The technology doesn't allow tampering. And the crazy mining people, what they're doing is they're saying, okay, it's harder to make bitcoins today than it was. So I want to compete with the other crazy people. So the idea is, the more hashes you can produce, the more - remember that the way this works is it's the number of leading zero bits in the hash. And so the requirement is changing in the way that - in the guesses you make to perform the hash of a chain in order to find the result that gives you all zeroes at the front of the hash.

So what's happened is, among the miners, there has been this crazy escalation in performance. But the Bitcoin technology has immediately reacted by making them work much harder than if this escalation hadn't happened. So in fact, now what we're seeing is mining pools. It's so difficult to actually get physical bitcoins yourself that people pool their resources. And if anyone in the pool scores a bitcoin, that bitcoin is divvied up based on their relative computing contribution to the pool. So, I mean, it's really been a very clever evolution over time. And as you say, Leo, I think it is ultimately, I mean, it's a phenomenon that the Treasury Department has just blessed, essentially.

Leo: Wow. That's stunning.

Steve: They said we have no problem with this.

Leo: Now, there are other, there are competitors like Litecoin. But that's okay. There can be other coins. First of all, Security Now! 287 we explained the cryptographic standard behind Bitcoin. So go back to 287 and listen to that one. And there's a book which I am about to read, I haven't read it yet, but it's been on my Audible list for some time, called "The End of Money," that talks about this whole notion. And money is just an agreed thing. It's not - there's no inherent value. So I just - I find it fascinating and somewhat unsettling. But I guess, as with many modernisms, we'll get used to it. And I can see this becoming an accepted standard, not eliminating greenbacks or euros or anything else, but supplementing it.

Steve: Well, and it...

Leo: I won't be able to pay my taxes in bitcoin, I don't think, in my lifetime.

Steve: At some point, because it's inherently virtual, it may be less prone to manipulation than physical currency which is sort of trying to straddle the virtual Internet world.

Leo: Right. We have seen peaks and valleys in value, however.

Steve: Yeah, I mean, there have been...

Leo: There've been crashes.

Steve: Yeah. I mean, I didn't know that it was at 63. That's great. I'm holding onto mine.

Leo: I would hold on. It's only going to get more valuable.

Steve: I think so. Well, because they're not going to make any more.

Leo: There's built-in scarcity, yeah.

Steve: Yeah. And in fact what may have to happen, Leo, is that there will be, once it stops, then there will be only this much bitcoin, and it will have a value.

Leo: Which, by the way, eliminates inflation.

Steve: Yes.

Leo: I think, if I understand how all this stuff works.

Steve: Yup.

Leo: There's a big payments conference [Innovation Project 2013] going on right now. And Al Gore apparently, according to the chatroom, today said he's all in favor of Bitcoin. He says, "I'm a [big] fan of Bitcoin," at the payments conference today. So, wow.

Steve: Just the technology is solid. We have just one more really interesting thing to keep an eye on.

Leo: Yeah, yeah. Well, you introduced me to Bitcoin, and I'm going to keep on you on this.

Steve: Read that book. Read that book.

Leo: I am. Have you read it?

Steve: I bet you get - no, I haven't.

Leo: Yeah, I can't wait. I downloaded it months ago, and I just haven't gotten around to...

Steve: I can imagine. You've got a few things going on.

Leo: Yeah. I keep reading - I do fiction/nonfiction, and I happened to pick a 48-hour book. Actually it was two books, so it's more like a hundred hours. But I'm almost done.

Steve: Okay. Now I've got bad news.

Leo: Oh, no.

Steve: Yeah. It's really bad.

Leo: What? Let me scroll down and see.

Steve: Okay. I created a bit.ly shortcut. The bit.ly shortcut is interscan, bit.ly/interscan,

interscan as short for Internet scan. So bit.ly/interscan.

Leo: Oh, dear. I'm reading it now, the "Internet Census 2012: Port scanning /0 using insecure embedded devices," from Carna Botnet.

Steve: Yeah. So here's the deal. First of all, I'm going to quote some things from this paper. Everybody, I tweeted the link, but also the bit.ly link is easy to find. You're going to love the graphics. Click, up on the top, click the graphics button. And look, and he's also got super-high-resolution versions of those thumbnails.

So here's what happens. The guy, he says "we" throughout this paper. And at the end he confesses, okay, "we" actually means "I" because it just was impossible to say "I this," "I that," and "I this" and so forth throughout the whole thing. So it's a guy. And with any luck he kept it quiet. And it's a good thing it's one guy because secrets are difficult to keep among people because then there's no accountability. Operating alone for six months, he poked his head out onto the Internet, wondering how many telnet ports were open. And he...

Leo: Telnet's the old, insecure way of getting terminal access to a server.

Steve: Yes.

Leo: Nobody uses it anymore. We all use SSH. Or maybe not [laughing].

Steve: Okay. 1.2 million unique, unprotected devices exposing telnet on the 'Net.

Leo: Oh, dear.

Steve: What he did was he scanned a small piece of the 'Net and found a surprising number of telnet ports. That's port 23. It's one of the ones that ShieldsUP! has been checking for people from day one because it is so bad to have - arguably, it's worse than Windows file sharing, port 23. And no one blocks it. That is, ISPs, it's off their radar. They're not blocking it. And as you said, it's like remote terminal. You use a telnet client, which are freely available. You simply connect to this port, and you get a prompt.

Leo: Now, you'd have to know a login and password.

Steve: And he tried either blank logins or admin:admin or root:root. He also tried admin:blank password and root:blank password, and that got him into the majority of these boxes.

Leo: Oh, oh. So this map that we're looking at is 460 million IP addresses, all of which respond to, well, these are ping requests. I don't care about pings.

Steve: I know. Leo, he wrote a bot which he then carefully uploaded into an initial set of these, which then scanned for others, and they sent themselves there. He wrote a worm, essentially...

Leo: This guy should be - I hope he's being careful because this is the kind of thing people go to jail for.

Steve: Oh, Leo.

Leo: Unmalicious or not.

Steve: Here's the problem. Now everyone knows. This, I mean, this is why this is the worst news I've had this year.

Leo: Well, but who - but what are these servers? They're probably old machines in the closet and stuff. I mean, what are they?

Steve: It doesn't matter. They can launch DoS attacks.

Leo: Oh, they can be used.

Steve: They can be - they are - they're Linux machines. So he says: "We used a strict set of rules to identify the target devices' CPU and RAM to ensure our binary was only deployed to systems where it was known to work."

Leo: So this is 420 - this map I'm going to show you from the paper...

Steve: 420,000 devices.

Leo: Botnets.

Steve: Yes.

Leo: These are all botnets. They're installed.

Steve: These are, no, these are host - these are available host machines with telnet exposed that will accept a remote load of code. This guy is a good guy. He wrote his system so that he was very careful not to crash anyone's machine. They expire and remove themselves. I mean, I really want...

Leo: Yeah, but he's clearly - he's in trouble. He's broken the law to do this.

Steve: Oh, my god. It's why he is completely anonymous. He posted this stuff up on Bitbucket.

Leo: Oh, okay.

Steve: He has a PGP signature only to prevent anyone else from claiming that they did this.

Leo: Got it. But we don't know who he is.

Steve: We will hopefully, for his sake, never know. And it doesn't matter. The problem is all the bad guys know.

Leo: Everybody can do it now.

Steve: Yes.

Leo: In fact, I could write a script to do this in minutes.

Steve: Oh, my god, Leo.

Leo: This is easy. And by the way, if you look at the map, the heat map, it's population centers. You could, if you overlaid this with a map of where the populations are in the world, it would look just like this.

Steve: So he said: "We also excluded all smaller groups of devices since we did not want to interfere with industrial controls" - he found open, accessible industrial control systems - "or mission critical hardware in any way." He found that, too. So the bad guys are going to. He said: "Our binary ran on approximately 420,000 devices. These are only about 25 percent of all unprotected devices found." Okay? 420,000 was 25 percent, meaning that it was 1.3 million potential targets, from which he carefully selected a subset because that's all he needed. But not everyone is going to be that thoughtful and careful.

He said: "There are hundreds of thousands of devices that do not have a real shell so we could not upload or run a binary, a hundred thousand MIPS 4KCE machines that are mostly too small" - now, that's probably Cisco routers because they use MIPS, or PowerPCs, I can't remember now, but so small machines - "and not capable enough for our purposes, as well as many unidentified configuration interfaces for random hardware. We were able to use ifconfig" - I mean, you get a full Linux prompt. You're sitting there at somebody else's Linux machine, and you have access to their LAN also.

Leo: But that's really not as bad as the fact that these default passwords still work.

Steve: I know.

Leo: So what it really is, is somebody installed Linux, didn't pay attention. Telnet was turned on.

Steve: No, no. No, no. I don't think this was installed. I think these are embedded Linux...

Leo: Ah.

Steve: Well, okay. Many of these are HP printers. Scroll down to the bottom of that, and you will see the enumeration of these.

Leo: Okay. But so somebody hacks my printer. It's not the end of the world. Can you use it as a bot?

Steve: Yes. He did. Yes.

Leo: Wow.

Steve: So he says: "We were able to use ifconfig to get the MAC address on most devices. We collected these MAC addresses for some time and identified about 1.2 million unique unprotected devices."

Leo: Nice thing about MAC address is you can tell who the manufacturer is.

Steve: Yes. And it doesn't change when the IP address floats around. So if these things were, like, on ISPs floating around, this disambiguated them. He says, "This number does not include devices that do not have ifconfig." So only the subset of those, and that was 1.2 million, had ifconfig utility installed on this Linux machine, accessible over port 23 to anyone with a telnet client. So finishing up under "Trivia," he said: "A lot of devices and services we have seen during our research should never be connected to the public Internet at all. As a rule of thumb, if you believe that 'nobody would connect that to the Internet, really nobody,' there are at least 1,000 people who did."

Leo: HP LaserJet P2055 Series. There are 6,628 of those. LaserJet 4250, there are 4,678 of those. I don't know, you know, what? Hello?

Steve: He said: "Whenever you think 'that shouldn't be on the Internet, but will probably

be found a few times,'" there are a few hundred thousand of those.

Leo: I love all these UPnP devices.

Steve: Oh, my god, I know.

Leo: Using that UPnP hole, the Portable SDK from Intel.

Steve: Uh-huh. He says, "Like half a million printers, or a million webcams, or devices that have 'root' as their root password."

Leo: Oh, scary.

Steve: He said: "We would also like to mention that building and running a gigantic botnet and then watching it as it scans nothing less than the whole Internet at rates of billions of IPs per hour, over and over again, is really as much fun as it sounds."

And then finally, under "Who and Why," he said: "You may ask yourself who we are and why we did what we did. In reality, 'we' is me. I chose 'we' as a form for this documentation because it's nicer to read, and mentioning myself a thousand times just sounded egotistical. The why is also simple: I did not want to ask myself for the rest of my life how much fun it could have been or if the infrastructure I imagined in my head would have worked as expected. I saw the chance to really work on an Internet scale, command hundreds of thousands of devices with a click of my mouse, port scan and map the whole Internet in a way nobody had done before, basically have fun with computers and the Internet in a way very few people ever will. I decided it would be worth my time."

Leo: Yeah.

Steve: Now, this guy, in this paper, which is up on Bitbucket, it's linked to from the link I gave, bit.ly/interscan, he lays out the architecture. This is even if somebody copied what he did. But the problem is he was very white hat. He was very careful. He didn't need to push the limits because he had all the willing machines he needed, even if he only used those with lots of RAM and lots of CPU horsepower. He also ran his bot at the lowest possible priority so that it wouldn't interfere with anyone else's traffic, and he didn't need it to take over. But, Leo, mark my words, I mean, this is - all the hackers know this now. This is going to launch a revolution. And it's not good because this is going to be far more fun than them trying to get people to click on a link in a browser to get some bot loaded into someone's machine that then lives for a while.

Leo: There's millions of machines just sitting there waiting. Wide open.

Steve: Yes.

Leo: Waiting for - just saying, come on, come on.

Steve: Accepting a command-prompt logon and then...

Leo: He even told people what passwords to try. I mean, he's given - the farm has been given away.

Steve: Yes, completely.

Leo: Although it's so obvious that I can't imagine others have not already - are not aware of this. He took a big chance in coming public with this. And my strong advice to him is do not boast. Do not go into IRC, say, yeah, that was me. Do not say a word. Go underground, deep, deep underground because you'll be going to jail for a long, long time as soon as anybody catches you. Unfortunately. Because I don't think he's done anything wrong. But now the bad guys can.

Steve: I know. They all know.

Leo: And what that means is massive botnets for DDoS attacks; right? That's the primary use of this.

Steve: Yes. Yes. Or email spamming, I mean, anything where you could use distributed low-power machines. Well, basically botnets. He really lays it out. His machines expire themselves. They leave gracefully. I mean, it took him six months to build this and test it and deploy it. And he talks about PHP and Python code and how he set it up. And he had a web interface that allowed him to control this thing. I mean, the guy had a ball. And he had a sort of a...

Leo: A little too much fun.

Steve: Yeah, I mean, I would - this would be just a kick in the pants. But the bad news is, this is not rocket science. This is standard Internet technology. Everybody knows how to do this. And the revelation that there are this many machines that you can log onto remotely that are unattended, they're in people's closets, they're in people's racks that have been forgotten, I mean, they are sitting there waiting to be taken over. And just count the minutes. I mean, we're going to be hearing about this. This is not over. This has been a nice, happy little white hat adventure. There's more coming because there's no way this is not going to get leveraged.

I don't know it gets fixed. That's the problem, is these are machines that will never be changed. They will never be secured. We talked about the UPnP problem and how widespread that is and that there are many boxes that are never going to have their Universal Plug & Play locked down because people are not coming by ShieldsUP! at GRC to scan themselves and take action affirmatively. Similarly, these port 23 telnets with empty or default logons, those are going to be there forever. And now everybody knows.

Leo: Yeah, because whoever turned that on, whether it's an HP printer, although that's kind of a shocking flaw, clearly didn't pay any attention. They turned on a telnet service, didn't modify the password. You shouldn't have telnet on anyway.

Steve: But this can't be 120 million people or 420 million people. This just has to be...

Leo: No, it's the manufacturer.

Steve: Yes. It's the manufacturer. And, I mean, that's the problem.

Leo: So somebody's saying "What's the fix?" There's no fix. This exists and will always exist.

Steve: Yes. It's done. It's out there. It's too late. It's over.

Leo: Well, I don't know if it's over. But...

Steve: Oh, wait. It's over. No, I mean...

Leo: You expect to see massive DDoSes all of a sudden?

Steve: I don't think - well, okay. There are already massive DDoSes. There are already botnets. They're just not taking advantage of people's routers. And so now here's a whole 'nother class of opportunity for networks, for malicious networks, and for people to, like, bounce their traffic a few times. I mean, you can't do - well, I don't know. I was going to say you can't do really sophisticated things like Tor nodes. But maybe you can.

Leo: Depends what's inside that telnet.

Steve: Yeah, if you have enough...

Leo: If there's a full Linux box, you could do anything you want.

Steve: Yup.

Leo: And I imagine, given the millions of available devices, there are probably hundreds of thousands of full Linux boxes at the other end of this. I don't know why. Certainly, anybody who's at home and almost anybody listening to this show has a router. And this isn't going to happen unless the router has telnet turned on. But I

doubt it.

Steve: All you have to do is go to ShieldsUP!.

Leo: Go to ShieldsUP!.

Steve: There's no test you can run at GRC in ShieldsUP! that won't tell you if you have telnet port 23 open.

Leo: Port 23 is turned on.

Steve: It's the first thing I check. It's just like, oh, my god.

Leo: Actually, the first thing you check is probably NETBIOS because that's why you made ShieldsUP!.

Steve: Yeah, I do. And actually I greet you by name if you're crazy enough to have NETBIOS enabled. I say, "Hi, there, Mark."

Leo: Hey, Leo, you have NETBIOS turned on, huh? Wonder why you knew that?

Steve: That was the original shocker. People would come to GRC for the first time, and I would know their name. And it's like, holy crap, how does he know my name?

Leo: Wow. This is interesting.

Steve: Oh, Leo. So everybody listening, you've got to go: bit.ly/interscan. Read this guy's paper. Look at those images. The images are, like, wallpaper for your desktop. They are gorgeous.

Leo: They're beautiful. And they're very high-res.

Steve: Yes, he's got them in 2200x1600 and higher. And did you see the animated one? There's one you can click on to start the animation, where it shows he took snapshots as the Earth rotated, and you can see a very dim, whatever they call that cool sine wave that moves across the map, showing where the sun is lighting the landscape. There's a neat name I can't think of. Begins with D, maybe?

Leo: Oh, yeah, the, yeah, the terminator.

Steve: Terminator, yes, you can see the terminator slowly move back and forth. And you see the lights, you see the scan change over time. So some of these things are being turned on and off. And they're, like, on during the day...

Leo: Well, they're printers [laughing].

Steve: ...and off at night [laughing].

Leo: That's what I find amazing. These things are printers in many cases. So people are saying, oh, well, everybody ought to have a router and turn - but really these are neglected devices or devices people don't even know have telnet turned on.

Steve: The word is "appliance." They are appliances.

Leo: They're appliances. They're on the Internet direct because, if you're behind a router, chances are pretty good it's not exposed. These are Internet appliances, like printers, that are just sitting on the 'Net for some reason.

Steve: Internet-facing appliances.

Leo: Which is bizarre.

Steve: Yeah.

Leo: Yeah, I like this animated GIF. This is good. You can see the terminator line.

Steve: Isn't that neat? He did a really nice job.

Leo: Well, you know, he's probably given way too many clues as to his identity. I hope...

Steve: Whoever you are, hats off to you for a beautiful piece of work, and darn you for exposing it. I mean...

Leo: Well, I bet you bad guys knew this. This isn't that hard to figure out. Is it?

Steve: I guess maybe. Maybe bad guys were keeping it quiet?

Leo: That's what my guess would be.

Steve: It's just entirely - okay, but look, Leo. We are always running across things that are frightening that no one knew, like the Universal Plug & Play port being open. It's like, there they were, all open. And it took HD Moore to scan the 'Net and find them.

Leo: I'll tell you, though. If I look at my server logs, I see pretty much nonstop telnet bangs on my servers.

Steve: Oh, I know. I know. 23 is...

Leo: Mostly from China. And so I'm pretty much guessing some smart university student in China, or maybe somebody in the military, has figured this one out. Don't you think?

Steve: Yeah.

Leo: Because, I mean, telnet is - that's the first thing people try.

Steve: And Leo, the nice thing is there's enough there for everyone to share.

Leo: [Chuckling]

Steve: You got 420 million. How many do you need? How greedy are you?

Leo: Well, okay. So the way a DDoS works is you have enough machines pinging a site that the site, no matter how much bandwidth it has, cannot service them all. The bandwidth gets clogged. And of course there are companies, lots of them, that provide DDoS protection by merely widening the pipe. But with millions of machines, I don't know how many it would take to kind of overrun the largest possible pipe.

Steve: It's dishearteningly few.

Leo: Several hundred thousand would be more than enough; right?

Steve: Well, and the worst attacks are the in-protocol attacks. A ping is sort of old school, and lots of ISPs block them.

Leo: You send a SYN, though, if you send a SYN to port 80, you can't block that because you wouldn't have a website.

Steve: What's worse is send a valid request.

Leo: Okay.

Steve: Because then the website has to deliver a page.

Leo: Has to respond, yeah.

Steve: And if it's a PHP site, and it's using computational resources to interpret and...

Leo: Could bring it down instantly. Look how many sites we bring down all the time.

Steve: Yes, yes. The moment we talk about something...

Leo: Send a thousand people, it's going to bring a site, most sites, down.

Steve: Yes.

Leo: Send 100,000 people, I doubt there's any site that can survive.

Steve: No, no.

Leo: Well, the good news is all the gambling sites will be offline during major gambling events. I guess the next one is the Indy 500. We'll see if, come Memorial Day, you cannot get online [laughing]. Wow.

Steve: Yeah. I mean, it is really, really significant that there is this kind of - there's this presence of unattended, obeying machines...

Leo: Now, this guy already is in deep trouble because what he's done violates every law known to man. It's federal wire fraud laws that don't allow you to log onto somebody's computer. Even though they leave it wide open, you're still not allowed to do that. Why doesn't this guy write a bot that just changes the password to some random string on all of these devices? What would stop him from doing that? He's already on these devices.

Steve: Or just shut down - better would be...

Leo: Shut down telnet.

Steve: ...to shut down the telnet service. Just edit it. He may not be able to make a

permanent change, that's the problem, because he may not have access to...

Leo: Change the RC file or whatever, yeah. But he could at least shut it down for now. Of course the machine's turned off and on, then it's going to start up again.

Steve: And they often do. He explains in here that...

Leo: You could see them on that map.

Steve: Yes. He was seeing machines disappear. They were moving, or he said also some machines just reboot themselves by schedule, on a schedule, every few days, just to clean out any debris that they've accumulated. So unless he could make permanent changes to the nonvolatile memory in those machines, anything he did would be temporary.

Leo: My point being he's already violated every federal, U.S. federal law, and probably federal laws in most countries. Might as well go all the way and fix the problem.

Steve: He sounds like a nice guy, too.

Leo: He sounds like a nice guy. I'm sure he's considering it. I mean, in many cases he had root.

Steve: Yes. That's what he was getting. What he was getting was full root access. He was logging in, either with a blank username and password or as admin or as root.

Leo: And that gives him write access. He could probably fix a few of them.

Steve: Yeah.

Leo: Maybe a few million.

Steve: Well, he has the infrastructure in place to do it before anybody else could.

Leo: That's what's interesting, because he was able to do this by commandeering these machines to spread the botnet. It wasn't all from one PC in his closet.

Steve: That's why it was a worm. He built a beautiful...

Leo: It's amazing.

Steve: ...Linux worm which then propagated, just like in a flash, across the Internet. And its goal was to find other bots. And he shows how it escalates. The first few, he, like, launched a few thousand. They all begin scanning. He partitioned the IPv4 address space. Now, that's one other point that he makes that I didn't read because I didn't want to read the entire paper verbatim, anyone can find it, is he mentions that this is only possible on IPv4 because we only have 4.3 billion IPs, and they can be scanned. When you go from a 32-bit address to a 128-bit address, everything changes.

Leo: Good. Let's all go IPv6 now.

Steve: Well, none of those bots are going to. None of those boxes are going to. They're just passive...

Leo: They're printers. And we already know how little these device manufacturers care about fixing their problems. This UPnP, not a word from any router manufacturer. Not a word.

Steve: Nope, none. I wonder if there's going to be a sudden spike in demand for toner.

Leo: You know, that's what he should just do is, the ones that are printers, just print a big page that says, "Hey, moron, lock down your machine."

Steve: [Laughing]

Leo: Okay, that's all you do. You print one sheet on every printer that you can get to and say here's what you need to do.

Steve: And also, Leo, remember this. There are infrastructure-critical machines, he refers to them in more detail than I did in the paper.

Leo: Like SCADA boxes, things like that.

Steve: Yes. And he's also on routers. And because he is who he is, he is not turning around and looking into the network. He talks about all the tasty machines behind these. This is not going to be a hands-off policy for most of the hackers on the Internet. They're going to get on a box and go, hmm, where am I? Poke around. What machines are connected? What fun can I have? I mean, it is - this is a catastrophe.

Leo: [Laughing] Wow. Okay.

Steve: Yeah. Yeah. Okay.

Leo: Bury the lead, Steve.

Steve: I know. Well, and we're not going to get to it this week. I have two things left I want to share.

Leo: Okay.

Steve: Our friend Simon Zerafa, who - he tweeted me something that is really cringe-worthy. He said, "Two bytes walk into a bar. First one, the first byte turns to the second and says, 'I think I may have a parity error.' The second one says, 'Yes, you do look a bit off.'"

Leo: Oh, it's horrible.

Steve: Oh, ow, yeah [laughing]. I got a really, really nice note from a listener, Richard Curtis, who said, "I've written a testimonial," but he didn't know where to send it. So he sent it to my tech support guy, Greg. So the subject is "I've Written a Testimonial." And then his letter, his note starts, "But couldn't find anywhere on GRC's or SpinRite's pages to submit one. So I decided to submit it this way. Please let me know if there's anything else I need to do."

He said, "Just another miracle to add to your enormous collection. I have a Dell Inspiron 1520 laptop running XP Professional SP3." Man after my own heart. He said, "In early September 2012," so a few months ago, "I got a BSOD," the Blue Screen of Death, "on startup, informing me that an essential system file in the boot process was corrupt. I had purchased the computer in '08," so four years previous, "so it was out of warranty. I paid Dell customer service $129, seeking their help in getting it up and running." So, okay, $129 to Dell.

"The best they could give me for the price of admission was to tell me to reinstall the operating system. Like everyone else, I had thousands of pictures and my personal, professional, and financial life on that computer. Like almost everyone else, I didn't observe a regular backup schedule, even though I own two 1TB Phantom external hard drives. I wasn't about to do anything as drastic as a system reinstall before I could engage in data recovery. But I had previous experience with data recovery and knew it would likely cost me about as much as a new computer." That's true, or a lot more, actually.

"I switched over to using my wife's brand new Asus laptop with a Core i7 processor and Win 7 while I pondered my approach to data recovery. Several months went by; and, tiring of my monopolizing her new computer, my wife suggested I buy a new one of my own. Nice as her Asus is, I didn't want to pull the trigger on that kind of financial commitment, either. So I began scouring the web to find recommendations for user-controlled data recovery.

"Among several promising programs, SpinRite stood out. I read absolutely everything on the SpinRite website about the program and how it worked. I'm no techie, but it all made

sense to me. Impressed by Steve's background in computer hardware, preexisting the Internet and PCs; his long-term commitment to SpinRite for decades; SpinRite's nondestructive process; the glowing external reviews; the many user testimonials about not just data recovery, but the restoration of failing drives; and SpinRite's money back guarantee and lifetime updates, there was no question about the choice of program.

"I paid my $89 lifetime license fee, burned SpinRite to CD on my wife's computer, and started it on my nonbootable Dell at 5:00 a.m. four days ago. It finished its work nine hours later." That is, not four days and nine hours, but it only took him nine hours. He didn't write "for four days." He says, "Holding my breath, I started the Dell up, and, wham, the Windows start screen appeared. It booted flawlessly, and there were all my precious files. I'm writing this message on the Inspiron right now. All the previous warnings of impending doom, such as hanging processes and stack dumps, are gone.

"Add me to the family of true believers. SpinRite is the most reasonably priced, absolutely essential program that every computer owner owes to him/herself to obtain and have on hand to stave off the inevitable drive failures. I will be running it on the Dell, my wife's Asus, and my son's Dell with Vista, quarterly, to keep them in shape. And I'll back up all my files. I promise." And then he concludes with, "By the way, SpinRite found comparatively few bad sectors, so I guess the drive was actually in fairly good shape." And he demonstrates that he really did read everything because he learned the lesson about maintenance, that SpinRite can not only recover, of course, but is really good for long-term maintenance, run every few months. So, wow, great testimonial. Thank you, Richard.

Leo: Isn't that nice. So do you want to save the hash tables for later?

Steve: We have to.

Leo: We're kind of out of time.

Steve: Yeah. We will do it week after next. I have tons of really interesting material about the way they work, about who uses them, about how they operate. It'll make for a great podcast, which unfortunately, well, not unfortunately, we had a great one just now, really.

Leo: Yeah. It turns out to be a pretty important thing.

Steve: This is very, very important. When you learn that the Internet has telnet logon-able, unattended appliances in the hundreds of millions - and remember, I will say again, Leo, this is not just for outbound-reflected traffic. All of these are in front of somebody's private LAN. And they allow admission to that LAN. So, I mean, this is not good.

Leo: Not good would be an understatement.

Steve: Yeah.

Leo: Steve Gibson is at GRC.com. Next week, Q&A, which means if you go to GRC.com/feedback you can ask your question. Steve will pick - actually, we have leftovers from last week. We'll use some leftovers, maybe some fresh. Mix it in, it'll make a nice casserole. Put some potato chips on the top. You can also, while you're there, get 16Kb audio versions of the show; transcriptions, too. He does all that just for you, for the bandwidth-impaired. For those of you with ample bandwidth, watch live every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC. Or download audio or video after the fact, high-quality versions of both available at TWiT.tv/sn for Security Now!, or wherever better podcasts and Internet broadcasts are stored. Just search for "TWiT" or "Security Now!," and you'll find it. I guess - oh, and this would be a good time maybe to go to ShieldsUP!. Just make sure that you don't have a telnet port lying open, flapping in the wind.

Steve: Yeah. I would love to know more about those boxes. The only thing that we didn't get is what are all those. I mean, we know that a bunch are printers. That's crazy. Why does a printer have telnet at all running? But one of the problems is people tend to leave things in default mode, even people apparently setting up and installing firmware in unattended boxes. I mean, port 23 is nuts to have wide open and running a telnet server, just like, okay. So these must have been around for a long time. And they're going to be around forever. [Frustrated noises].

Leo: I'm sure we'll hear more. And this is the show where you learn about all of that stuff. And Bitcoin, too. Thank you for joining us, Steve. We'll see you next time on Security Now!.

Steve: Thanks, Leo.